NIST PUBLICATIONS

NIST Special Publication 500–218

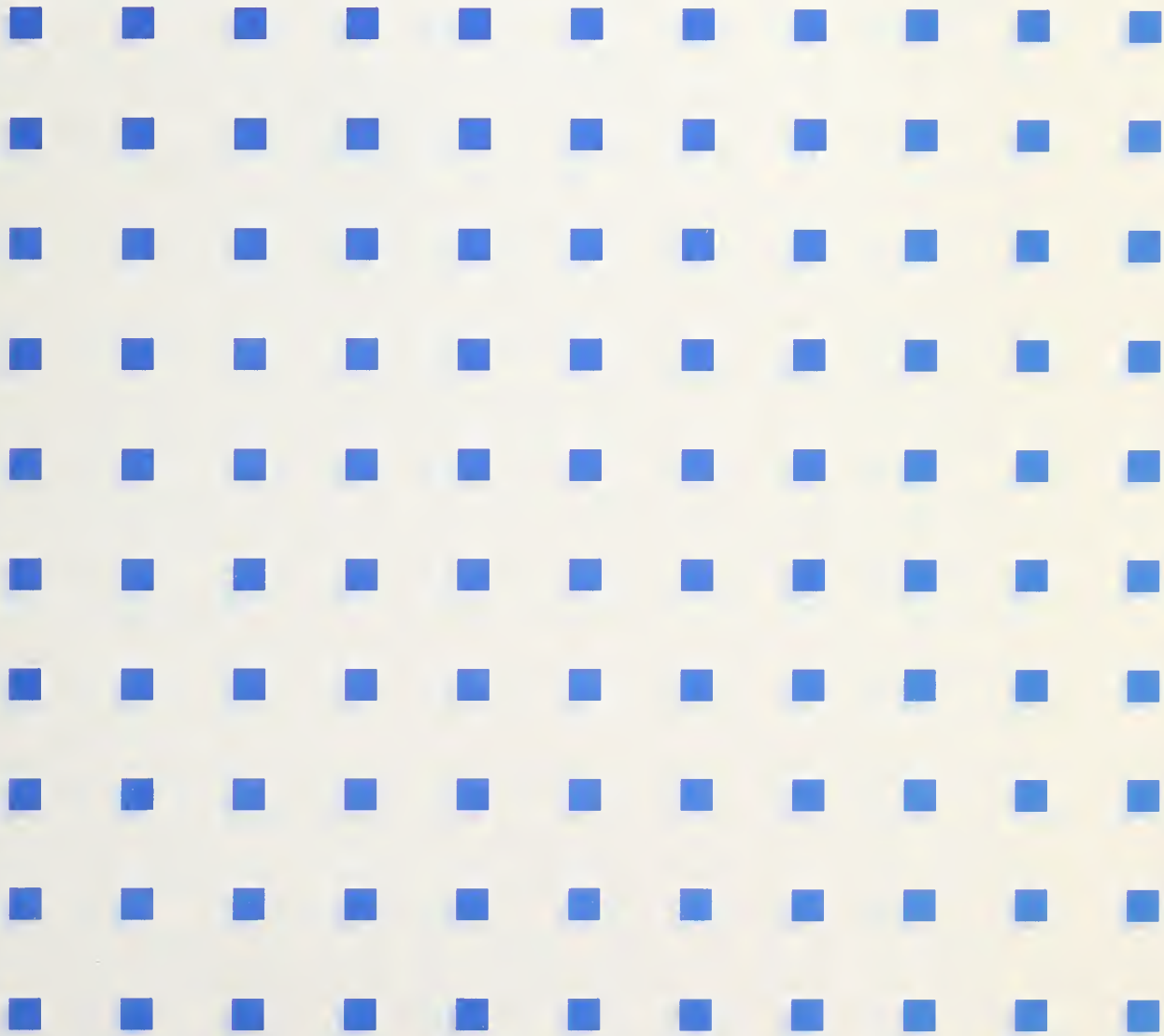
Computer Systems Technology

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards and Technology

NIST

Analyzing Electronic Commerce

Len Gebase
Steve Trus



The National Institute of Standards and Technology was established in 1988 by Congress to "assist industry in the development of technology . . . needed to improve product quality, to modernize manufacturing processes, to ensure product reliability . . . and to facilitate rapid commercialization . . . of products based on new scientific discoveries."

NIST, originally founded as the National Bureau of Standards in 1901, works to strengthen U.S. industry's competitiveness; advance science and engineering; and improve public health, safety, and the environment. One of the agency's basic functions is to develop, maintain, and retain custody of the national standards of measurement, and provide the means and methods for comparing standards used in science, engineering, manufacturing, commerce, industry, and education with the standards adopted or recognized by the Federal Government.

As an agency of the U.S. Commerce Department's Technology Administration, NIST conducts basic and applied research in the physical sciences and engineering and performs related services. The Institute does generic and precompetitive work on new and advanced technologies. NIST's research facilities are located at Gaithersburg, MD 20899, and at Boulder, CO 80303. Major technical operating units and their principal activities are listed below. For more information contact the Public Inquiries Desk, 301-975-3058.

Technology Services
- Manufacturing Technology Centers Program
- Standards Services
- Technology Commercialization
- Measurement Services
- Technology Evaluation and Assessment
- Information Services

Electronics and Electrical Engineering Laboratory
- Microelectronics
- Law Enforcement Standards
- Electricity
- Semiconductor Electronics
- Electromagnetic Fields[1]
- Electromagnetic Technology[1]

Chemical Science and Technology Laboratory
- Biotechnology
- Chemical Engineering[1]
- Chemical Kinetics and Thermodynamics
- Inorganic Analytical Research
- Organic Analytical Research
- Process Measurements
- Surface and Microanalysis Science
- Thermophysics[2]

Physics Laboratory
- Electron and Optical Physics
- Atomic Physics
- Molecular Physics
- Radiometric Physics
- Quantum Metrology
- Ionizing Radiation
- Time and Frequency[1]
- Quantum Physics[1]

Manufacturing Engineering Laboratory
- Precision Engineering
- Automated Production Technology
- Robot Systems
- Factory Automation
- Fabrication Technology

Materials Science and Engineering Laboratory
- Intelligent Processing of Materials
- Ceramics
- Materials Reliability[1]
- Polymers
- Metallurgy
- Reactor Radiation

Building and Fire Research Laboratory
- Structures
- Building Materials
- Building Environment
- Fire Science and Engineering
- Fire Measurement and Research

Computer Systems Laboratory
- Information Systems Engineering
- Systems and Software Technology
- Computer Security
- Systems and Network Architecture
- Advanced Systems

Computing and Applied Mathematics Laboratory
- Applied and Computational Mathematics[2]
- Statistical Engineering[2]
- Scientific Computing Environments[2]
- Computer Services[2]
- Computer Systems and Communications[2]
- Information Systems

[1] At Boulder, CO 80303.
[2] Some elements at Boulder, CO 80303.

NIST Special Publication 500–218

Analyzing Electronic Commerce

Len Gebase
Steve Trus

Systems and Network Architecture Division
Computer Systems Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-0001

June 1994

U.S. Department of Commerce
Ronald H. Brown, Secretary

Technology Administration
Mary L. Good, Under Secretary for Technology

National Institute of Standards and Technology
Arati Prabhakar, Director

Reports on Computer Systems Technology

The National Institute of Standards and Technology (NIST) has a unique responsibility for computer systems technology within the Federal government. NIST's Computer Systems Laboratory (CSL) develops standards and guidelines, provides technical assistance, and conducts research for computers and related telecommunications systems to achieve more effective utilization of Federal information technology resources. CSL's responsibilities include development of technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive unclassified information processed in Federal computers. CSL assists agencies in developing security plans and in improving computer security awareness training. This Special Publication 500 series reports CSL research and guidelines to Federal agencies as well as to organizations in industry, government, and academia.

National Institute of Standards and Technology Special Publication 500-218
Natl. Inst. Stand. Technol. Spec. Publ. 500-218, 40 pages (June 1994)
CODEN: NSPUE2

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1994

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402

Contents

List of Tables

List of Figures

Acknowledgments

An earlier report entitled, *Electronic Commerce: Analysis, Findings, and Opportunities for the Computer Systems Laboratory*, issued as an internal report of the NIST's Computer Systems Laboratory (CSL), provided the basis for much of the material presented in this document. In particular, the material on EDI in Chapter 2 of this document was borrowed largely from that document. The earlier report represented the findings of an Electronic Commerce study group, created by the director of CSL. Steve Trus chaired the group, and Joe Collica served as technical editor. Other participants were Donna Dodson, Larry Welsch, David Su, Judi Moline, and Lynn McNulty.

