



---

# Socio-Legal Issues Affecting the Use of Digital Signatures for Secure E-commerce Transactions: A Caribbean Perspective

By Richard M. Escalante, Lecturer/ IT Officer, University of the West Indies, Trinidad

Email: [rescalante@fss.uwi.tt](mailto:rescalante@fss.uwi.tt)

Richard M. Escalante, LL.M (IT and Telecom. Law), is Lecturer / IT Officer at the University of the West Indies, Trinidad. In addition to developing and teaching courses in Information Technology, Public Information Systems, and E-government at the Faculty of Social Sciences, he manages the IT Lab at the Institute of International Relations. His research and publications focus on such themes as E-commerce, E-government, Information Security Policy, and Telecommunications Liberalization in Developing Countries.

---

## Abstract

This article examines the socio-legal issues surrounding the role of digital signatures as an internet technology for secure e-commerce transactions in Caribbean developing countries. It highlights the view that as internet technologies become more affordable in developing countries, the societal changes surrounding digital signatures will be even greater than that of developed countries. Further, the increasing use of internet technology in electronic transactions raises the issue of the legality of these transactions. As in similar developing countries, socio-legal issues in the Caribbean Region will include perception, privacy and authentication, trust and confidence, psychology and culture, internet access and cost, and increased security. Given the absence of adequate legislation on digital signatures in Caribbean countries, the article concludes that for this technology to meet the need for user confidence in secure e-commerce transactions, an information infrastructure must first be put in place before users in Caribbean developing countries can actively engage in secure e-commerce.

**Keywords:** Caribbean, Cryptography, Developing Countries, Digital Signatures, Electronic commerce, Model Law, Perception, Security, Socio-legal Issues.

---

## 1. Introduction

As an internet technology, digital signatures have opened up a virtual Pandora's box in that they have been perceived by users to pose security problems to the continuing development of e-commerce in today's society. Yet much of the hype and anxiety over the security of e-commerce transactions are unfounded since digital signatures can in fact meet the need to build user confidence in secure e-commerce transactions. According to Wiederhold (1999), internet technologies have become sufficiently pervasive in developed countries that they have changed societal interactions. He also postulates that these technologies are also becoming affordable in developing countries with even greater societal

changes. The increasing use of internet technology in electronic transactions has also raised the issue of the legality of these transactions. This article examines the socio-legal issues affecting the use of digital signatures in developing countries, specifically the Caribbean, as these countries seek to support and engage in e-commerce development. It concludes with a recommendation that an information infrastructure must be first developed before digital signatures can be confidently used by both local consumers and businesses in these developing countries.

## **2. The Use of Digital Signatures in E-commerce**

Digital signatures can be any form of an 'electronic seal' agreed to by contracting parties. They are used to authenticate the origin of a document, the identity of a computer or user, the time and date a document was sent and/or signed, and other electronic data. Because digital signatures, like written signatures, are also vulnerable to forgery and fraudulent use, they depend on the PKI system (otherwise known as public-key/private-key or asymmetric encryption) to encrypt the text of a data message, such that the entire message becomes the digital signature. PKI seeks to establish credibility, security, and trust. It also maintains a trustworthy environment via digital certificates issued and certified by Certification Authorities (CAs) known as trusted third parties. Together, digital signatures and PKI are the main internet technologies used for secure e-commerce transactions.

These methods of cryptography play a major role in meeting the need to build user confidence in secure e-commerce transactions and information system security. However, despite there being sufficient Internet technology to meet this need, there is the perception that there is a technological weakness with this technology. It is therefore important to go beyond the technical issues and consider some of the social and legal factors that affect e-commerce transactions using digital signatures.

## **3. Social Factors Affecting Secure E-commerce Transactions**

### **3.1 Perception**

Perception is far from reality. For developed countries, the most consistently perceived technological weakness was security. But although 'security' was ranked as the main barrier to secure e-commerce, it was ranked third in a 2003 Caribbean developing country study (Escalante 2003). In this study, gaining access to the internet and the high expenditure involved in doing so were rated much higher than security considerations. Nonetheless, in both developed and developing countries, consumers were of the perception that deception and risk of fraud and loss constituted one of the most important causes of the secure e-commerce transactions.

