INTRODUCTION
The computer revolution has transformed modern life by integrating every aspect of society. It has penetrated the way enterprises communicate, as well as the way they do business. Electronic commerce is contributing to this revolution by changing the way enterprises buy and sell products and services. Today, many enterprises are performing secure and reliable large-scale enterprise transactions over the Internet.

True electronic commerce is becoming a reality by the combination of electronic data interchange (EDI) standards; low-cost, high-speed open networks; and new authentication agent software. So, the emergence of the Internet, coupled with better network security, is resulting in rising expectations for data access, communications, and productivity throughout the enterprise world.

Communication via electronic means such as e-mail is becoming standard. In addition, the developments in Web browser software are bringing organizations a new awareness of the Internet's commercial potential. However, much of the potential has yet to be realized.

In using the Internet as a marketing medium, organizations must not only change their internal processes, but invent new electronic commerce procedures. For example, it is difficult to exchange merchandise for
money when neither the supplier nor the customer can confirm the other’s identity.

Many enterprises are reluctant to establish a World Wide Web presence for a variety of reasons, including the bad press attached to early failings in Internet security. Many organizations also perceive that the Internet is unreliable, noting the lack of a central management structure, coupled with the Internet’s rapid growth. In addition, many internal information technology (IT) managers still know little about the Internet.

Among organizations’ other concerns in establishing a Web presence are the vulnerability of electronic mail transactions to hackers, and the possibility of computer viruses coming in over the network. Enterprises also hesitate to offer their services over the Web because of unprofessional behavior on the part of their own employees, as well as the fear that external access could expose vulnerabilities in their own internal networks and systems.

For these and other reasons, online purchases currently account for only six percent of total global purchases. However, electronic commerce is likely to grow dramatically over the next decade. Thus, it is predicted that within four years, global shoppers will purchase $700 billion of goods and services, representing almost 10 percent of current purchases worldwide. And, by 2007, the number of transactions is expected to rise to 19 billion, which is almost 60 percent of the number of transactions made in today’s credit card market.

MANAGING ELECTRONIC COMMERCE
Recent years have seen great strides in automating many of the labor-intensive paper-based aspects of commerce. Thus, many enterprises now use electronic data exchange, e-mail, electronic forms (for ordering or for contracting), electronic catalogs, and electronic financial networks that speed the transfer, settlement, and clearing of funds and other financial instruments. These electronic tools and techniques provide many benefits to both customers and merchants. EDI standards, for example, enable fast, accurate information exchange between different automated systems for routine, relatively simple business transactions.

However, despite the widespread use of electronic support, electronic commerce is still not the most common method of carrying out enterprise transactions. One reason is that most enterprise transactions still require the physical exchange of paper documents and instruments, along with their inherent cost and delays. In addition, current electronic commerce approaches are not sufficiently well integrated, secure, open, or easy to use.

Partial Solutions
Today’s electronic commerce implementations automate only a portion of the entire transaction process. For example, although ordering and
distributing an information-based product (such as an electronic magazine or a software program) can be nearly simultaneous, the supporting accounting and inventory information, payment, and actual funds transfer tend to lag, often by days. Credit risks increase because of this time lag, as well as the resulting decoupling of the accounting and payment information from the ordering and delivery of goods and services. The time lag also increases the likelihood of discrepancies among the various information sources, requiring expensive and time-consuming reconciliation.

In addition, today's electronic commerce implementations are costly to develop and operate. The high cost of entry makes them unfeasible for the spontaneous, high-volume, low-value electronic transactions that analysts envision for the future.

By contrast, a fully integrated electronic commerce solution would provide many benefits. It would let users maximize their control over cash flow, enabling them to keep most of their funds in bank savings accounts or investments, and minimizing cash shortfalls. It would also eliminate the time gaps between ordering, distribution, and payment. This would in turn enable organizations to develop realtime links to their recordkeeping and accounting systems, with minimal transaction costs.