Abstract

One area certain to undergo rapid change in the foreseeable future is the way we conduct our business and social activities. Whereas in the past, business transactions and social exchanges have required direct personal interaction, or interaction through the phone or postal systems, in the future, this will be altered by the availability of automated processing procedures and a communications network. While large communications networks, such as the Internet, have not, as of yet, radically altered the way we conduct these activities, for several reasons this will almost certainly change in the future. One reason for this stems from advances in technology. Specifically, increased computing power and network bandwidth, and software able to effectively utilize these increases, will make it possible to carry out activities that, today, can only be carried out in a cumbersome manner. Furthermore, the expansion of network access to a much larger user community than presently exists, along with the benefits accompanying automation, will provide the impetus for making this transition.

Electronic commerce—the subject of this paper—is a term over which some confusion still exists. While we will attempt to be precise in defining this term, and thereby eliminate confusion over its meaning (at least within the context of this paper), this is not the primary reason for producing the paper. Perhaps, the foremost reason for doing this is to foster movement in the direction of automation, necessary if the above changes are to become a reality. The primary way in which this paper can aid movement in this direction is by illuminating the benefits that can be obtained when these changes are effected. Here we will argue abstractly (supported by some experience—evolving through ongoing work in the NIST Electronic Commerce Integration Facility) that significant benefits can be expected when certain business procedures are automated, i.e., when they fall within the purview of electronic commerce. Furthermore, we will argue that there is a set of services: communications, data management, and security, that are essential for establishing an electronic commerce capability.

Chapter 1

Introduction to Electronic Commerce

This report begins, after citing some important technological advances, by defining electronic commerce and identifying the scope of issues to be addressed within this paper. It then proceeds to examine some ways in which electronic commerce is presently being conducted, most notably with Electronic Data Interchange (EDI). An architectural model for supporting services necessary to conduct electronic commerce is then defined. The chapters that follow provide further detail on the model's components. The final chapter draws some conclusions about the benefits of deploying electronic commerce.

1.1 Laying the Groundwork for Electronic Commerce

Continuing increases in the computational power of computers and the capacity of networks to carry data have put us on the doorstep of a new era in distributed computer processing. Teraflop computers and gigabit networks, now in the experimental stage, will enable computers to access remote information and provide services that will—for many applications—diminish the importance of distance to virtual insignificance. These advances in distributed computing will revolutionize the way we acquire information, interact with our colleagues, and carry out business and social activities.

Already researchers have benchmarked processors at 20-gigaflops (10^9 floating point operations per second). Experimental networks have achieved data rates in excess of several gigabits per second. Oak Ridge National Laboratory has announced that it has contracted with Intel for a machine with a peak processing rate in excess of 100 gigaflops [1]. Scientists are also designing machines using massively parallel processors (MPPs) they believe will be able to operate at the rate of a teraflop or more by the end of the decade [2]. Some network researchers believe that future optical networks will be capable of achieving data rates as high as a terabit per second [3].

Along with these technological advances, many economists believe that the nation's economic success will hinge on the ability to innovate, design, and manufacture—areas for which increased computing power is essential. Recognizing the importance of these increases in computing power and network capacity, a National Information Infrastructure (NII) [5] has been proposed by the Administration that will link together our educational institutions, health care facilities, businesses and industry, public libraries, and homes. Furthermore, a

report from the Office of Science and Technology Policy, entitled the *High Performance Computing and Communications Program* (HPCC) [4], proposes a program of research to address "grand challenge" scientific and engineering problems, and to accelerate the availability of high performance computers and networks. Grand challenge problems include, among others, weather prediction, design of protein structures, rational drug design, researching human anatomy, solving national security problems, and improving research and education communications. The Computer Systems Policy Project (CSPP), a committee of CEOs from some of the nation's leading computer manufacturers and software companies, have noted the importance of the HPCC program, but they believe it does not go far enough. They believe there is a need to build a national information infrastructure (NII) that will link together four major components: computers, networks, information, and people. Computers will provide the raw computational power necessary to support new and powerful software applications; high speed networks will support convenient user to user communications and allow access to information throughout the network.

In this future environment, commerce will be carried out in a way that is markedly different from the way it has been carried out in the past. Many of our business transactions will be carried out without human intervention. Many of our educational endeavors and social interactions will take place without leaving our homes. Our health-care facilities and our research institutions will share information which cannot be readily shared today. This new manner of carrying out commerce we characterize with the term *electronic commerce*—the subject of this paper.

The HPCC has characterized electronic commerce as follows:

> *Electronic Commerce: Electronic commerce integrates communications, data management, and security services, to allow business applications within different organizations to automatically interchange information. Communications services transfer the information from the originator to the recipient. Data management services define the interchange format of the information. Security services authenticate the source of information, verify the integrity of the information received by the recipient, prevent disclosure of the information to unauthorized users, and verify that the information was received by the intended recipient. Electronic commerce applies and integrates these infrastructure services to support business and commercial applications including financial transactions such as electronic bidding, ordering and payments, and exchange of digital product specifications and design data.*

In the following section, commerce as it has been conducted traditionally, and as it will be conducted electronically, is discussed. This discussion leads to the formulation of a working definition of electronic commerce suitable for the purposes of this paper, and consistent with the HPCC's above characterization.

1.2 Defining Electronic Commerce

Commerce is usually thought of in a business context to mean an exchange of goods or commodities, especially on a large scale. Goods are not conveyed without being accompanied

by a variety of information. A typical commerce activity may include a purchase order and invoice. It may require updating accounting and inventory records, and it may require manipulating and modifying administrative information. Commerce, though, is not limited to business activities, it also applies to social exchanges, such as exchanges of ideas or opinions. Commerce, therefore, can be considered to be an exchange of goods or information in carrying out social or business activities. For some commerce activities, it is the exchange, or conveyance, of information itself that is the end objective. Examples of these types of activities include mail or phone exchanges, and may, or may not be, directly related to a business transaction. Thus, information—as the object of a commerce activity or accompanying a commerce activity—has been an integral part of conducting commerce traditionally.

Information is also an integral part of electronic commerce, but electronic and traditional commerce each deal with information differently. Conveying information has traditionally been done through paper exchanges, direct personal contact, or through the phone or postal systems. In electronic commerce, information may be conveyed via a communications network, or other electronic media. The way information is processed in electronic commerce also differs from the way it has been processed traditionally. Traditionally, information accompanying a business transaction had to be acted upon by the individuals involved in the transaction. In electronic commerce, information processing is automated, reducing or eliminating the need for human intervention and the use of paper. Thus, conducting commerce electronically, differs from conducting commerce traditionally, in the way information is exchanged and processed. Since it is this change in the way information is processed and exchanged that distinguishes electronic from traditional commerce, we formulate the following definition: *Electronic commerce is commerce transacted using automated processing procedures integrated with automated procedures for the interchange of information.*

This integration in the processing and exchange of information can itself be achieved through integrating a set of services. As will be seen in Chapter 4, this set is made up of communications, data management, and security services. By integrating these services with the business application, electronic commerce can make these services transparently available to the user; (the application could be unrelated to business without being inconsistent with the view of traditional commerce, as can be seen from the above discussion, but the focus of interest here is primarily on business applications). Through this integration and automation, conducting commerce is made more efficient, convenient, and accurate.

A number of activities, including mail exchanges, remote access to database systems, and automatic monitoring of store inventory levels, can be used in electronic commerce. It is the expansion of these activities, along with their incorporation into the process of conducting commerce electronically, that is one of the major objectives of examining the topic of electronic commerce—ultimately, one would like to see these activities become as commonplace as the use of the telephone is today. Regardless of the merits of the above definition of electronic commerce, it can, nevertheless, serve as a reasonable basis for focusing discussion. Discussion should foster movement in the direction of automation, i.e., it should help publicize the topic, stimulate interest, and, in doing so, encourage organizations to establish a capability to carry out activities electronically.

Given these objectives, the study of electronic commerce is not intended to define new technologies, per se, but rather to specify an environment in which new, as well as estab-

lished, technologies can be applied. This will require determining the necessary infrastructure components for enabling electronic commerce activities. In practice, this may require determining how various components can be integrated to support new, or previously unavailable, applications.

1.3 An Overview of Electronic Commerce

Creating a ubiquitous electronic commerce environment will require deploying a network capable of providing connectivity to a large user and service provider community. Hardware, software, and security issues must be addressed. New applications that take advantage of networks and improved computer performance will be required. Networking software that utilizes the increased bandwidth will be needed to support the new applications. Applications beyond those currently envisioned will evolve, and sophisticated user interfaces that allow users to conveniently take advantage of the services provided by this new environment will emerge. One of the key components for developing an electronic commerce environment will be software that can support local applications and interoperate in a heterogeneous networking environment; this will require the use of open systems based on national and international standards.

To limit the size and scope of this paper to a manageable size, rather than attempting to address the full range of issues that must be addressed in developing an electronic commerce environment, this paper will focus on an examination of some of the essential software components needed for developing an electronic commerce infrastructure. The broader environment, its impact on users, and the range of new applications likely to emerge in this environment will only be given cursory coverage.

