Bruce Klopfenstein. “Key Concepts in Internet Commerce”
*Handbook of Emerging Communications Technologies: The Next Decade.*
Ed. Saba Zamir
Boca Raton: CRC Press LLC, 2000

# 17 Key Concepts in Internet Commerce

*Bruce Klopfenstein*

## CONTENTS



This chapter briefly introduces the key concepts surrounding Internet commerce. This fluid topic is tremendously broad, the implications are vast, and the landscape is rapidly changing. Internet commerce includes complex issues related to technology, policy, privacy, and security, each of which has both national and global implications. Definitions of terms surrounding Internet commerce are still being formulated (Smedinghoff 1998). Media scholars are loath to talk about revolutions because new media tend to evolve on the established media infrastructure. Internet commerce is, perhaps, as close to a *bona fide* revolution (which implies the displacement of an established way of doing things with a new one) in business as anything witnessed in this generation. It would be difficult, for example, for most businesses to reasonably argue against having some presence on the World-Wide Web (WWW). As this chapter discusses, the remaining barriers to rapid adoption and diffusion of Internet commerce are more social and psychological than they are technical.

## 17.1 BACKGROUND

What is Internet commerce? Theoretically, Internet commerce is a subset of electronic commerce. It and electronic commerce are perceived to be virtually synonymous in 1999. Finding a standard definition for electronic commerce, however, is

more difficult than one would expect. In fact, one recent definition of electronic commerce includes the Internet:

> Electronic Commerce is the buying and selling of goods and services or the transfer of money over the Internet or an Intranet. This can involve stores or banking activities. Standards have established to make the process easier and more secure. (Electronic Commerce, 1998)

On the other hand, this definition could be far too narrow because of its focus on the use of currency. A broader definition includes customer service over the Internet, electronic responses to requests for proposals, or simply the automation of any business-to-business or consumer-to-business relationship (Jordan, 1998; see also Minoli and Minoli, 1998, 8). It must also be noted that the parties for Internet commerce can be business-to-business, business-to-consumer, and/or intraorganizational (Mougayar, 1998). For the purposes of this chapter, no distinctions are made between electronic commerce and Internet commerce. Most of the focus here is also on business-to-consumer Internet commerce.

Research indicates that the market for electronic commerce is burgeoning. According to figures cited by Howell (1998), nearly 50 million U.S. users will be purchasing goods and services online by the year 2000. As of 1998, the average online purchase was $350 and the electronic commerce market was in the neighborhood of $16 billion. While 40% of U.S. businesses were involved in electronic commerce in 1997, that figure grew to nearly two-thirds in 1998. Worth noting is that the number of online shoppers in 1998 was much higher than the number of online buyers, but this is simply a harbinger of things to come. Chrysler, for example, expects 25% of its sales to come from the Internet by 2001. As reported by Jordan (1998), citing Forrester Research Inc., total commerce over the Internet may already have been $17 billion in 1998 and will grow to $350 billion by 2002. The 1998 Christmas season may be remembered as the turning point for shopping online as far more consumers took the plunge.

The U.S. Commerce Department estimates that by 2002, the $300 billion-plus in annual revenue from goods and services sold over the web will represent more revenue than the annual sales of General Motors Corp. and General Electric Co. combined. Channel companies are selling nearly $9 billion a year in products and services related to building e-commerce sites for end-user businesses, according to Channel Information Services (CIS), a business unit of the Channel Group of CMP Media Inc. Sales of web servers and e-commerce products are growing faster than sales of any other software products (Jordan, 1998).

A number of factors have coalesced to create a highly favorable environment for electronic commerce. At the start of 1999, approximately half of all U.S. households had a personal computer. The number of people with access to the Internet is further buttressed via connections at school, work, and public places such as libraries. Internet access appears to be well on its way to having the same ubiquity as the telephone. (If that prediction sounds overly optimistic, consider the fact that nearly as many American households now have VCRs as have telephones.) Access via other online technologies such as WebTV actually may bring the number

of online households above the number of computing households by 2002 (NFO Interactive, 1998).

Another factor that is serving as a catalyst for electronic commerce is the real and perceived time constraints under which people are living. It can be less time-consuming (if not faster) to do business online (note that e-commerce is not limited to electronic shopping) than physically traveling to a business place. Book buyers, for example, can either drive to a bookstore or order books online via an online bookseller such as Amazon.com. The tradeoffs, which include waiting for books to be shipped and paying an additional shipping charge, should be compared to the positives of a tremendous selection of titles (many of which can be delivered more quickly than if special ordered via a traditional bookstore) at prices often discounted from the suggested retail price.