**Rigid Requirements**

Electronic commerce applications usually require highly structured protocols, previously established arrangements, and unique proprietary bilateral information exchanges. These protocols, arrangements, and exchanges generally involve dedicated lines or value-added networks and batch processing.

For example, EDI requires rigid agreements between the two or more transacting parties about the structure and meaning of data. These agreements are often time-consuming to negotiate, inflexible, and difficult to maintain, especially in a rapidly changing enterprise environment. The resulting costs and required lead times frequently bar small- and medium-sized enterprises from investing in and using electronic commerce applications, thus inhibiting the expansion of electronic commerce beyond large enterprises and their major trading partners.

**Limited Accessibility**

In today's electronic commerce applications, the consumer can seldom communicate or transact with vendors in a simple, direct, free-form environment. For example, to access most electronic shopping services, a consumer must subscribe to an online service (such as Prodigy or cable TV shopping channels) that then provides proprietary hardware and software for communication with the vendors that have also registered with that service.
Limited Interoperability
Most current electronic commerce implementations depend on proprietary solutions, which do not easily interoperate, if at all. Notable exceptions are Internet e-mail and the World Wide Web. A truly interoperable electronic commerce infrastructure would allow parties to conduct their transactions in private, without paying any fees to intermediaries unless they provide some real added value, such as credit services. This infrastructure would make it easier for any and all interested persons to become service providers as well as consumers.

Insufficient Security
It is difficult to authenticate parties and detect intruders due to the lack of personal contact and anonymity associated with doing commerce over a telecommunications network. This in turn makes the system vulnerable to fraud, thereby increasing the need for security services.

Additionally, the speed with which electronic commerce can be conducted leaves parties with less time to react, check, and respond appropriately, again creating the potential for system fraud and abuse. Lack of sufficient security inhibits the introduction of direct, secure, realtime electronic payment and settlement systems that can support secure exchanges without prearrangements or third parties.

Inadequate Search Capabilities
Participants in today’s electronic commerce applications must find methods of navigating effectively through the sea of rapidly increasing online electronic information and services, in order to find trading partners and items of interest. This problem will only increase as more information and enterprises go online. The EDI standard can help.

EDI STANDARDS
Before organizations can begin to conduct full-scale trading operations over the Internet, they must solve the problems of electronically exchanging large quantities of transactional data (e.g., purchase orders, invoices, and shipping documentation). At the same time, they must ensure complete authenticity, confidentiality of every exchange, data integrity, and nonrepudiation of both sender and receiver.

Electronic data interchange was designed to fulfill these requirements. As the lowest level of communication among enterprises, EDI provides the automated, application-to-application exchange of structured enterprise data — such as purchase orders and invoices — between an enterprise and its suppliers, customers, banks, and other trading partners.

EDI automates the slow, labor-intensive processes of exchanging transactional documents in hardcopy form. Typical paper transaction sys-
tems require extensive keying and re-keying of data, voluminous fax transmissions, mailings, express deliveries, internal routing for approvals, and a host of other processes that require significant outlays of time and money. EDI eliminates these manual transactions by electronically handling these tasks. The benefits of EDI are improved cycle times, reduced error rates, and significant cost savings.

EDI standards specify the format and data content of electronic business transactions by defining a common syntax for transferring information across departments, enterprises, industries, and countries. And standard EDI transaction sets allow enterprises to exchange various kinds of transactional data regardless of its original format.

EDI standards began in the 1960s with a cooperative effort to develop industrywide EDI standards for purchasing, transportation, and financial applications. Eventually, the idea of national standards for use across industries received substantial support.

Today, EDI standards are developed and maintained by two recognized standard bodies. The U.S. EDI standards body, Accredited Standards Committee X12 (ASC X12), chartered in 1979, meets under the auspices of the American National Standards Institute (ANSI). In 1983, ANSI published the first American National Standards for EDI. For its part, the Electronic Data Interchange for Administration, Commerce, and Transport (EDIFACT) is an international standards body, established by the United Nations in 1985.

