B2B E-commerce: Technological, Legal and IPR Issues*

V K Gupta

National Institute of Science Communication
Dr K S Krishnan Marg, New Delhi 110012†

(Received 16 April 2001)

E-business, e-commerce, e-marketplace, B2B, and B2C are now common business parlance. E-business involves all the enterprise-procurement, supply-chain management, sales and customer relationship management, online business transactions, etc. IP/VPN, digital watermarking, encryption, public key infrastructure are the essential technologies, which are required to be deployed for implementing B2B e-commerce solutions. This paper describes the B2B and associated technologies, legal framework for B2B, and IPR issues of B2B.

Twenty first century will be the century of knowledge, indeed the century of mind and a nation's ability to convert knowledge into wealth and social good through the process of innovation that will determine its future. The increasing knowledge gap is a major concern between the developing and developed world. The knowledge differential can be bridged in a short time by understanding the technology, which is driving the knowledge revolution. Business-to-Business (B2B) is one such area, which makes direct impact in reducing the differential between the developed and developing countries. Technology is accelerating and has become the engine of globalization. The 24 hours a day and seven days a week markets and e-commerce are both enabled by technology. Internet has supposedly democratized the world and has simultaneously thrown major challenges for the developing world. It is said that business normally moves at

*Based on the paper 'Issues on B2B E-commerce with Practical Application of Inter-firm Electronic Networking' presented by Mr V K Gupta, Director, NISCOM, New Delhi, at the symposium on Inter-firm Electronic Networking, organized by the Asian Productivity Organization, Tokyo, held on 17 April 2001 at Taipei, Republic of China. †E-mail: vkg@nistads.res.in
three times the speed of government and laws. E-business moves at three times the speed of normal business, therefore, e-business is nine times faster than government and laws. The problem of speed differential between e-business and government is being increasingly felt even by developed world. The necessity of much higher degree of response was never being more urgent for countries as is being felt now.

The emergence of e-commerce as a tool for global competitive advantage is engaging increasingly greater attention since the mid 1990s. With increasing global dimensions of knowledge-based economy and the growth of knowledge-based products, several challenges are appearing in the administration and management of commerce and trade. The implementation of an appropriate and regulatory framework, the development of skills and competence to manage e-commerce, with a view to leverage its influence and gain competitive advantage, needs increasing focus in particular among the developing countries.

E-business, e-commerce, e-marketplace, B2B, and business-to-consumer (B2C), are now common business parlance. Every organization is defining and implementing its e-strategy. The question is no longer whether to migrate to an e-environment, but what is the best way to migrate to a Web- and Internet-based business model.

The Internet allows businesses to reach their customers, and vice versa, anytime and anywhere in the world. An Indian company need not deploy any resources or infrastructure in China, for example, to do business in China. A father-and-son e-business in a non-English speaking country has as good a probability of reaching a customer in the USA as an American multi-billion dollar company. A common challenge to both companies is the use of the Internet to leverage their business.

**Business Problem**

Before the popularity of the Internet, large enterprises were building multi-million dollar private data networks (now called intranets), using telecommunications services such as leased lines, frame relay and Asynchronous Transfer Mode (ATM) to communicate among geographically dispersed sites. These services were often supplemented with services, such as switched analog or ISDN, to connect smaller sites and mobile users.

These intranets were expensive and required large number of support personnel. Intranets also had long planning, design and implementation cycles, resulting in tremendous lost-opportunity costs. As the Internet became ubiquitous and as ISPs offered high-speed Internet access, enterprises reduced the cost and the time to deploy their intranets by off-loading them on to the Internet.

As enterprises dabbled in e-commerce, whether as B2B or as B2C, it became clear that the Internet was the practical and cost-effective way to connect with customers and partners. The concept of connecting with external users or organizations came to be known as extranets.

As cost-effective as the Internet is, it introduces one major challenge—security. Though the Internet has emerged as the network foundation for e-endavours, it is paradoxically a public-shared network of networks and is not suitable, in its natural state, for secure transactions or private communications.