### **3.2 Privacy and Authentication**

Issues of privacy and authenticating the identities of the parties involved in e-commerce transactions are also among foremost societal concerns of businesses and consumers. According to the Washington Post, "90 percent of Web sites fail to comply with basic privacy principles." In monetary terms, Forrester Research showed that, "due to consumers' privacy concerns, e-commerce companies lost some \$2.8 billion in the last year."

### **3.3 Trust and Confidence**

Although the Secure Sockets Layer (SSL) protocol is a successful commercial application of Digital Signatures technology used in credit card payments, it only meets half of the requirements of a trusted web site since it is biased in favour of the merchant. Specifically, its limitation is that it only makes use of digital signatures to authenticate the identity of one party to the transaction - the merchant. It does not provide any means by which the merchant can reciprocate the authentication of identity for the potential customer. Consequently, many persons tend to refrain from engaging in e-commerce transactions that require confidential information being sent across the Internet. It also explains why "93% of all online transactions in the United States are still credit card-based" (Tumin, 2002).

### **3.4 Psychology and Culture**

Traditionally, all commerce has depended on trust, and that includes e-commerce which is seen as complementary to traditional commerce. Although trust is of major importance and most people want it, they are wary of using the Internet technologies available for secure e-commerce transactions. Egger (2000) shows that the "difficulty of use and lack of trust with respect to online payment, privacy, and consumer service have been found to constitute a real psychological barrier to e-commerce." This psychological uneasiness could represent a culture that is not yet familiar with secure Internet technologies, but who are willing to 'log on' to Internet web sites to "access information, communicate, and download software." In a very real sense, "as time goes by, the kids who have been brought up doing everything on computers will replace the generations brought up working on paper" (Wilde, 2000).

## **4. Legal Factors Affecting Secure E-commerce Transactions**

### **4.1 The Issue of 'Signature'**

Although the growth of online transactions (particularly credit-based) has relied to some extent on trust, it has however, raised the issue of the legality of electronic transactions. Like e-consumers, legal authorities also equate digital signatures with manual signatures in the traditional contracting contexts. In reality, although the word 'signature' connotes letters and writing, and the term "digital signature" has been conceived in a generic and technology-neutral way, it has been argued that, to apply the term "signature" to what can be performed using (asymmetric) cryptography technology is "simply inappropriate and misleading"(Winn 2001). But although digital signatures have acquired legal status, the legal definition of "digital signatures" is proving very difficult to map onto online security technology functions.

### **4.2 Model Law on Electronic Signatures**

In an attempt to bring additional legal certainty regarding the use of digital signatures, the United Nations Commission on International Trade Law (UNCITRAL) adopted a Model Law on Electronic Signatures in 2001. Based on Article 7 of the UNCITRAL Model Law on Electronic Commerce (1996), it inferred that subject to certain criteria of technical reliability, electronic signatures will be treated as equivalent to hand-written signatures. The Model Law thus adheres to a technology-neutral approach and avoids any bias toward the use of any specific technical product.

However, although the Model Law establishes basic rules of conduct for the parties involved in the electronic signature process, Winn (2001) asserts that 'silence within a statute with regard to technological specifics may rather indicate a decision to leave decisions about the network architecture of electronic commerce to private agreements between the parties and technological standard developing organizations.'

## **5. The Caribbean Situation**

### **5.1 Current Legal Infrastructure**

In any e-commerce transaction, it is important to guarantee that a valid contract has been entered between the parties especially since the contracts are paperless. Hence many developed countries have enacted legislation to this effect. However, in the Commonwealth Caribbean nations, there is an absence of legislation on electronic transactions, and hence assessing the validity of electronic contracts and other electronic documents becomes complicated as existing legislation is inappropriate in dealing with online business transactions. This puts Caribbean businesses at a greater risk than businesses in developed countries when engaging in e-commerce transactions.

### **5.2 Internet Access and Cost**

Although there is emphasis on security in the developed world, other major problems to the expansion of e-commerce in the developing world are the lack of telecommunications and Internet connectivity, as well as access to the necessary hardware and software, all of which are fueled by the associated high financial costs. This was confirmed in a study on Barriers to E-commerce Development (Escalante 2003) which showed that the major barriers were "Financial Cost "and "Access to the Internet," closely

followed by "Security."

### 5.3 Increased Security

Further, since September 11, 2001, issues of authentication have now become extremely important. Many US web sites now only cater for US customers while former international customers, who were previously issued international visa cards, are debarred from engaging in online purchases. This has negative connotations for both local businesses and consumers to buy-in into global e-commerce. Consequently, there is a lack of confidence in digital signatures and a general reluctance to engage in e-commerce.