ASC X12 and EDIFACT have developed more than 400 transaction sets intended to satisfy a broad spectrum of data requirements. Recent industry research indicates that EDI reduces cycle time by an average of 60 percent. These improvements affect such enterprise functions as order entry, procurement, manufacturing, logistics, and finance.

Cutting cycle time reduces inventory, increases working capital, and speeds up order fulfillment — a key to customer satisfaction. By improving cycle time, EDI enhances the enterprise’s ability to implement just-in-time (JIT) inventory and manufacturing processes. In addition, EDI eliminates errors that are introduced through the re-keying of transactional data — its most important benefit.

The cost savings from EDI are equally dramatic, ranging from $3.80 to $7.40 per document in 1996. These savings come from cutting redundant processing steps; eliminating paper, postage, and data entry; and reducing the hours spent signing, checking, or approving transactions. Thus, the ultimate reasons for doing EDI are to improve customer service and competitive advantage.

For many enterprises, EDI is a requirement for doing business with key trading partners. Large manufacturers and retailers often require that their suppliers use EDI as a pre-condition for all purchase agreements. These large hub sites are in a position to dictate the use of EDI to their smaller trading partners, or spokes. In 1997, EDI hub enterprises aver-
aged more than 600 EDI spokes, representing more than 70 percent of the enterprises with which they do business.

In order to implement EDI, organizations must develop or acquire EDI translation software, integrate EDI with their core business applications, and select a communications architecture for data transmission. EDI translation software automatically converts documents from their original enterprise applications into the desired EDI standard format, and then wraps them in an electronic envelope with a unique identification code. Data from such departmental applications as order entry, invoicing, accounts receivable and payable, and freight tracking must be translated into EDI standard formats for transmission to trading partners. The EDI translator is designed to interact smoothly and efficiently with a variety of off-the-shelf software applications.

In addition to translation software, EDI requires communications software to transmit EDI messages over a variety of network transport protocols. EDI translation software usually comes with communications modules, enabling customers to choose the network communications option that best suits their enterprise and trading partners. Currently, most EDI-capable enterprises are third-party service providers that operate value-added networks (VANs) and serve as intermediaries to all transactions. Proprietary VANs such as Advantis, GEIS, Sterling Software, and others assume responsibility for transmitting, controlling, logging, and archiving all messages through a central electronic clearinghouse; they also offer extensive customer support.

To eliminate the need for a VAN, some enterprises offer trading partners a direct connection to their internal networks. This is the fastest growing form of EDI today because it allows trading partners to avoid VAN transmission charges and monthly maintenance fees. Market growth for direct connectivity (already approaching half the size of the VAN market) has been inhibited only by the fact that the technology alone does not ensure the authenticity, integrity, and message tracking normally provided by VANs.

The emergence of the Internet as a medium for electronic commerce offers a potential solution to the limitations of proprietary networks. Electronic commerce via the Internet offers many advantages over traditional paper-based commerce:

- It provides the customer with more choices and customization options by better integrating the design and production processes with the delivery of products and services.
- It decreases the time and cost of search and discovery, both in terms of customers finding products and services (by shopping, navigating, etc.) and enterprises finding customers (by advertising, target marketing, etc.).
• It expands the marketplace from local and regional markets to national and international markets with minimal capital outlay, equipment, space, and staff.
• It reduces the time between the outlay of capital and the receipt of products and services, or vice versa.
• It permits just-in-time production and payments.
• It allows enterprises to reduce overhead and inventory through increased automation and reduced processing times.
• It decreases the high transportation and labor costs of creating, processing, distributing, storing, and retrieving paper-based information; and of identifying and negotiating with potential customers and suppliers.
• Through automated information, it enables the production of a reliable, shareable historical database of design, marketing sales, and payment information.
• It facilitates increased customer responsiveness, including on-demand delivery.