A third catalyst for electronic commerce is the underlying computer hardware and software infrastructure. Electronic databases have made the process of shopping online efficient and simple. One of the keys to technology is making the interface transparent to the user; in other words, we simply want things to work without having to worry about how they are being done. This is happening.

People's own experiences with the web at home and work are making its use a normal part of their living environment. The number of people who have not used the web continues to decline. Meanwhile, households with web users are generally better educated with higher incomes than those who do not. This group often includes consumers attractive to a variety of businesses, but it also includes enterprise decision-makers who have the influence to move their own organizations to integrate the web into their normal operating procedures.

Finally, the price of consumer Internet access decreased in the 1990s. Many observers had believed that metered Internet pricing was on the way, but this has yet to happen. Indeed, the real price of consumer Internet access has actually declined (especially when accounting for inflation) despite contrary predictions by a number of Internet economists (Klopfenstein, 1997a; 1997b). As Internet access is bundled with other telecommunications services, such as regular telephone or cable television service, prices may decline further. Advertiser-supported services will also serve to lower the direct cost to consumers. This premise adds to the likelihood that Internet access is becoming as ubiquitous as telephone access.

## 17.2 THE INTERNET VERSUS OTHER NETWORKS

E-commerce began in the 1970s in large corporations with Electronic Data Interchange (EDI), a set of standards that allows companies to send invoices to and order from other companies, all electronically by means of data networks, via value-added networks (VANs). EDI also implies closed, private networks. VANs are developed for a specific application (Cook, 1998), but they are disappearing. The Internet is driving today's burst of e-commerce. The Internet is not as robust a medium as EDI via VAN, but it is less expensive by a factor of 100. Expensive VANs still make sense in one-to-many distribution, such as discount retail chain Wal-Mart (Jordan, 1998). Interestingly though, companies are moving from EDI to the Internet, a network designed to be open.

### 17.2.1 Internet Security and Encryption

Although transparent to the user, a secure environment for conducting electronic commerce is essential for both pragmatic and psychological reasons. Tremendous legal liabilities are also present for anyone who wishes to offer products and services over the Internet in return for electronic payments such as those made possible by credit cards (Crocker and Stevenson, 1998). Zimits and Montaño (1998) provide an excellent overview of technical issues related to Internet commerce.

With its roots firmly in military applications, encryption is the conversion of data into a form, called a cipher, that cannot be easily read by unauthorized people. Decryption is the process of converting encrypted data back into its original form. Simple ciphers include the substitution of letters for numbers, the rotation of letters in the alphabet, and the scrambling of voice signals. More complex ciphers work according to sophisticated computer algorithms that rearrange the data bits in digital signals.

In order to easily recover the contents of an encrypted signal, the correct decryption key is required. The key is an algorithm that undoes the work of the encryption algorithm. Alternatively, a computer can be used in an attempt to "break" the cipher. The more complex the encryption algorithm, the more difficult it becomes to eavesdrop on the communications without access to the key. Encryption is critical in electronic commerce applications such as a credit-card purchase online, or the discussion of a company secret between different departments in the organization. The stronger the cipher — in general, that is, the harder it is for unauthorized people to break it — the better. However, as the strength of encryption/decryption increases, so does the cost (Thing, 1998).

### 17.2.2 Public Key Infrastructure

Public key infrastructure, PKI (see Table 17.1 below), includes dual public and private encryption keys, digital certificates, digital signatures, key-management protocols, and certificate authorities. By many measures, the PKI provides mechanisms for establishing trust and binding commitments that are superior to accepted business practices. Over time, electronic commerce tools based on public key technology will substitute for and eventually replace established commerce archetypes such as paper contracts, personal signatures, and currency (Zimits and Montaño, 1998).

Public-key encryption is a method of encrypting and decrypting data using a pair of keys: a public key available to everyone and a private key owned by an individual and available to only that individual (Technology Overview, 1998).