Enterprises have recognized that e-business is more than just Internet connectivity
or the exchange of e-mails and files. E-business needs real time exchange of data. This involves all of the enterprise-procurement, supply-chain management, sales and customer relationship management, online business transactions, online dealings with financial institutions, etc. These requirements make security over the Internet paramount.

**B2B and Associated Technologies**

One of the key technologies for using the Internet in a secure and private manner is the virtual private network (VPN). IP/VPN, digital watermarking, encryption, and public key infrastructure are the essential technologies, which are required to be deployed for implementing B2B e-commerce solutions. In addition to these technologies, there are several other technological options; deployment of these options will enhance the effectiveness of B2B implementation. Peer-to-peer, XML, Bluetooth, application service providers, digital compression techniques, software agents, and business process innovations are some such options.

**VPN Overview and Benefits**

A firewall is an important security feature for Internet users. It prevents unauthorized users and data from leaving and entering an enterprise. However, when packets pass through the firewall to the Internet, sensitive data such as user names, passwords, account numbers, financial and personal medical information, server addresses, etc. is visible to hackers and to potential criminals. Firewalls do not protect from threats within the Internet. This is where a VPN comes into play. A VPN, at its core, is a fairly simple concept—the ability to use the shared, public Internet in a secure manner as if it were a private network. VPN permits flow of encrypted data as well as user and data authentication. We need software or some other device at each end of the tunnel to initiate, authenticate, and terminate a VPN tunnel. In addition to encryption, VPN also allows for user- and data-authentication.

**VPN—The New Solution for E-Business (Extranet)**

VPNs have emerged as the key technology for achieving security over the Internet. While a VPN is an inherently simple concept, early VPN solutions were geared towards large organizations and their implementation required extensive technical expertise. As a consequence, small and medium-sized businesses were left out of the e-revolution. Recently, VPN solutions have become available that focus specifically on the needs of small and medium-sized businesses.

VPN is driven by re-engineering of business operations. As can be seen from the Fig. 1, VPN provides implementable solutions, which are secured. It is possible to establish Intranet between sales and marketing, maintenance and product management functions normally over the enterprise LAN infrastructure, in case these functions are co-located within the same campus. Whereas e-business or B2B is established between major suppliers and known clients as an extranet catering to the needs of functions such as procurement, delivery and construction aspects of the business. Today B2C in a secured manner is transacted over Internet.

**Technical Concepts and Enabling Technologies**

Tunneling (encapsulation), Encryption, and Authentication are key enabling technolo-
Fig. 1—Business process drive VPNs

Encryption Technology Overview

"Encryption" is as old as humanity. From communications in Ancient Egypt to modern-day digital techniques, human beings have always tried to find ways to ensure that their communications could not be understood by "unintended recipients". Businesses that need confidentiality (negotiations of a business agreement, protection of trade secrets, etc) or want to restrict access to material (pay television); or consumers and citizens who want to protect their privacy.

Against this backdrop, encryption can be defined as a generic term covering all techniques to encipher or encode a transmission of information. Replacing the letters in a message with a corresponding number or by the next letter in the alphabet is a form of encryption.

Symmetric Encryption

There are two main kinds of encryptions: symmetric and asymmetric. Symmetric encryption means that the same key that is used to encrypt a message is also used to decrypt a message. For most its existence, encryption has used symmetric keys. The problem with symmetric encryption is that the parties to the transmission must have access to the key and must, therefore, find a
secure way to exchange the key or password necessary to encrypt and then decrypt the file or message. Naturally, they must keep the key secret, and any one gaining access to the key (with or without the knowledge of the parties) would be able to decrypt the message. While this risk exists in any form of encryption, it may be greater in the case of symmetric encryption, as parties might be tempted to use the same key for a long period of time.

One of the most popularly used symmetric encryption algorithms is the Digital Encryption Standard (DES), which is used, inter alia, on bankcards for automated teller machines (ATMs).