The Internet would seem at first glance to be an ideal medium for electronic commerce, with its low cost, high speed, open access, and robust architecture. There are significant issues, however, associated with its use for commercial transactions; these include:

• difficulties in obtaining a reliable assurance of authenticity or receipt
• an inability to confirm message integrity
• a lack of security
• vulnerability of messages to interception and fabrication
• lack of user support

Until recently, these concerns have stymied efforts to conduct enterprise transactions over the Internet. Now, however, software is available to solve these problems. For example, to guarantee secure EDI transactions, many software packages incorporate data encryption technology, such as that from RSA Data Security, Inc., the de facto standard for public-key encryption and digital signatures.

These products then allow users to encrypt communications at the EDI application layer, ensuring end-to-end security regardless of the networks used. For each outbound message, this software generates a digital signature that verifies the identity of the sender, and automatically detects any alteration of the message upon receipt. The software also automatically returns a confirmation that the document was received, unaltered, and digitally signed by the intended recipient. It thus enforces reliable data integrity, authenticating the sender of the message, and providing nonrepudiation of both origin and receipt.
The technology that enables secure EDI over the Internet will change the foundation infrastructure of global business. Already, many public and private enterprises are rising to the opportunity, offering services designed to facilitate secure electronic commerce over open networks.

In June 1995, both the U.S. Postal Service and VeriSign, Inc. announced plans to provide certification authority for EDI users over the Internet. The goal of these efforts was to provide business Internet users with the ability to expand trading partner communities with the added assurance that they would be authenticated by an independent third party. By registering with a certification authority, any enterprise will be able to list its public key in an official, certified directory and enjoy secure trading privileges with a wide array of potential trading partners.

In a related development, the American Bar Association’s (ABA) Information Security Committee recently announced an initiative to establish a legal foundation for use of digital signatures as a security mechanism for electronic commerce. This initiative is an important step toward the legal certainty of public-key exchange and digital signatures. The ABA is working to provide the legal infrastructure that will address the enterprise issues faced by organizations that are currently developing electronic commerce strategies.

MANAGING SECURITY AND PAYMENT

A secure system of payment is the basic requirement for commerce over the World Wide Web. There are many protocols to solve this problem. The issues in designing such systems are scalability, security, and anonymity. These issues are addressed to prevent enterprises from gathering information relating individuals with the amounts that they have spent, the locations involved, and the types of goods purchased, since the misuse of such information threatens personal privacy.

The most effective method of achieving this is to implement some form of electronic cash, where the coins being spent cannot be linked to their owner. Since this potentially introduces the fraudulent use of duplicated coins, such a payment system must guard against the coin being spent more than once. And it should not be possible for an attacker to bypass the system, or to falsely obtain monetary value from it.

Such a system must support large numbers of buyers and sellers who are affiliated with many different banks. Since the detection of double-spending is a major concern with multiple banks, solutions must allow large numbers of payments to be made, without requiring the maintenance of unreasonably large databases.

Two systems for electronic payment are Ecash and NetCash. In addition, a new set of protocols, the PayMe Protocol and the PayMe Transfer Protocol (PMTP), surmount some of the inherent problems.
Ecash
Ecash is a fully anonymous electronic cash system because it uses numbered bank accounts and blind signatures. Electronic cash is the electronic equivalent of real paper cash, and can be implemented using public-key cryptography, digital signatures, and blind signatures. In an electronic cash system, there is usually a bank responsible for issuing currency, and customers with accounts at the bank who can withdraw and deposit currency.