Table 17.1 lists important concepts related to encryption. The public and private keys in a key pair are related in that: data encrypted with a public key can be decrypted only with the corresponding private key. For example, to send someone confidential information, you can encrypt data with a person's public key. The encrypted data can be decrypted only by the private key, which should be accessible to only the intended recipient. Data encrypted by a private key can be decrypted only with the corresponding public key. For example, to prove that you are the person sending the data, you can encrypt data with your private key. Anyone using

**TABLE 17.1**
**Public Key Infrastructure Building Blocks**

| | |
|---|---|
| Encryption Algorithms | The basic mathematical algorithms used to scramble information. Symmetric encryption uses the same keys to encrypt and decrypt, whereas asymmetric encryption uses separate keys to encrypt and decrypt information. |
| Private and Public Keys | A secret, private key and a mathematically related public key are generated for each party in a transmission. Given the public key, it is nearly impossible to determine the private key. |
| Digital Signatures | An electronic signature that is irrefutable, unique, and virtually impossible to copy or transfer. |
| Digital Certificates | An electronic document comprising a public key, digital signature, owner identity, serial number, issuer, and expiration date. |
| Certificate Authorities | Issuers of digital certificates acting as a trusted third party in electronic transactions. |

Source: Zimits and Montaño, 1998

your public key can decrypt the data, which verifies that the data was encrypted (and sent) by you.

The public key infrastructure is a system centered on the use of public key cryptography that provides each of the following critical elements:

- Information confidentiality
- Information integrity
- Authentication
- Difficult repudiation

The last point involves disallowing easy claims by a purchaser that he or she did not actually initiate an exchange.

How can one be certain that the name on a given public key truly represents the person with whom a transaction is desired? Digital certificates use a public key and owner information that together have been digitally signed (certified) by a trusted third party organization (Schnell, 1996). It gives Internet commerce customers the assurance that a web site, for example, is legitimate and not that of an impostor. It also provides a legal basis for transactions on the Internet. However, a problem with digital certificates is that if one person uses another's computer he can also thereby use the owner's certificate (Howell, 1998).

Use of digital certificates should, however, reduce fraudulent transactions (i.e., the classic ordering of a pizza delivery for an unsuspecting recipient). Certificates contain information about the certification authority, the owners of the certificate, a public key, the period for which the certificate is valid, and the host to which the

certificate was issued. The token is designed in such a way that none of its details can be changed without invalidating the digital signature. Eventually, digital certificates could be built into web browsers and *virtual wallets*, which are stored on a person's computer hard drive and contain encrypted payment and billing information for ordering online. Eventually, wallets could contain checks, coins, and credit cards (VNU E Commerce Glossary, 1998).

Howell (1998) gives an example of how a secure transaction on the WWW can take place. The person initiating the transaction on a client PC requests an item from a web server. The server returns its digital signature saying, in effect, it is what the client thinks it is. The client next passes ths digital signature on to a trusted third party, the digital signature registry, which then confirms (or refutes) the server's identity. Once this is successfully completed, the client completes the transaction. In each instance, all data sent uses dual key encryption.

## 17.3 INTERNET COMMERCE PAYMENT SYSTEMS

Crocker and Stevenson (1998) note that there are three basic architectures for Internet commerce payment systems: wallets, cash registers, and gateways. As noted above, a wallet is software that runs on a consumer's PC (a term originally coined by the firm CyberCash). A second network computer operates as the merchant's Internet *cash register*. The gateway server is operated by the system operator, a bank, or a transaction processor. Each provides cryptographic capacity for secure transactions. The greatest security threats come from scam artists who can create fake online businesses with the sole purpose of getting consumer credit card information, and from honest merchants who record credit card information on insecure computer systems.

Other Internet commerce payment systems are in various stages of development. Internet check transactions are possible whereby a consumer's actual checking account could be linked to an electronic wallet. Consumers who are accustomed to check floating (taking advantage of the time it takes from the point at which a check is written to the point at which money is actually removed from the checking account) may be dissuaded from using Internet checking systems. Also in development are account-based and token-based *digital cash* systems that create cash-like payment systems allowing immediate and even anonymous payments. Smart cards are an example of token-based payment, and they may require a card reader at the consumer's PC (Crocker and Stevenson, 1998). A smart card is similar to a credit card with embedded electronics and/or a microchip that stores cash in encrypted form to be used with PCs, telephones, ATMs, and other devices with built-in card readers (VNU E Commerce Glossary, 1998).

## 17.4 OTHER INTERNET COMMERCE TECHNICAL CONCERNS

Internet pioneer and enthusiast Vinton Cerf (1998) worries about utopian views of the encroaching virtual world of the Internet. The opportunities for fraud and

deception are there, and anonymous digital cash systems allow for possibilities such as money laundering. Law enforcement agencies are acutely aware of this potential, which has created tension between business and government (see portions of U.S. Department of Commerce, 1998; Canadian Minister of National Revenues, 1998). Minoli and Minoli (1998) is an excellent and thorough text that reviews many key threats to successful Internet commerce systems.