Asymmetric Encryption

Another form of encryption is now more commonly used and may be more flexible. Asymmetric cryptography became known in the 1970s. The main difference between this form of encryption and symmetric cryptography is that asymmetric encryption makes it possible to divide an encryption key into two parts: one part is private (or secret) and the other part is public. In fact, asymmetric encryption is also referred to as private key/public key encryption. It allows one person to send an encrypted message to another person without worrying about how the other person will get the secret key. The sender uses the receiver's public key (which is freely available, for example in a key directory) and the receiver uses the private key that corresponds to the public key to decrypt the message.

Digital Signatures

Asymmetric encryption may also be used to “sign” the message, whether or not the message itself is encrypted. This “digital signature” normally works as follows: A sends a message to B and includes an encrypted signature that corresponds to the text that was sent. This encrypted message is known as a “hash”. When B receives the message, he/she decrypts the message using A’s public key. If A’s public key successfully decrypts the hash, this proves that A actually sent the message or, more precisely, that the message was sent by someone who used A’s private key. A digital signature may also be sent without additional data, and may be decrypted using the same technique. If the sender’s public key matches the private key that he/she sent, the receiver knows the message was indeed sent by A (or someone using A’s signature).

The purpose of a digital signature is not to guarantee the confidentiality of the message, but rather to ensure its integrity. If the public key/private key pairs are properly managed, in the sense that only A uses A’s private key, then the signature also proves the origin of the message. It is worth noting that a person may have more than one public key/private key pairs.

Public Key Infrastructure

A public key infrastructure (PKI) may be defined as the legal and technical structure necessary to issue digital certificates and Licence Certification Authorities (CAs).

Digital certificates are the identity cards of those who buy and sell on networks. Issuance of a certificate is normally required before a CA will accept to register A’s public key as belonging to A. The certificate might contain A’s identity, the public key number(s) and algorithm used, since there are many in circulation. It might also have an expiry date and identification about the Certification Authority.

Digital Water Marking Technology

Watermarking is the process of modifying image data for inserting codes for carrying
Information. Watermarking of contents is carried out to ensure: (i) copyright protection, (ii) data authentication, and (iii) ownership identification.

Watermarking could be of several types such as blind vs non-blind, availability of identification. In case of public/private watermark, private watermark can be read only by owner whereas public watermark can be read by anyone. Similarly, watermark could be readable and detectable. Watermarking along with Electronics Rights Management Systems (ERMS) enables enforcement of copyrights in digital networks.

**Peer-to-Peer Technology**

Peer-to-peer computing is considered as the Internet's great leveler. With this technology even the normal PC can become a server on Internet serving up music files, web bages and even spare computing power to other users.

Napster and Guntella are the best-known examples. The music files which Napster users share with one another are not stored on a central server but on the PCs of users themselves. Napsters own server merely downloads the software to new users and keep a universal directory of music files. In case of Guntella even the directory information is stored on users PCs. Intel is using peer-to-peer for sharing the computing power. Intel utilises more than 10,000 of its PCs, workstations and servers which would be otherwise idle and saves about $500 million.

**Extensible Markup Language (XML)**

XML is a data manipulation standard over Internet. HTML was the key to solving display problems. XML is likely to solve data manipulation problem, a key issue in B2B. With a single command a browser will be able to collect required information from several sources and will provide direct answers. B2B transactions will become smoother. Most companies use purchase orders and many have computerized ordering process. But each company describes the element of purchase order in a slightly different way. XML will let companies encode the information in a purchase order so that it will be recognizable to every other company.

**Bluetooth Technology**

Broadband and Bluetooth together are likely to solve many of the current B2B problems. Bluetooth is a new technology standard for short-range wireless communication. It will let laptops communicate with printers, cell phones, palms, vending machines, and each of these devices with Internet. Bluetooth also adds built in security and faster data rates. Bluetooth is named after Herald Blat and (Bluetooth) II, king of Denmark from 940 to 981, the man who unified the Danes under Christianity.