The one electronic commerce application, however, that will be examined in some detail is Electronic Data Interchange (EDI[1]) [6] [7]. Work on the standardization of business forms dates back to the 1960s. Today a large number of implementations for supporting EDI and EDI environments have been developed and are in operational use. These environments may represent the most advanced state of electronic commerce currently in use; this has resulted in EDI and electronic commerce sometimes being viewed synonymously—a viewpoint not adopted here. But EDI does represent a significant achievement in the area of electronic commerce. Even though its use has been rather limited, the benefits accruing from its use have been clear. For this reason when the architectural model for electronic commerce is formulated in Chapter 4, the model is motivated—to some extent at least—by the example of EDI; this is not because EDI encompasses all of electronic commerce, but because there is a need for electronic commerce to encompass EDI.

In addition to looking at EDI, a few other examples of communications applications will be examined. EDI itself is not a communications application but it does require communications software to convey EDI forms between users. Other communications applications discussed include electronic mail protocols, file transfer protocols, directory services protocols, and virtual terminal protocols. These, in turn, require a number of software modules that provide networking services.

[1]Unless indicated otherwise, no distinction in made between X12 and EDIFACT EDI.

The fundamental components of an electronic commerce infrastructure (in our view), are data management, communications, and security. While security may not seem necessary for setting up an experimental environment, its importance is so fundamental to conducting even simple business activities electronically, that it can be seen as essential for conducting electronic commerce even on an experimental basis. Thus, particular attention is paid to each of these items in this paper. Finally, it should be noted that by no means do these three components comprise all that is required for effecting electronic commerce. Hardware, operating systems, user interfaces, and the applications themselves are arguably as important. The latter two are included in the architectural model formulated for electronic commerce in Chapter 4; the former two are not part of the model for reasons that are explained when the model is presented.

Chapter 2

Electronic Data Interchange

Electronic Data Interchange (EDI), strictly speaking, is simply a set of data definitions that permit business forms, that would have been exchanged using paper in the past, to be exchanged electronically. This simple set of definitions has spurred a number of organizations to put in place an operational environment in which the exchange of electronic business forms substitutes for the exchange of paper forms. This has resulted, in some cases, in the establishment of an EDI environment which arguably represents the most advanced state of electronic commerce today, causing some to view EDI and electronic commerce as one and the same. We view EDI only as a subset of electronic commerce, albeit a very important one. As such, EDI provides an excellent example of a working electronic commerce environment and is a good starting point for examining electronic commerce. This chapter, therefore, will provide an overview of EDI, before establishing a more general model for electronic commerce.

2.1 Using EDI

Rather than look at EDI methodically, we begin informally by looking at some practical ways in which EDI can, and is, being used today.

EDI establishes a set of standardized forms referred to as either transaction sets or messages[2]. These forms are defined for common business transaction functions, such as purchasing and finance. As a simple example of how EDI can be used consider the following scenario: A retail store's inventory has been depleted and must be restocked. Instead of proceeding conventionally, an EDI purchase order is sent to the supplier. On receiving the order, the supplier sends an EDI invoice form to the retail store advising that the order has been shipped. When received, the retail store sends a payment order form to its bank requesting that an electronic funds transfer (EFT) be made. Taking advantage of the electronic capabilities available to it, both the retail store and the supplier have conducted a business transaction without the use of paper or the need for human intervention. In eliminating these, the transaction is less subject to error and also more efficient. Table 2.1

[2]X12 uses the term "transaction set", EDIFACT "messages"; throughout this paper "form" will be used when distinguishing between these is unimportant.

contains a sampling of some common business function standardized EDI forms and their usage.

2.2 The Basics of EDI

EDI is defined as the exchange of computer processable data in a standard format between organizational entities. The formats and procedures needed to generate EDI forms have been standardized. Although many EDI standards exist today, the X12 and EDIFACT (EDI For Administration, Commerce, and Transport) family of standards are the two most widely used.

EDI transactions can be divided into two components: form generation and communication. EDI forms are generated by combining standard EDI elements according to standard procedures. The forms have a wide range of applicability. Some apply to wide sectors of the economy (e.g., invoices, price quotations), while others are sector specific and developed by special groups (e.g., insurance forms, transfer of funds).

Commercial EDI software provides the mapping and translation functions for generating EDI forms. Mapping functions convert data from a local representation used by an EDI application to an internal representation of a standard EDI form, and vice versa. Translation functions convert an internal representation of a standard EDI form to an encoded standard EDI form and vice versa.

Once an EDI form is generated and encoded, it must be communicated to a trading partner. EDI standards specify data formats, but are designed independent of communications protocols. Today, EDI users typically communicate over Value Added Networks (VAN). As Open Systems become an integral component of our computer environments, X.400 based electronic mail systems and File Transfer Access and Management (FTAM) systems will be used more and more by EDI users.

2.3 Status of EDI Standardization

There are two prevailing EDI translation standards. The Accredited Standards Committee (ASC) X12 is the standard in North America and UN/EDIFACT is the standard in Europe and most of Asia. The format and the data that can be exchanged for any particular EDI business transaction are defined in the X12 EDI standards and EDIFACT EDI standards.

The EDI standards development process has evolved continuously since the first standards were conceived by X12 in 1979. By 1987 there were only 16 (transaction sets) X12 standards. However, since 1987 tremendous growth in EDI has taken place in standards committee members, users, transaction standards and the complexity of EDI standards. As of the end of 1991, there were 600 committee members, 12 subcommittees, an estimated 20,000 users, 106 approved (transaction sets) standards and 150 new (transaction sets) development projects. The EDIFACT standards are following the path of X12, but the EDIFACT progress is behind X12.

Although X12 is the prevailing standard in North America, EDIFACT is becoming more widely accepted internationally, especially in Europe and in Asia. The Department of Com-

Table 2.1: Sampling of Transaction Sets

Business Function	Example of Transaction Set
Health Care	Health Care and Disability Insurance Claim - used to transmit health care service data from providers, hospitals and physician to payees.
Education	Request for Student Educational Record (Transcript) - used to request a student educational record from an educational institution that the student has attended or is currently attending.
Government Reporting	Economic Census Report - can be used to respond to a request from the U.S. Bureau of Census for economic census data.
Taxes	Electronic Filing of Tax Returns - will allow the sender to file tax returns with federal, state or local taxing authorities.
Warranties	Warranty Registration - can be used for original warranty registration, extended warranties, and service contracts.
Performance Feedback	Automotive Inspection Detail - used by automotive manufacturers, inspection agencies or carriers to report motor vehicle inspection results to other interested parties.
General Transportation	Shipment Information - used to transmit detailed bill of lading, rating, and/or scheduling information pertinent to a shipment.
Ocean Transportation	Reservation (Booking Request) - used by a shipper or forwarder to reserve space, containers and equipment for transport by by ocean vessel.
Motor Transportation	Motor Carrier Shipment Information - used to transmit motor carrier bill of lading information to a motor carrier or third party.
Air Transportation	Air Shipment Information - provides the sender with the capability to transmit detailed bill of lading and rating information pertinent to an air carrier shipment.
Rail Transportation	Train Sheet - allows railroads to exchange train sheet information so that crews operating equipment on other railroads are aware of current operating conditions.
Warehousing	Warehouse Shipping Order - used by a depositor to advise a warehouse to make a shipment.
Product Development	Specifications/Technical Information - complete or partial specifications, or technical information related to products and services.
Project Management	Contract Proposal - can be used to provide cost and pricing data related to a contract proposal in response to a request for proposal.

merce has published Federal Information Processing Standard (FIPS) 161 on EDI [26]. This FIPS states that federal agencies that are implementing EDI shall use ANSI X12 and/or UN EDIFACT in the cases where these standards provide EDI form definitions that meet the agencies EDI requirements.

Very recently, the X12 committee voted (as a whole) to adopt the EDIFACT syntax by 1997. Thus, the original X12 syntax will be phased out for many, or most, or possibly all applications. Exactly how this will occur is not known now, since implementation plans have not yet been put into place. (FIPS 161 is currently being revised to reflect this situation.)

X.435 [27] is the only existing International Standard for communicating EDI transactions. X.435 defines and standardizes an EDI message which can be communicated over X.400 [28] based electronic mail systems.

2.4 Setting Up for EDI

Because EDI is becoming a requirement for conducting business in many areas, more and more businesses are integrating EDI into their systems. The integration of EDI into an existing computing and communications environment is not trivial; there are a number of issues that should be considered before attempting to do so. Among these are the computing environment, i.e., the computer hardware and operating system; the communications environment, including the protocols used and the method of accessing the network such as direct connection or use of a public data or value added network; the data management environment; and the organization's security requirements.