Encryption is a fairly obvious requirement for Internet commerce transactions, but there are other equally significant concerns important to one or both parties in an electronic commerce transaction. Some of these issues are listed in Table 17.2. Access control is especially of concern to would-be providers of Internet commerce; Surveys continue to show that it is one of the barriers to commercial web site implementation by existing businesses.

**TABLE 17.2**
**Fundamental Internet Commerce Security Requirements**

| | |
|---|---|
| Access Control | Determines who may have access to information within a system |
| Authentication | Verifies the identity of communicating parties |
| Privacy | Protects sensitive information from being viewed indiscriminately |
| Integrity | Guarantees that information is not tampered with or altered |
| Non-Repudiation | Provides inability to disavow a transaction |

Source: Zimits and Montaño, 1998

It is worth noting that authentication may be on the verge of moving beyond digitally encrypted signatures. Retinal scans, palm prints, and voice verification are three examples of authentication technologies that might be close to market introduction. Merkow (1998) reviews the state of these technologies in 1998.

The topic of Internet privacy, even if limited to Internet commerce, is one worthy of doctoral dissertations, scholarly books and other works, Congressional hearings, and commercial writers. Beyond the ethics of privacy is the pragmatic concern many consumers have about their online privacy. Research repeatedly demonstrates that concerns about privacy are among the most important barriers to consumer online shopping. The Electronic Frontier Foundation (www.eff.org), one of the most well known and respected Internet advocacy groups, has a repository of privacy-related information online. The Internet Privacy Coalition (www.privacy.org/ipc), an organization devoted to enlightening people about issues of privacy, and the Internet Privacy Information Center (www.epic.org) also have similar information. Readers are encouraged to visit these and other sites for current information and debates related to privacy. Responsible companies know that protecting consumer privacy is in their own best interests; to do otherwise can harm their efforts to conduct business online.

### 17.4.1 SET: Secure Electronic Transaction

On February 1, 1996, MasterCard International and Visa International jointly announced the development of a single technical standard for safeguarding payment card purchases made over open networks such as the Internet. This trademarked standard, the SET Secure Electronic Transaction™ specification, also known as the SET™ specification, includes digital certificates and will provide financial institutions, merchants, and vendors with a safe way of getting the most from the emerging electronic commerce marketplace (see http://www.setco.org/).

A fairly thorough review of what SET is trying to accomplish can be found in Minoli and Minoli (1998, Chapter 6). SET features include:

- Confidentiality of information
- Integrity of data
- Cardholder account authentication
- Merchant authentication
- Interoperability

Interoperability means that for SET to work, it must be hardware and software independent. SET is not the only avenue available for Internet commerce, but its importance is clear given its support by MasterCard and Visa.

### 17.4.2 SSL (Secure Sockets Layer)

SSL is a program layer created by Netscape for managing the security of message transmissions in a network. Netscape's idea is that the programming for keeping messages confidential ought to be contained in a program layer between an application (such as a web browser or HTTP) and the Internet's TCP/IP layers. The sockets part of the term refers to the sockets method of passing between a client and a server program in a network or between program layers in the same computer. Netscape's SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate.

Netscape includes the client part of SSL in the Netscape web browser. If a web site is on a Netscape server, SSL can be enabled and specific web pages can be identified as requiring SSL access. Other servers can be enabled by using Netscape's SSLRef program library which can be downloaded for noncommercial use and licensed for commercial use. Netscape has offered SSL as a proposed protocol to the World Wide Web Consortium (W3C) and the Internet Engineering Task Force (IETF) as a standard security approach for web browsers and servers. In order for SSL to work, both the client and the server must be SSL-enabled (Minoli and Minoli, 1998). For better or worse, Microsoft will have something to say about the adoption of SSL in the world of Internet commerce.

## 17.5 SUMMARY AND CONCLUSIONS

Electronic commerce on the Internet implies the integration of various sophisticated technologies. The primary barriers to the growth of electronic commerce are most likely not of a technical nature. Instead, consumers and businesses both must develop confidence in electronic commerce systems. Both worry about privacy and security, and credit card companies (among others) must be very concerned with issues of liability.