**Application Service Provider (ASP)**

ASP provides software application capabilities on rental basis in accordance with the service level agreement. These services are delivered on a one-to-many basis via a WAN usually an IP network. ASP value chain includes: (i) independent software vendor, (ii) application infrastructure provider, (iii) network service provider, (iv) service portal, (v) service aggregator, (vi) value added reseller, and (vii) system integrator. ASP industry is expected to reach $44 B by 2004 and is an important component of B2B.

**Legal Framework for B2B**

For business to get conducted over a network, it is necessary to meet essential conditions of: (i) confidentiality, (ii)
authentication, and (iii) non-repudiation. United Nations Commission on International Trade and Law (UNCITRAL) evolved the model e-commerce law in 1996 to provide legal framework to e-business. Model law addresses the issues relating to digital signature digital contract, digital certificates, etc. Several of the countries have enacted legislations known as Cyber Laws. India has also enacted Indian IT Act, 2000. The Information Technology Act provides legal recognition to e-commerce. The act is comprehensive in nature and addresses the amendments in related acts such as the Indian Penal Code. The Indian Evidence Act, 1872, The Bankers Book Evidence Act, 1891, and The Reserve Bank of India Act, 1934. The Act is broadly in accordance with the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law.

The IT Act provides legal recognition to electronic records, digital signatures, retention of electronic records, and the publication of electronic gazette. Digital signatures shall be utilized to authenticate electronic records and verification of digital signatures will be realized through the public key of subscribers. For addressing the issue of non-repudiation, arbitration and acknowledgement mechanism has been provided in the Act. 

Provisos including PKI are being realized by establishing the Office of CCA, who is responsible for issuing digital signatures certificates based on PKI.

Under this Act cyber offences have been defined as: (i) unauthorized access, (ii) unauthorized duplication, (iii) introduction of computer virus, (iv) causing damage to data or systems, (v) denying access rights to authorized users, and (vi) providing assistance in commission of offences. A Cyber Regulation Appellate has been established to provide for an expeditious dispute resolution mechanism. Provision for appeal against the orders of the Tribunal in higher courts is available.

The IT Act also provides for comprehensive amendments in related Acts, so that problems in utilizing electronic record in place of paper records while deciding the cases in courts of law as per provisions of Indian Penal Code or Indian Evidence Act are obviated. Amendments to the Banker's Book Evidence Act will provide ease of operation of bank records, which include ledgers, daybooks, cashbooks, account, etc. Amendments to the Reserve Bank of India Act will ensure the establishment of a payment gateway in the country.

**B2B and Intellectual Property Rights**

B2B is also utilized for digital delivery of products in particular in infotainment and software sector. Since it is possible to replicate digital products countless times and each copy has same value in its own rights. Also Internet has made stealing of digital IP easier where on Crackz, a code word for circumvention sites, more than three hundred thousand pages of information gets provided, offering patches designed to defeat technological protection. Therefore, protection of digital IP has become very important.

Digital technology offers the opportunity to make perfect copies with levels of speed, accuracy and volume well beyond its predecessors. Each copy in turn can be further reproduced and disseminated, against without any loss of quality. Even more significant is the ability of this technology to make works available to the public in large numbers almost instantaneously. Digital networks allow dissemination to many
individuals from a single point; each recipient on the network can engage in further dissemination of the work, causing the work to spread exponentially.

Unlike previous technologies, digital technology also makes it possible for users as well as the original creators to alter and modify works with ease. Moreover, equipment needed to do all these things exists not just in centralized locations and commercial establishments but also in private homes—millions of them spanning the globe.

**WIPO Treaties**

From the early 1990s there was a discussion on the need to update the major international treaties to address the impact of digital technologies. The texts of the Berne and Rome Conventions date back more than a quarter century ago. The culmination of these discussions was the conclusion of two new World Intellectual Property Organization (WIPO) treaties: the WIPO Copyright Treaty (WCT), and the WIPO Performance and Phonograms Treaty (WPPT) in Geneva in December 1996. Among other things, these treaties and their interpretive statements require that right holders enjoy exclusive control over on-demand electronic disseminations of their works, and confirm that the reproduction right is fully applicable in the digital environment. They also require member countries to protect the technologies used to prevent infringement and the rights management information that right holders may choose to provide in digital form.