Incorporating EDI into an existing environment is further complicated by the lack of a common Application Program Interface (API[3]) for EDI applications. Each EDI application uses proprietary access methods for invoking communications services. As a result, trading partners must make bilateral agreements for two EDI trading partners to transfer data. Existing EDI applications have also been slow to take advantage of advances in computer networking. Standard means of networking are still mostly low-speed, asynchronous connections, or point-to-point connections using proprietary or older protocols.

Potential EDI users will also, almost certainly, have to establish trading partner agreements before they conduct business transactions using EDI. Trading partner agreements typically include information such as the type of security to be used in the transmission of the transaction (e.g., authentication, integrity, and confidentiality), the means of communicating the transaction between the trading partners (e.g., X.400, FTAM [14], VAN, direct modem-to-modem communications), and the forms that can be transmitted. In the future, database services—in conjunction perhaps with the X.500 Directory [9] [10] (see Chapter 5)—may allow some aspects of this process to be automated.

[3]APIs are developed by the Technical Committees of the Institute of Electrical and Electronics Engineers (IEEE).

2.5 Conducting a Typical EDI Transaction

Having examined some of the requirements for establishing an EDI capability, this section looks at the sequence of events involved in a typical EDI transaction.

There are two primary functions that EDI software must provide, translation and transmission. Translation software is necessary to map between local representations of EDI data forms and standardized representations. EDI does not define a means of transmission to be used for transferring data forms, but one of two communications mechanisms will commonly be used for this purpose. These are electronic mail and file transfer. Electronic mail uses the store and forward paradigm to send an EDI form from an the originator to the recipient's mail box. The transaction is saved in the recipient's mail box until the recipient is ready to retrieve it. File transfer allows a user to directly transfer a form from the originator's to the recipient's file system.

When the EDI form is received by the trading partner's computer system the translation process is reversed. The form is received in a standardized format and is then converted to the system's local representation. Once converted, the form can be saved in the user's local database system.

It should be noted that EDI transactions may require human intervention or may be effected automatically. To automatically effect a transaction, EDI software must be integrated with software, such as a local database management system, that allows events to be triggered under the appropriate set of conditions. This enables, for example, an EDI transaction to be effected when inventory levels fall below a certain predefined level. Of course, support for automatic transactions requires greater effort, but, correspondingly, it also results in greater benefits.

Chapter 3

A Sampling of Electronic Commerce Applications

This chapter continues with the practical assessment of electronic commerce begun in the previous chapter. Here the assessment is broadened by looking at a variety of electronic commerce applications. Before looking at these applications, the issue of data representation is discussed and some of the standards used for this purpose are introduced. The applications themselves are then described, followed by an evaluation of the benefits that have accrued as a result of their use.

3.1 Data Representation

The basic components for supporting electronic commerce are shown in figure 3.1. Each of the applications presented in this section share in their common adherence to this model.

For applications adhering to this model to exchange information, a commonly agreed upon representation for the information they exchange is necessary. Although data representation is a fundamental component of communications protocols, there are also a number of standards designed specifically to establish a common data representation for information exchanged between applications. EDI, discussed in the previous chapter, is one example

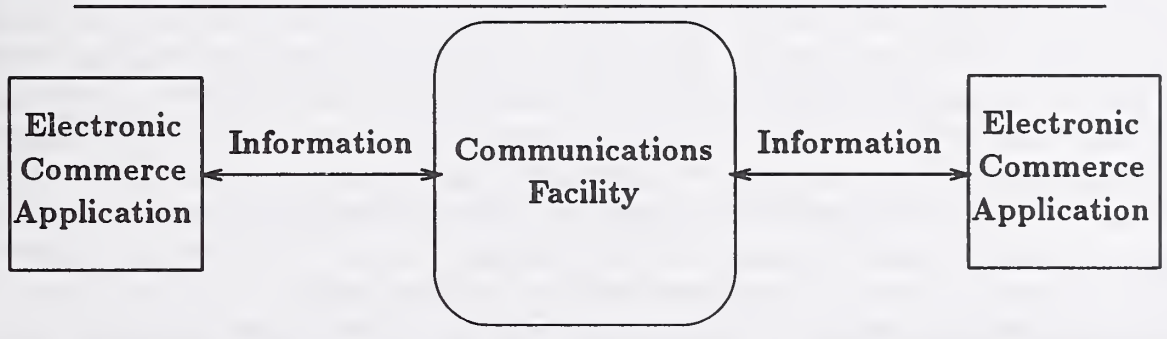


Figure 3.1: Basic Components of Electronic Commerce.

of such a standard. Other examples are provided below. Each can be used by more than one application. For example, EDI may be used by procurement, banking, or health care applications. Only a few of the standards are presented below, designed to highlight some of the various areas where such standards are used.

IGES (Initial Graphic Exchange Specification) (see [25]) is a standard that can be used for exchanging CAD/CAM data. IGES defines representations that allow users to exchange technical drawings, geometric figures, documentation, and other product design and manufacturing data.

ODA (Open Document Architecture) [24] defines an architecture that allows users to exchange the logical structure, content, and layout style of office documents.

STEP (Standard for the Exchange of Product Data) provides data representations for the exchange of product data. This includes all aspects of product data that may be collected throughout the product's life cycle. STEP is a draft standard that at its current stage of development primarily addresses the exchange of material and shape data.

3.2 Description of Electronic Commerce Applications

Electronic commerce is a relatively new technology based on the use of computing and communications services to transfer digital information between remote sites. The type of information that can be transferred with electronic commerce is not restricted. But in general, electronic commerce is used to transfer information that has traditionally been transferred by paper, voice, or analog electronics (e.g., telephone). This section describes many of the capabilities that electronic commerce currently provides, as well as some that will be provided in the future. For electronic commerce to reach its potential, these capabilities must be widely available to all potential users.

There are a number of services that electronically provide users with information. The types of information include: world, national, and local news, sports and weather; entertainment news including movie and television reviews; financial information including stock and bond prices, interest rates, and foreign exchange rates; and books, encyclopedias, and journals, such as may be found in a public library.

Personal shopping services electronically transfer descriptions of items from a retailer to a shopper, and purchase orders from the shopper to the retailer. A shopper may search through an electronic retail catalog to obtain a description and price of products. If the shopper wishes to order an item in the catalog, the order is electronically placed. Other examples of the personal shopping model are: home finance (the shopper buys and sells stocks and bonds electronically), and home entertainment and reservations (the shopper selects, reserves, and pays for sports, theatre, opera, and concert events as well as airline, hotel, and car rental reservations for a vacation.) Home banking is a variation of the home shopping model. In home banking, the user, through the use of a touch-tone telephone keypad, requests the electronic payment of bills by his or her bank.

Online information services, electronic mail vendors, and most networked computer systems provide services to transfer unstructured information. In an unstructured electronic exchange of information, thoughts and ideas can be exchanged between two or more individuals. Users can exchange messages electronically (referred to as electronic mail), post

electronic messages for public viewing (referred to as bulletin boards), carry on conversations between two or more individuals, on a terminal (referred to as talk, chat, or cb mode of communications), have one or more speakers present views and answer questions from a remote audience (referred to as talk, chat, or cb conferences or seminars).

Most digital information transferred electronically today is ASCII text. Many other types of data, such as drawings, images, video, and voice are starting to be transferred. For example, a patient's medical records may include a combination of a text description of the patient's history, and images, such as x-rays and photographs. Product data, such as an autopart description may require a text description as well as a drawing of the part.

Complex data structures built upon the basic forms of data will be transferred by electronic commerce applications. For example, the electronic distribution of software requires the transfer of unstructured text and related information, along with the software files. The printed matter may include instructions (with drawings or images), and registration materials. The software files may include binary program executable files, and binary or text data files. The electronic transfer of newspapers and magazines, which are composed of a set of text articles and images, is another electronic commerce application requiring the transfer of complex information.

Electronic commerce may be used to transfer educational information, such as a doctors presentation on how to perform a complex surgical procedure. This information may contain a text summary, and a video demonstration of the procedure including narration. This information could be useful to doctors located in geographically remote locations, lacking the facilities available in large cities.

The interactive electronic transfer of complex information may allow a student to take a course, visit a museum or library, or perform a chemistry experiment through his or her computer. This electronic commerce application can make the vast information resources of this country available to people all over the world.

The electronic transfer of information facilitates the integration and automation of business functions that are typically carried out separately. Examples of this can be found in the retail industry today. A retail store's computer may maintain a database of the store's inventory. Bar Code technology can allow the database to be automatically updated when items are sold, as well as when new items are received. In this environment, when the inventory of an item falls below a certain predetermined level, a purchase order can be automatically generated and transferred to the supplier. When the product arrives and the database is updated, an electronic form can be generated and sent to the retailer's bank requesting electronic payment to the supplier's bank account. In addition to the benefits of improved efficiency and accuracy resulting from this automation, the automation also makes it easier to gather marketing information that can be used to influence the type and level of inventory maintained.