Electronic commerce is literally a new way of doing business. As was the case with innovations that preceded it, some people have rapidly adopted electronic commerce while others are taking a more conservative approach, allowing the technology to prove itself before they jump in. The rapidity with which this might happen should not be underestimated. Many believed that consumers would not accept automatic teller machines for many legitimate reasons, such as a lack of confidence in electronic bookkeeping and concern for their as physical safety while retrieving cash in open and public places. However, the advance of electronic commerce is as inevitable as the drive for lower costs of doing business and better service. This drive is what will push electronic commerce, as an acceptable way of completing transactions, into the next millennium.

## REFERENCES


Canadian Minister of National Revenues (1998). *Report of the Committee on Electronic Commerce*. North York, Ont.: CCH Canadian.

Cerf, V. G. (1998). Stranger than truth or fiction: Fraud, deception, and the Internet. In Tapscott, D., Lowy, A. and Ticoll. D. (eds.), *Blueprint to the digital economy: Creating wealth in the era of e-business* (pp. 371-383). New York : McGraw-Hill.

Cook Report Internet Glossary by Subject (1998). [Online http://www.cookreport.com/cook/glossary.html, as of 1998, November 27].

Crocker, S.D. and Stevenson, R. B. (1998). Paying up: Payment systems for digital commerce. In Leebaert, D. (Ed.), *The Future of the Electronic Marketplace*. Cambridge, Massachusetts: The MIT Press.

Electronic Commerce (1998). *WDVL: The Illustrated Encyclopedia of Web Technology* [Online http://wdvl.com/Internet/Commerce/index.html, as of 1998, November 24].

Howell, G. (1998, November 8). *Electronic Commerce Rev. Proc. WebNet 98 World Confer. of the Assoc. for the Adv. of Comput. in Educ*., Orlando, Florida. Available on CD-ROM.

Insights into Online Advertising: Highlights from "The Online Consumer Survey." (1998, August). Northwood, Ohio: NFO Interactive and Jupiter Communications.

Jordan, P. (1998, November 16). E-Business Report Part 1: E-Business Click On Profit — Electronic commerce reaches beyond simple transactions. It's a whole new way of doing business. *VarBusiness*, 88.

Klopfenstein, B. C. (1997a). Internet economics: An annotated bibliography. *J. Media Econ.*, 11(1), 33-48.

Klopfenstein, B. C. (1997b). Internet economics: Pricing Internet access. *Convergence: J. Res. New Media Technol.*, 3(4), 10-20.

Merkow, M. (1998, June 17). Your Body IS Your PIN! [Online http://www.webreference.com/ecommerce/mm/column3, as of 29 November 1998 Westport, CT: Mecklermedia.

Minoli, D. and Minoli, E. (1998). *Web commerce technology handbook*. New York: McGraw-Hill.

Mougayar, W. (1998). *Opening digital markets: Battle plans and business strategies for Internet commerce* 2nd Ed. New York: McGraw-Hill.

Schnell, S. (1996, November). Codes, Commerce, and National Security: A 10 year Perspective on Cryptography [Online http://www.rsa.com/oracle4/, as of 28 November 1998] Bedford, Massachusetts: RSA Data Security, Inc.

Smedinghoff, T. J. (1998, November 25). Summary of Electronic Commerce and Digital Signature Legislation [Online http://www.mbc.com/ds_sum.html, as of 28 November 1998] Chicago: McBride, Baker & Coles [law firm].

Tapscott, D., Lowy, A. and Ticoll. D., (eds.) (1998). *Blueprint to the digital economy: Creating wealth in the era of e-business*. New York: McGraw-Hill.

Technology Overview (1998). Netscape Security Features Evaluation Guide [Online http://www.netscape.com/products/security/resources/evalguide/tech.html, as of 28 November 1998].

Thing, L. (1998). Encryption and Decryption [Online http://whatis.com/encrypti.htm, as of 28 November 1998] Kingston, New York: whatis®.

United States Department of Commerce (1998, April). *The Emerging Digital Economy.* Washington, D.C.: National Technical Information Service.

VNU E Commerce Glossary (1998). [Online http://www2.vnu.co.uk/e_com/e_07_01.htm, as of 29 November 1998] London: VNU Business Publications.

Zimits, E.C. and Montaño, C. (1998, April). Public Key Infrastructure: Unlocking the Internet's Economic Potential. iWord, 3(2). [Online http://www.iword.com/iword32/istory32.html, as of 28 November 1998].