Every customer, merchant, and bank has its own public/private key-pair. The keys are used to encrypt (for security) and digitally sign (for authentication) blocks of data that represent coins. A bank digitally signs coins using its private key. Customers and merchants verify the coins using the bank’s public key. Customers sign bank deposits and withdrawals with their private key, and the bank uses the customer’s public key to verify the signature. The Ecash system consists of three main entities:

- banks that mint coins, validate existing coins, and exchange real money for Ecash
- buyers who have accounts with a bank, from which they can withdraw and deposit Ecash coins
- merchants who can accept Ecash coins in payment for information or hard goods; it is also possible for merchants to run a pay-out service where they can pay a client Ecash coins

Ecash is implemented using RSA public-key cryptography. Every user in the system has his or her own public/private key-pair. Special client and merchant software is required to use the Ecash system. The client software, called a cyberwallet, is responsible for withdrawing and depositing coins from a bank, and paying or receiving coins from a merchant.

NetCash
NetCash is a framework for electronic cash developed at the Information Sciences Institute of the University of Southern California that uses identified online electronic cash. Although the cash is identified, there are mechanisms whereby coins can be exchanged to allow some anonymity. The system is based on distributed currency servers, whereby electronic checks such as NetCheque can be exchanged for electronic cash. The use of multiple currency servers allows the system to scale well.

Buyers, merchants, and currency servers are included in the NetCash system. An enterprise wanting to set up and manage a currency server obtains insurance for the new currency from a central certification authority. The currency server generates a public/private key-pair. The public key is then certified via Central Authority signature. This certificate contains a certificate ID, the name of the currency server, the currency
server’s public key, the issue date, and an expiration date, all signed by
the Central Authority.

PayMe Protocol
A new payment system called the PayMe Protocol Set was devised in an
attempt to combine the best features of the two systems described above.
A major goal was to preserve as much of the anonymity provided by
Ecash as possible, while adopting the features of NetCash that allow it to
scale to large numbers of users with multiple banks.

PayMe is an online electronic cash system that involves banks and us-
ers. While users can be either buyers or merchants, all can make pay-
ments, accept payments, or deal with the bank. Each bank mints its own
identified electronic cash with serial numbers. The bank prevents dou-
ble-spending of coins by maintaining a database of coins in circulation.
This scales better than the blind signature electronic cash approach.

Any user in the PayMe system can accept and make payments. Mer-
chants can receive payments for selling Web goods, and also make pay-
ments to the buyers, in case of refunds or in pay-out services.

To communicate between entities, the PayMe system uses its own se-
cure communications protocol, the PayMe Transfer Protocol (PMTP).
This provides security and a means of communicating out-of-band (i.e.,
outside the Web’s HTTP protocol). This approach was adopted to devel-
op a full prototype that could eventually be used with any emerging Web
security standard.

PMTP Security. PMTP security prevents eavesdropping, message tam-
pering, replay, and masquerading. It also offers private-key protection.

Eavesdropping Prevention. The contents of a PMTP message cannot
be seen by an attacker because the message is encrypted with the public
key of the receiver. Only the private key can decrypt the message or en-
crypt it with a symmetric session key that has been distributed securely.
The session key is distributed by sending it in a public-key encrypted
message.

Message Tampering Prevention. Because it will not be possible to
decrypt an encrypted message after it has been changed, most encrypted
messages cannot be tampered with. Because message digests are used, a
digitally signed message cannot be tampered with.

Replay Prevention. To ensure that the message can be used for only
one occasion, and to prevent a replay of the message, a nonce is used
within each PMTP message. This ensures that the message comes from a
specific network address, and within a small time window. If an attacker
can forge the IP network address to be the same as that of the message sender, then he or she could possibly replay the message within the short timeframe that it is valid. To help prevent this, the software keeps track of all recently received nonces, and will not accept two messages with the same nonce, which would be the case for a replayed message.

**Masquerading Prevention.** All messages are authenticated with a digital signature where possible, and bank withdrawals also require the bank account’s password. In anonymous messages where a digital signature is not possible, a symmetric session key is used. Thus, the network address within the nonce prevents an attacker at another site from masquerading as the message sender at the original network address.