Another potential application of electronic commerce is cooperative development. That is, individuals at disparate locations may be able to jointly develop software implementations, documents, diagrams, and other applications. Increased computing power and network bandwidth may allow the developers to carry out the necessary activities of accessing and manipulating information, unencumbered by the distances separating them.

3.3 Benefits of Electronic Commerce

Electronic commerce has many benefits over traditional commerce[4]. Electronic commerce automates the interchange of all information needed to conduct business. Automated business transactions have two primary benefits: speed and accuracy. The time interval required to create, transfer, and process a business transaction between trading partners is significantly reduced using electronic commerce. Furthermore, human errors and problems associated with traditional commerce are largely eliminated with electronic commerce. As suggested by the examples presented above, these improvements in efficiency and accuracy can result in significant cost savings to both government and industry. Retail stores can operate more efficiently, medical costs can be reduced using electronic billing, insurance providers can reduce costs by using electronic filing and standard cost codes, and other sectors of the economy can also benefit by employing electronic commerce in their business activities.

One application designed to exploit the time efficiencies of automation is called Just-In-Time (JIT) manufacturing. The goal of JIT manufacturing is to minimize inventory levels. The manufacturer, by automating inventory maintenance procedures, keeps inventory levels much closer to the exact level necessary for production. This allows a reduction in inventory investment, and also reduces the requirement for storage space.

Beyond the cost and time savings offered by electronic commerce, there are other benefits, both tangible and intangible, that will result from its deployment. Databases may hold information that could not have been accessed in a timely manner in the past—perhaps information needed to carry out medical diagnosis or procedures. They may also provide a wealth of information that simply could not have been accessed in any practical way in the past. Providing access to such information may allow scientist and researchers to solve problems in a much more timely fashion; furthermore, collaboration, that previously would not have been possible, can enhance the likelihood of solving complex problems. And certainly access to new information and facilities, the ability to interact and to collaborate between individuals across large distances, and the ability to carry out public business and private affairs will produce results, the consequences of which are very difficult to foresee.

[4]See, for example, [11].

Chapter 4

The Electronic Commerce Model

Electronic commerce was defined in Chapter 1 of this document. In Chapter 3 a number of examples of its use were presented. In this section, a more concrete view of electronic commerce is formulated by presenting an architectural model for electronic commerce which will serve as the basis for the material to be presented in the remaining sections of this paper. Here we describe the model and introduce each of its components; in the subsequent sections we elaborate more fully on these components.

4.1 An Architectural Model for Electronic Commerce

Commerce, whether conducted through traditional means or electronically, relies on the conveyance of information. In traditional commerce, the information may be conveyed by the purchaser going in person to a store, it may be conveyed by the purchaser using the telephone system, or it may be conveyed by the purchaser using the postal system to purchase an item. For a more complicated purchase, the purchaser may type a purchase order and send it through the postal system, or deliver the order in person. Commerce activities need not be restricted to business activities either, in some cases the conveyance of information is itself the end objective; mail exchanges, electronic or through the postal system, are typical examples of this type of activity. In each of these activities information, properly conveyed, is crucial for the success of the transaction.

Properly conveyed information is also crucial for the success of electronic commerce transactions, but the means of conveyance differs from that used in traditional commerce. In electronic commerce, a communications network is typically employed for conveying information. Electronic commerce also differs from traditional commerce in the means used for processing information. Whereas, traditionally human intervention has been required to process and act on information accompanying a business transaction, in electronic commerce, human intervention is minimized. This is achieved by automating procedures, and eliminating the use of paper, wherever possible.

The characteristics, then, of electronic commerce that distinguish it from traditional commerce are the means used for conveying information and the methods used for processing it. To effect changes in the way information is conveyed and processed, two support services are clearly needed: communications and data management. In addition, for realistic use of

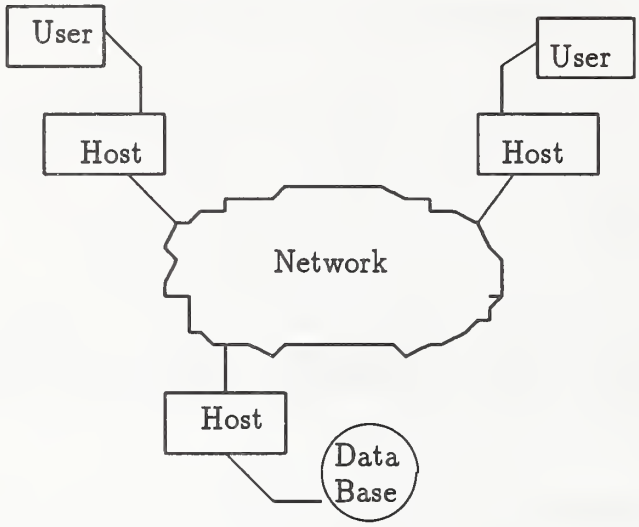


Figure 4.1: A Simple Network Configuration.

electronic commerce applications in an operational setting, security is also essential.

To enable a clearer understanding of this environment, before presenting the model, it may be useful to have a brief look at a communications network.

Figure 4.1 depicts a simple network configuration. For our purposes this simple configuration will be suitable. The important aspect of the network is that it provides a link between users—and between users and information—which allows information to be transported from one location in the network to another location in the network. The network depicted in figure 4.1 shows host systems that provide user services and support user access to the network, and host systems that provide automated access to information repositories. In this environment users can electronically convey information to each other, and local applications can use information available anywhere in the network to support the services they offer. To exchange information, users may send mail electronically, rather than use the telephone or postal system. To send a purchase order, an electronic form may be used.

As noted above, the architectural model for electronic commerce must include communications, data management, and security. Of course, the application must also be part of the model. Figure 4.2, then, depicts an architectural model for electronic commerce comprised of five major components: a user interface, an application, communications, data management, and security. Notably, the model includes a user interface element which has seemingly not been included in any of the above discussion. This is because the user interface and the application are typically coupled so tightly that they often exist as a single entity which cannot be separated. Nevertheless, separation of these components is useful for discussing functionally. Each component will be discussed briefly below and elaborated upon in later sections.

Before discussing these components, it is worth noting their relationship with electronic commerce. The major task in effecting electronic commerce is not in enhancing or developing new technologies, rather it is in integrating existing technologies. That is, the focus of

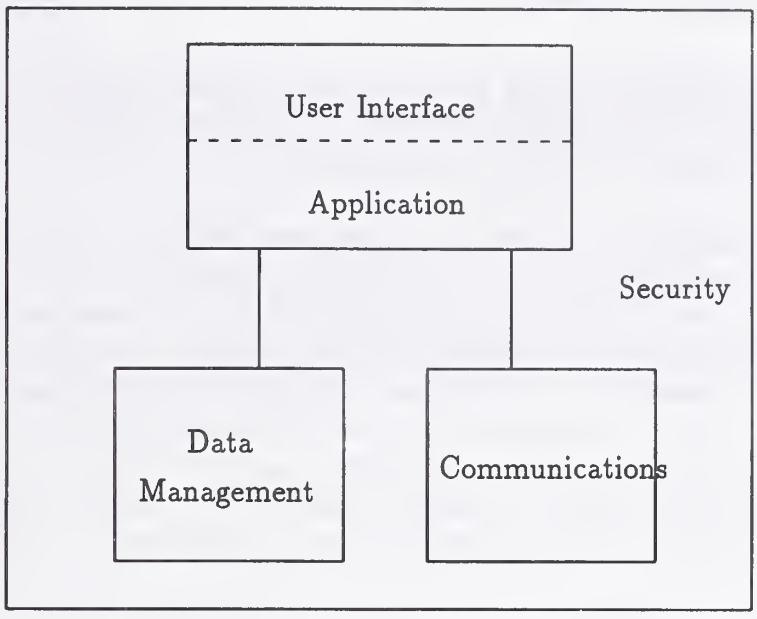


Figure 4.2: Electronic Commerce Architectural Model.

electronic commerce is on incorporating the support services into a cohesive environment that provides a framework for supporting electronic commerce applications. Of course, an examination of each of these areas is necessary to accomplish this.

A few additional comments are warranted before discussing the model's components. Neither operating systems nor hardware have been included in the model. This is certainly not due to their lack of importance. As has already been mentioned in the introductory chapter of this document, advances in hardware technology are a major facilitating factor in promoting electronic commerce; operating systems that take advantage of these advances and provide users and applications with the corresponding benefits, are equally important. They are left out of our model primarily because they are taken for granted—i.e., their presence is implicitly clear—and because they do not present any major issues that directly bear on the development of an infrastructure for electronic commerce.