Article 11 of the WCT obliges contracting States to provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty.

Article 12 of the WCT obliges contracting States to provide adequate and effective legal remedies against any person knowingly performing any of the following acts knowing, or with respect to civil remedies having reasonable grounds to know, that it will induce, enable, facilitate or conceal an infringement of any right covered by this Treaty to remove or alter any electronic rights management information without authority; and to distribute, import for distribution, broadcast or communicate to the public, without authority, works or copies of works knowing that electronic rights management information has been removed or altered without authority.

As can be seen now adequate legal provisions exist to protect IPR of B2B.

**Establishment of the South Asian Intellectual Property Network: SAIPnet**

SAIPnet is being established for SAARC countries where major focus is going to be on IPR. It is expected that with the establishment of SAIPnet, SAARC countries will be able to exchange information in a cost-effective, highly secured environment. SAIPnet will provide a platform on which SAARC countries can build and run current and future processes and applications and will be able to take advantages of international initiatives such as WIPOnet. SAIPnet will be able to serve the information needs on intellectual property information, for the general public, which includes investors, associations, institutions and those individuals who are interested in understanding the process of protecting their concepts/ideas.

Aims of SAIPnet are to: (i) promote the use of intellectual property information among
the SAARC countries, by the IP community and the public at large, thereby ensuring the effective enforcement of IPR, (ii) facilitate the dissemination of IP information so as to provide catalytic effect for technology transfer for the SAARC countries, (iii) build, preserve and promote information of traditional knowledge of the SAARC countries and ensure prior art gets established, (iv) ensure that required legal framework is in place in SAARC countries, so that SAIPNet is able to meet the objectives of providing cost effective and quality service to the applicants of the SAARC countries and is able to utilize newer technologies in IPR such as e-commerce and Internet.

Modernized national patent offices, extranet (IP/VPN) at intellectual property / industrial property offices and interface with international networks such as WIPOnet are the essential components of SAIPNet, and traditional knowledge databases, IP-related search and examination (Web-enabled), Web-enabled electronic filing and e-commerce would be its main services.

Challenges for Developing World

E-commerce provides the opportunities for organizations to open new international markets, improve their competitiveness through lower transaction cost and better customer services independent of their locations. To realize this, there are several challenges, which are to be faced and managed by developing world before an indiabook.com can aspire to become an amazon.com or the equivalent of travelocity.com gets created in a country like India. These challenges primarily relate to providing a similar environment for organizations and customers to operate with comfort and ease with regard to electronic transactions as they are available to their counterparts elsewhere. Some of the major areas, in addition to providing legal environment, are: (i) providing reliable, efficient and economical telecom infrastructure, (ii) enhancing PC penetration, (iii) providing similar level of confidence and comfort for electronic transactions as available to that of paper based transactions, (iv) establishing electronic payment gateways, (v) security against fraud/cyber laundering, and (vi) meaningful contribution in setting up of standards.

Business and customers are required to have a similar or a better level of confidence and comfort in electronic transactions as they have in paper-based transactions. Adequate safeguards are required to be in place in respect of confidentiality, authentication, access control, etc. For this regulations relating to public key infrastructure, encryption, digital signatures, rules, anti-circumvention provisions are necessary. Knowledge of security and encryption related aspects are the key to success or else the payment gateway may get hacked into. Even a few incidences of such a nature will result in a major setback to the advancement of e-commerce in the country. Awareness and education programmes at national level are required to be launched.

It is necessary also that efforts are made to contribute towards evolving and establishing standards relating to e-commerce. Presently, there are barriers to export of encryption technologies. For reasons of sustainability, it is essential to understand e-commerce related technologies. This can be achieved by undertaking research projects in close cooperation with the private sector. This will enable developing countries to contribute to encryption technology and products. This will also provide the ability to assist and contribute in the process of evolving and establishing e-commerce standards.