**Private Key Protection.** Finally, the private user key is stored on file at the user’s local site, encrypted with a secret passphrase. If someone breaks into the user’s account, the attacker cannot access the private key. Without this private key, any cash stored locally cannot be decrypted, and PMTP messages cannot be sent.

**CONCLUSION**
There are many new systems and service initiatives for the Internet that address the current deficiencies of managing electronic commerce and security. These initiatives include:

- CommerceNet and Secure HyperText Transport Protocol (SHTTP)
- electronic catalogs
- advanced search engines
- e-mail-enabled EDI
- digital cash

In addition, several alliances and partnerships have been announced that address the need for secure, affordable payment, which is linked in realtime to ordering and billing systems. These initiatives include ventures by Open Market, Microsoft/Visa, Netscape/First Data/MasterCard/Bank of America, Cybercash/Wells Fargo, American Express/America Online, First Virtual/EDS, NetBill, NetCash, Café-Digicash, Mondex, NetCheque, NetAccount, Netchex, AT&T, and Internet-MCI. More such alliances and start-ups are announced each day. These initiatives promise to accelerate the future growth of electronic commerce, while substantially decreasing the overhead and time associated with today’s paper- and people-intensive activities.

Therefore, there should be a broad range of new value-added electronic commerce services in the near future, including the following, which are built around trust and security:
• appraisal services
• authentication over public networks
• automated dispute resolution
• certification of information, parties, and transactions
• electronic escrow
• performance bonding
• transaction insurance
• trusted agents to resolve disputes and claims
• various electronic broker services

There is also the risk of creating isolated, non-interoperable implementations that will inhibit progress toward truly free, open, and spontaneous electronic commerce. Joint ventures tend to vary in their approach to security and privacy, their ability to handle micropayments, and their applicability to various types of transactions. They also differ in their enterprise models; for example, in their pricing strategy, and in determining who bears the risk in case of insufficient funds or disputes.

The electronic commerce infrastructure must therefore allow for interoperability on the one hand, and maximum flexibility on the other, to permit innovation. To enable this, the infrastructure must be based on a common set of services and standards that ensure interoperability. Preferably, these services and standards can be used as standard building blocks that service providers and application designers can combine, enhance, and customize.

In addition, the infrastructure must allow for maximum flexibility to permit innovation. As the management of electronic commerce and security evolves, it will grow and mature significantly, possibly in ways not even imaginable today. As it grows, new services and enterprises will emerge. For example, the electronic marketplace will provide new opportunities for narrow-case marketing to short-lived niche markets. Also, existing services and products will be redefined and modified. Thus, the electronic commerce infrastructure must be sufficiently flexible to accommodate all of these changes, while being able to address new applications and requirements as they arise.

Finally, upon entering the 21st century, the Internet and the World Wide Web will become more of an integral part of our everyday lives. Because the reality of electronic commerce is here, and the infrastructure for a successful electronic enterprise venture is within reach, it will not be long before enterprises realize the benefits. In the near future, electronic transactions will be as popular if not more so, than the credit card purchases of today.

John R. Vacca is an information technology consultant and internationally known author based in Pomeroy, Ohio. Since 1982, John has authored 27 books and more than 330 articles in the areas of Internet and intranet security, programming, systems development, rapid application development, multimedia, and the Internet. He has also
been a configuration management specialist, a computer specialist, and the computer security official for the
NASA space station program (Freedom) and the International Space Station Program. He can be reached on the
Internet at jvacca@hti.net.

Notes
1. The address of CommerceNet is 10050 N. Wolfe Road, Suite SW2-255, Cupertino, CA 95014.
2. RSA Data Security is located at 2955 Campus Drive, Suite 400, San Mateo, CA 94403-2507.
3. The address of VeriSign, Inc. is 1350 Charleston Road, Mountain View, CA.