4.2 Applications

The breadth of electronic commerce applications spans a wide range and will be further broadened as electronic commerce matures. The scope of these applications was hinted at in Chapter 1 of this paper, and a number of examples were examined in Chapter 3. The focus for the remainder of this paper will be away from the applications, and will instead center on the components most electronic commerce applications will require.

4.3 The User Interface

The user interface will provide most users with their only working view of electronic commerce. The flexibility and convenience with which this is accomplished, therefore, will be a major factor in determining the overall success of electronic commerce and the rate at which it develops.

The purpose of the user interface is to provide users with a comfortable and convenient means for accessing application services. The preponderant form of most new interfaces is one that places users in a windowing environment. Windowing interfaces generally accept input from a mouse and minimize the number of key strokes users must enter. Additionally, use of such interfaces is fostered by the limited amount of instruction required for their effective utilization. Other interactive interfaces that place fewer requirements on system resources are also possible; the advantages they offer however are continually being diminished by the decreased cost of computing power. Non-interactive interfaces are also possible, a significant disadvantage of these is that they generally require a greater level of technical expertise.

4.4 Data Communications

Data communications is an area that is undergoing rapid change. The most significant factor accounting for this change has been the increased bandwidth and reliability of the physical network. This change has not only spawned new ideas for applications but has also resulted in a re-examination of some of the underlying communications protocols, rested on assumptions about the network that are no longer valid.

There are two key components to data communications that make computer-to-computer data exchanges possible: protocols and a network architecture. Protocols establish the rules that govern data exchanges and a network architecture provides the structural framework for defining protocol requirements and understanding the physical network. As suggested above, protocols based on open standards are necessary for electronic commerce to achieve wide-spread deployment. There are two widely touted sets of protocols that fall into this category: TCP/IP (Transmission Control Protocol/Internet Protocol) and OSI (Open Systems Interconnection), the former the work of the Defense Department's ARPANET, the latter the work of the International Standards Organization (ISO). There are other protocol suites, such as ISDN (Integrated Services Data Network), designed to utilize the high bandwidth and improved reliability of newer network technologies.

4.5 Data Management

The function of the data management component of the electronic commerce model is to support the storage, retrieval, and manipulation of data. The mechanism used to effect this function is a database management system (DBMS). The most commonly selected system for general purpose usage is a relational DBMS. Other, newer and more sophisticated systems that store and manipulate more complex data types called objects are gaining in popularity; the management of objects is also being incorporated into the relational model.

4.6 Security

Security plays a crucial role for realistic operations and is pervasive throughout the electronic commerce model. Each component of the model will require its own security measures. The application may not be available to a user without the user going through a login procedure. The data management module may deny data access to users without proper credentials. And the communications module may employ cryptographic procedures to ensure the integrity or confidentiality of the data it transports. Additionally, different levels of security may be needed to reflect the sensitivity of data and the consequences of its disclosure or tampering by unauthorized users. Finally, a clear administrative policy consistent with company objectives is necessary for effective security.

Chapter 5

Communications

Central to electronic commerce is communications, at the heart of communications are protocols. Protocols define a set of procedures that allow systems at disparate sites to exchange data and apply a consistent interpretation to the data they exchange. The two sets of protocols that have received the most attention in recent years have been TCP/IP (the suite of Internet protocols developed by the Department of Defense), and OSI (Open Systems Interconnection, developed by International Standards Organization); each set will be discussed in this chapter. In addition to these protocol suites, newer protocols, such as ISDN and B-ISDN[5] that take into account recent advances in network technology, will also be discussed.

5.1 Network Architectures

Both the TCP/IP and OSI protocol suites are designed to provide communications between heterogeneous systems. Providing communications between heterogeneous systems presents a complex problem, recognizing this, both protocol designers developed a structured solution to the problem. For comparing the two solutions, the architectural model employed by TCP/IP can be viewed as a four layered vertical stack, while the OSI model consists of seven layers arranged in a vertical stack. There is a significant overlap in the functionality both suites provide, but a different approach to providing it. Generally, TCP/IP has followed a pragmatic approach, while OSI has followed a more abstract approach, attempting to define functionality satisfying a broad set of requirements. The more focused approach of TCP/IP has allowed for quicker development of implementations resulting in widespread deployment of TCP/IP protocols, the acceptance of OSI has been slower in coming; some believe it is too encumbered with unnecessary functionality to serve as a practical replacement for TCP/IP.

Regardless of the merits of either approach, both provide a set of open standards for basing the development of implementations on; this feature is essential for achieving widespread interoperability between applications running in an heterogeneous environment. Protocol— or communications— applications supported by both platforms include file transfer, electronic mail, and virtual terminal protocols. The OSI protocols for accomplishing these tasks

[5] See, for example, [20].

are File Transfer Access and Management (FTAM), X.400, and Virtual Terminal (VT) [12], respectively, the TCP/IP variants are the File Transfer Protocol (FTP) [13], the Simple Mail Transfer Protocol (SMTP) [15], and the Telnet protocol. OSI also supports a distributed database service, X.500, that provides a facility for storing relatively static network and user information in a distributed environment.

Communications standards do not define an interface to describe the way in which communications services are to be provided. Thus, applications must account for the different methods employed by different implementations in providing the same set of services. This implementation dependency results in the development of applications that are not portable. To deal with this problem, IEEE has sponsored the development of standards to define application program interfaces (APIs). APIs allow software developers to build applications based on the use of a commonly defined interface, thereby removing implementation dependencies and allowing for the development of more portable applications.

To support communications applications, an underlying communications structure is required to provide reliable end-to-end delivery of data. This is provided by the bottom four layers of the OSI stack, and the bottom three of the TCP/IP stack. Interoperability between applications running on different stacks is difficult, but even within the same stack there are a number of network platforms which frustrate interoperability. For example, OSI defines five different transport protocols, each designed to operate over a different set of underlying network protocols. Interoperation between applications using different architectural models such as OSI and TCP/IP cannot be accomplished without building special software, or gateways, to translate between protocols. Gateways can be used to link together heterogeneous subnetworks. A large scale network is not comprised of a single network linking together all end systems. Instead, there are typically a number of subnetworks that must be linked together using either gateways or bridges, which link homogeneous subnetworks. Subnetworks can range in size from local area networks (LANs) that may link together a single organization's work stations, to wide area networks (WANs) that may link sites separated by hundreds of miles.

Although the development of gateways comes outside the purview of the standards process and typically results in some loss of functionality, it does provide interoperability between applications and thereby contributes to the development of a more integrated network. Recently, efforts to address problems with networking in the TCP/IP environment have resulted in proposals such as TCP and UDP with Bigger Addresses (TUBA) [19] which would create a network structure capable of supporting both TCP/IP and OSI applications. Better transparency could also be obtained by integrating communications applications. For example, the X.500 Directory can be utilized to provide X.400 (electronic mail) with a name to address mapping. Users can directly query the Directory to provide the mapping, but greater transparency is achieved if X.400 queries the Directory without requiring any intervention on the part of the user.

A more integrated network capable of providing transparent communications services will be necessary for achieving the full potential of electronic commerce; the level of transparency will need to go well beyond what is currently supported. For comparison purposes it is instructive to consider the present telephone network. The telephone network is ubiquitous and distributed widely enough for availability generally to be taken for granted. Although

the deployment of electronic commerce applications and infrastructure is growing, it does not approach this the level of availability. For electronic commerce applications to reach this level a network as dispersed as the telephone network's with equally ubiquitous resources for running electronic commerce applications will be necessary.

5.2 Network Management

As indicated above, a network is generally a complex entity made up of subnetworks which may exhibit different physical characteristics and support different protocol stacks. Multiple protocols, bridges between subnetworks, and gateways may also be part of the network. Clearly, such a diverse structure necessitates a management strategy to ensure a smoothly functioning network and reliable delivery of data under a variety of conditions. To this end both the OSI and TCP/IP stacks have defined network management protocols. The OSI management protocol is the Common Management Information Protocol (CMIP) [16], the TCP/IP counterpart is the Simple Network Management Protocol (SNMP) [18].

CMIP identifies five areas requiring network management. These are network configuration, fault isolation, performance evaluation, network security, and network accounting. A generic set of functions are defined for supporting management in each of these areas. Their functionality is realized through the use of the Common Management Information Services (CMIS). CMIS utilizes the CMIP protocol to acquire remote data needed for providing this functionality. CMIP allows for the definition of a wide range of object types that can be managed, and a relatively sophisticated set of functionality for their acquisition and manipulation. Although SNMP identifies areas similar to CMIP requiring network management, the functionality it provides is somewhat simpler and the types of objects that can be defined more restrictive. This is in keeping with the more pragmatic view generally adopted by TCP/IP which allows for easier development of implementations. As might be expected, to date, SNMP has been more widely implemented than has been CMIP.

5.3 ISDN

The network architectures discussed above were designed to provide data services using physical networks that were not always reliable and offered limited bandwidth. Integrated Services Digital Network (ISDN) [20] was designed to provide both voice and a wide variety of data services, initially using the existing phone network. Broadband ISDN (B-ISDN) was designed to provide a more sophisticated set of services using reliable high speed networks that can be provided using optical fiber physical networks.

ISDN supports a transmission structure made up of multiple data channels and a separate signaling channel. This gives ISDN the flexibility to provide dedicated connections for applications requiring them (circuit switching), while also being able to support dynamic allocation of network resources for applications that require this network model (packet switching). Additionally, channels can be grouped in different combinations to provide differing network capacities based on user and application requirements. For example, a home user of ISDN may require only a relatively low data capacity to support phone and computer

services. A business may require a higher data capacity to support a local PBX or computer network, along with FAX and telephone services.

B-ISDN will require a high capacity network for providing a wide range of new services. These will include integrated video and phone services, videoconferencing, and it will also allow for high speed transfers of images, files, and integrated documents containing both text and graphics. Electronic mail services in which video, voice, and data are integrated will be supported. Also supported will be applications in which users interact with the application in real time.

Chapter 6

Data Management

As noted earlier, the function of the data management component of the electronic commerce model is to support the storage, retrieval, and manipulation of data. This function is most commonly handled using a database management system, usually an SQL relational system; newer systems that incorporate the object oriented paradigm for managing data are becoming more common.

6.1 Database Management Systems

Moving information through the network lies at the core of electronic commerce. Not only does information need to be moved between users but also between users and information repositories. Managing large amounts of data, such as might be held in an information repository, will generally require employing a DBMS. A DBMS may also be employed by users for managing local data. The preponderant choice for DBMSs today is an SQL based relational system. Relational DBMSs store data as column values in the rows of a table. A stored value must adhere to the type defined for the column in which it is stored, and each row is an instance of a relationship implicitly defined by the table in which it appears. The relational model provides a particularly simple and elegant model for managing data, rested on a solid underlying mathematical foundation. Using a DBMS data can be stored, retrieved, modified, or removed—SQL provides a language for effecting any of these capabilities. The SQL language has been the defacto standard for accessing relational DBMSs and is also now an ANSI and ISO standard [21].

Although SQL provides for standardized access to a local database, it does not provide a means for remote database access. To address this problem, ISO is proceeding with the development of a Remote Database Access (RDA) protocol [22]. RDA is based on a client/server architecture and will provide users with standardized procedures for issuing remote SQL requests. It should be noted that this does not provide support for a distributed database service. RDA defines a two-way service, not a means for accessing data distributed across multiple sites. Some early work is underway to address this problem, but developing a distributed relational database systems is a difficult problem. X.500, an OSI application layer protocol, is a distributed hierarchical database that, while providing effective database support in a distributed environment for some applications, lacks some important features

generally found in relational systems and thus is not suitable for certain applications.

While relational DBMSs provide a powerful mechanism for data management, they are not entirely satisfactory for managing some types of data. In particular, the only data types that are directly supported by the relational model are simple data types such as character strings and integers. Structured data cannot be directly stored in database columns and must first be broken into component parts and mapped onto the appropriate columns before storing. Object oriented databases support the manipulation of objects which can be complex data structures, thereby providing a more natural representation for storing structured data. The ability to manipulate complex data will certainly become more important as more applications offer services that require integrating text, image, binary, and voice data. Recognizing the importance of object oriented databases, work is underway to develop an extended version of SQL called SQL3 that will include the capability to manipulate data objects.

Chapter 7

Security

The major components of the electronic commerce architectural model introduced in Chapter 4 are applications and user interfaces, communications, data management, and security. This chapter examines the last of these, security. As noted previously security plays a crucial role in an operational environment for the success of electronic commerce.

7.1 Security in a Distributed Environment

When conducting commerce in a distributed environment, some level of integration between commercial systems— which may have nothing more in common than what results from the decision to engage in commerce electronically— will be necessary. This integration may result in security risks if the integrated systems are not properly insulated. In this environment there are two factors that must be taken into account in providing security that are not present in an isolated environment: outside users must be given access to local systems and data, and local users must entrust sensitive data to remote systems over which they have no control. Dealing with the first of these problems—in addition to requiring security administrators to extend local procedures to outside users over whom they may have little control—also requires administrators to guard against threats to system and data integrity from the outside. Dealing with the second problem, requires employing new procedures that are generally not part of local security measures.

Effective security can only be achieved within the context of an overall security policy. There are five security services that must be provided for achieving effective security: authentication, access control, data integrity, data confidentiality, and nonrepudiation.

Physical security aside, the first step in maintaining system and data security involves providing users with credentials that must be authenticated before allowing access to the system. For local users this involves, typically, providing a name and password. The same procedure is applicable to both local and remote users, although one may have little assurance about the sensitivity with which remote users treat their access credentials. Furthermore, restricted access may be granted to a whole community of users. This, however, can easily open system access to nearly everyone, and thus, render system security vulnerable; if a user with malicious intent is able to gain restricted access to the system, subverting the intended restrictions may be possible.

Even authorized users are not generally granted access to all data or system resources. Limiting access to selective users requires employing access control procedures. Effective access control procedures often rely on effective authentication procedures. Applying access control procedures in a distributed environment is a difficult problem; in addition to the considerations that must be accounted for in an isolated environment, the impact of dealing with other systems must be considered. A user's credentials may pass through several systems before arriving at the intended destination. Typically, security must be assured while assuming the intervening systems are untrustworthy.

For dealing with the problems of authenticating users in a distributed environment, additional procedures must be employed. As noted above, a simple name and password may be used for authenticating remote users. But using only these offers a very minimal level of protection against unauthorized system access.

Better protection against unauthorized system access can be provided using cryptographic procedures. Cryptography can also be used for ensuring data integrity, guarding against unwanted disclosure of information, and supporting nonrepudiation.

Cryptographic procedures are based on the use of data encryption algorithms that can be used to convert plain text into ciphered text. The result of applying an encryption algorithm to text is dependent upon an algorithm parameter called a key. Two possible approaches can be used when employing cryptographic procedures. One approach is symmetric, using the same secret key for both enciphering and deciphering text. With this approach the secret key must be shared among users. Integrity can be provided by computing a cryptographic checksum called a Message Authentication Code (MAC); this can be accomplished using the Data Encryption Standard (DES) [29]. If the secret key is only shared between the sender and the receiver, the receiver can use the MAC to verify the identity of the sender. This cannot inherently be used to provide nonrepudiation, i.e., it cannot be used for providing an impartial third party with convincing evidence that the sender was the party claimed by the receiver.

A second approach to cryptography is called public key cryptography. With this approach keys are generated in pairs. One key is secret known only to a single user, the second key is public and openly available. The Digital Signature Standard (DSS) [30], proposed by NIST, defines an algorithm for generating and verifying digital signatures. To generate a signature on a message, the owner of the secret key first applies an algorithm that produces a condensed representation of the message. The secret key is then applied to the condensed message to produce a digital signature. Using the corresponding public key, a recipient of the message can verify the integrity of the message (i.e., that the original content of the message has not been altered) and the validity of the signature. Additionally, public key cryptography supports nonrepudiation: the recipient can provide the message, digital signature, and signer's public key as evidence to a third party that the message was signed by the claimed signer. Given the evidence, the third party can also verify the signature.

The Digital Signature Standard does not provide confidentiality. Confidentiality can, however, be achieved by the signer first applying DES to the message and then signing it using the Digital Signature Algorithm (DSA) specified by the DSS.

Chapter 8

Conclusions

Having presented an overview of electronic commerce and having examined some of the key issues involved in its deployment, this chapter draws some conclusions about electronic commerce.

8.1 Conclusions

There can be little doubt that the trend in conducting business activities will be to move more and more away from the use of paper and towards the use of electronic media. Many procedures that in the past have required human attention and effort will be automated resulting in increased efficiency, fewer errors, and correspondent cost savings.

It is clear, as demonstrated in the introductory chapter of this document, that the computing power and network bandwidth needed to make the automation of many commercial and private activities a viable choice is forthcoming. Presently, the capacity to selectively automate commercial activities is being pursued. This is already being done in some cases with EDI, but can be pursued on a broader scale.

The examination of electronic commerce presented in this paper, concludes that communications, data management, and security modules are essential for establishing an electronic commerce infrastructure. This assessment appears to be sound, but it requires further evidence to substantiate. Efforts are now underway both within NIST and throughout the federal government[6] that will significantly expand the use of electronic commerce. These efforts will provide evidence for substantiating (or challenging) claims that significant benefits can be derived from deploying electronic commerce.

[6]There is an effort underway to deploy electronic commerce for procurement activities throughout the government resulting from a Presidential Memorandum of October 1993.

Bibliography

[1] Zorpette, Glenn. *Large Computers. Spectrum—January 1993.* The Institute of Electrical and Electronic Engineers, New York, NY, 1993.

[2] Zorpette, Glenn; Comerford, Richard; and Cybenko, George and Kuck, David J. *Reinventing the Machine. Spectrum—September 1992.* The Institute of Electrical and Electronic Engineers, New York, NY, 1992.

[3] Vetter, Ronald J. and Du, David H.C. *Distributed Computing with High-Speed Optical Networks. Computer—February 1993.* IEEE Computer Society, Los Alamitos, CA, 1993.

[4] A Report by the Committee on Physical, Mathematical, and Engineering Sciences. *Grand Challenges 1993: High Performance Computing and Communications* Federal Coordinating Council for Science, Engineering, and Technology; Office of Science and Technology Policy. Wasington, D.C. 1993.

[5] Information Infrastructure Task Force. *The National Information Infrastructure: Agenda for Action.* September 1993.

[6] The American National Standards Institute (ANSI). *Accredited Standards Committee (ASC) X12 Electronic Data Interchange (EDI).* Version 3. Data Interchange Standards Association (DISA); Alexandria, VA. 1993.

[7] United Nations Economic Commision for Europe (UN/ECE). *United Nations rules for Electronic Data Interchange for Administration, Commerce, and Transport (UN/EDIFACT).* Pan American EDIFACT Board at DISA; Alexandria, VA. 1993.

[8] *U.S. Government Open Systems Interconnection Profile (GOSIP).* U.S. Federal Information Processing Standard (FIPS) 146. 1990.

[9] The International Telegraph and Telephone Consultative Committee: *The Directory.* CCITT Recommendation X.500. 1993.

[10] International Organization for Standardization and International Electrotechnical Committee *Information Processing Systems – Open Systems Interconnection – The Directory.* ISO 9594. 1993.

[11] Data Interchange Standards Association (DISA). *DISA Publications Catalog, Incorporating Introduction to EDI.* Alexandria, VA. 1993.

[12] International Organization for Standardization and International Electrotechnical Committee. *Information Processing Systems – Open Systems Interconnection – Virtual Terminal Service.* ISO 9040. 1990.

[13] Postel, J.; Reynolds, J. *File Transfer Protocol (FTP).* Request for Comments 959, DDN Network Information Center, SRI International. 1985.

[14] International Organization for Standardization and International Electrotechnical Committee. *Information Processing Systems – Open Systems Interconnection – File Transfer, Access, and Management.* ISO 8571. 1988.

[15] Postel, J. *Simple Mail Transfer Protocol (SMTP).* Request for Comments 821, DDN Network Information Center, SRI International. 1982.

[16] International Organization for Standardization and International Electrotechnical Committee. *Information Processing Systems – Open Systems Interconnection – Common Management Information Protocol Specification (CMIP).* ISO 9596. 1991.

[17] 1098 Case, J.; Fedor, M.; Schoffstall, M.; Davin, C. *A Simple Network Management Protocol (SNMP).* Request for Comments 1098, DDN Network Information Center, SRI International. 1989.

[18] 1098 Case, J.; Fedor, M.; Schoffstall, M.; Davin, C. *A Simple Network Management Protocol (SNMP).* Request for Comments 1098, DDN Network Information Center, SRI International. 1989.

[19] 1347 Callon, R. *TCP and UDP with Bigger Addresses (TUBA), A Simple Proposal for Internet Addressing and Routing.* Request for Comments 1347, DDN Network Information Center, SRI International. 1992.

[20] Stallings, William. *ISDN, An Introduction.* MacMillan Publishing Company, New York, NY. 1989.

[21] *Database Language SQL.* U.S. Federal Information Processing Standard (FIPS) 127-2. 1993.

[22] International Organization for Standardization and International Electrotechnical Committee. *Information Processing Systems – Open Systems Interconnection – Remote Database Access (RDA).* ISO DIS 9579. 1992.

[23] International Organization for Standardization and International Electrotechnical Committee. *Information Processing Systems – Open Systems Interconnection – Abstract Syntax Notation 1.* ISO 8824. 1992.

[24] International Organization for Standardization and International Electrotechnical Committee. *Information Processing Systems – Open Systems Interconnection – Office Document Architecture and Interchange Format.* ISO 8613. 1989.

[25] *Initial Graphics Exchange Specification (IGES)*. U.S. Federal Information Processing Standard (FIPS) 177. 1989.

[26] *Electronic Data Interchange (EDI)*. U.S. Federal Information Processing Standard (FIPS) 161. 1993

[27] The International Telegraph and Telephone Consultative Committee: *Message Handling System (MHS) Application for Electronic Data Interchange (EDI) Messaging*. CCITT Recommendation X.435. 1990.

[28] The International Telegraph and Telephone Consultative Committee: *Message Oriented Text Interchange System (MOTIS) [Message Handling]*. CCITT Recommendation X.400. 1990.

[29] *Data Encryption Standard (DES)*. U.S. Federal Information Processing Standard (FIPS) 46-2. 1993.

[30] *Digital Signature Standard (DSS)*. Proposed U.S. Federal Information Processing Standard (FIPS).

ANNOUNCEMENT OF NEW PUBLICATIONS ON COMPUTER SYSTEMS TECHNOLOGY

Superintendent of Documents
Government Printing Office
Washington, DC 20402

Dear Sir:

Please add my name to the announcement list of new publications to be issued in the series: National Institute of Standards and Technology Special Publication 500-.

Name _____

Company _____

Address _____

City _____ State _____ Zip Code _____

(Notification key N-503)

NIST Technical Publications

Periodical

Journal of Research of the National Institute of Standards and Technology—Reports NIST research and development in those disciplines of the physical and engineering sciences in which the Institute is active. These include physics, chemistry, engineering, mathematics, and computer sciences. Papers cover a broad range of subjects, with major emphasis on measurement methodology and the basic technology underlying standardization. Also included from time to time are survey articles on topics closely related to the Institute's technical and scientific programs. Issued six times a year.

Nonperiodicals

Monographs—Major contributions to the technical literature on various subjects related to the Institute's scientific and technical activities.

Handbooks—Recommended codes of engineering and industrial practice (including safety codes) developed in cooperation with interested industries, professional organizations, and regulatory bodies.

Special Publications—Include proceedings of conferences sponsored by NIST, NIST annual reports, and other special publications appropriate to this grouping such as wall charts, pocket cards, and bibliographies.

Applied Mathematics Series—Mathematical tables, manuals, and studies of special interest to physicists, engineers, chemists, biologists, mathematicians, computer programmers, and others engaged in scientific and technical work.

National Standard Reference Data Series—Provides quantitative data on the physical and chemical properties of materials, compiled from the world's literature and critically evaluated. Developed under a worldwide program coordinated by NIST under the authority of the National Standard Data Act (Public Law 90-396). NOTE: The Journal of Physical and Chemical Reference Data (JPCRD) is published bimonthly for NIST by the American Chemical Society (ACS) and the American Institute of Physics (AIP). Subscriptions, reprints, and supplements are available from ACS, 1155 Sixteenth St., NW, Washington, DC 20056.

Building Science Series—Disseminates technical information developed at the Institute on building materials, components, systems, and whole structures. The series presents research results, test methods, and performance criteria related to the structural and environmental functions and the durability and safety characteristics of building elements and systems.

Technical Notes—Studies or reports which are complete in themselves but restrictive in their treatment of a subject. Analogous to monographs but not so comprehensive in scope or definitive in treatment of the subject area. Often serve as a vehicle for final reports of work performed at NIST under the sponsorship of other government agencies.

Voluntary Product Standards—Developed under procedures published by the Department of Commerce in Part 10, Title 15, of the Code of Federal Regulations. The standards establish nationally recognized requirements for products, and provide all concerned interests with a basis for common understanding of the characteristics of the products. NIST administers this program in support of the efforts of private-sector standardizing organizations.

Consumer Information Series—Practical information, based on NIST research and experience, covering areas of interest to the consumer. Easily understandable language and illustrations provide useful background knowledge for shopping in today's technological marketplace.

Order the **above** *NIST publications from: Superintendent of Documents, Government Printing Office, Washington, DC 20402.*

Order the **following** *NIST publications—FIPS and NISTIRs—from the National Technical Information Service, Springfield, VA 22161.*

Federal Information Processing Standards Publications (FIPS PUB)—Publications in this series collectively constitute the Federal Information Processing Standards Register. The Register serves as the official source of information in the Federal Government regarding standards issued by NIST pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973) and Part 6 of Title 15 CFR (Code of Federal Regulations).

NIST Interagency Reports (NISTIR)—A special series of interim or final reports on work performed by NIST for outside sponsors (both government and non-government). In general, initial distribution is handled by the sponsor; public distribution is by the National Technical Information Service, Springfield, VA 22161, in paper copy or microfiche form.

U.S. Department of Commerce
National Institute of Standards and Technology
Gaithersburg, MD 20899-0001