## 6. A Recommendation

Generally, credit card customers have complete legal protection for online purchases and aren't liable if the card is stolen or used without their authorization (Wolverton 2002). However, the development of new technologies is rarely affected by law. Yet, as societal use of internet technologies for e-commerce transactions becomes increasingly ubiquitous, the issue of the legality of these transactions arises since customers may even be at risk with the use of internet technologies than they are with credit cards online. That is to say, in an e-commerce transaction, both parties usually want to be certain of the (a) origin, receipt and integrity of information they receive, and (b) authenticity and identity of each party (OECD 1998). Thus, the enactment of laws recognizing the use of digital signatures is an exception to the above generality, given that e-commerce needs "standards, regulations, and law to create an environment of certainty, trust and security" (Mann, 2000).

For Caribbean developing countries to actively engage in e-commerce, it is necessary that an information infrastructure be initially developed and supported by the appropriate legislation. This can be achieved by promoting the 'development, expansion and operation of telecommunication networks and services'. However, this is incumbent on the governments in the Caribbean Region to liberalise the telecommunications industry from the monopoly Transnational Corporation (TNC), Cable and Wireless (West Indies) Ltd. Although Caribbean governments are undertaking some initiatives to do so, cooperation with established institutions such as WTO, WIPO and UNCITRAL, should be actively pursued in order to establish model legislation on digital signatures for secure e-commerce transactions.

## References

Albarran, A. B. and Goff, D. H., eds. *Understanding the Web: the social, political, and economic dimensions of the Internet*. Ames: Iowa State University Press, 2000

Candee Wilde (2000). *Legally Binding E-Documents Move Closer To Reality*. Information Week March 6, 2000. Retrieved from [http://www.eoriginal.com/press/articles/030600\\_informationweek.html](http://www.eoriginal.com/press/articles/030600_informationweek.html)

UNCTAD (2003). *E-Commerce and Development Report 2003*. Retrieved from <http://r0.unctad.org/ecommerce/docs/edrO3-en.htm>

Florian N. Egger (2000). *Towards a Model of Trust for E-Commerce System Design*, Retrieved January 2004 from Eindhoven University of Technology, Center for User-System Interaction website <http://www.ip0.tue.nl/homepages/fegger/>

Gio Wiederhold (1999, April). *Trends for the Information Technology Industry*. Retrieved January 2004 from Stanford University web site <http://www-db.stanford.edu/pub/gio/1999/miti.htm>

Hubert Schmitz, John Humphrey, Robin Mansell and Daniel Pare (2001, September). *E-commerce: accelerator of development?*, Policy Briefing Issue 14, Retrieved January 2004 from University of Sussex, Institute of Development Studies web site <http://www.ids.ac.uk/ids/bookshop/briefs/brief14.html>

Jane K. Winn (2001). *The Emperor's New Clothes: The Shocking Truth About Digital Signatures and Internet Commerce 2001*. Retrieved January 2004 from Southern Methodist University web site

<http://faculty.smu.edu/jwinn/shocking-truth.htm>

Mann, et al. (2000, July). Global Electronic Commerce: A Policy Primer. Institute for International Economics, USA: July 18, 2000

OECD (1998). An Inventory of Controls on Cryptography Technologies. Ottawa OECD Conference. Retrieved from [http://ottawaoecdconference.com/english/announcements/ecomm1\\_2.pdf](http://ottawaoecdconference.com/english/announcements/ecomm1_2.pdf)

OECD (1998). An Inventory of Approaches to Authentication and Certification in a Global Networked Society. Ottawa OECD Conference. Retrieved from [http://ottawaoecdconference.com/english/announcements/ecomm1\\_1.pdf](http://ottawaoecdconference.com/english/announcements/ecomm1_1.pdf)

Richard Escalante (2003), "High access costs hinders e-commerce growth" [Electronic version]. Executive TIME Magazine, Mar 2003, p 50 -51. Retrieved from <http://www.mycaribbeannews.com/features/tech0403f.htm>

Tom Melling (n.d.), Digital Signatures Create New Opportunities For Electronic Commerce. Retrieved January 2004 from <http://www.alliance.org/resources/papers/melling.html>

Troy Wolverton (2002), Despite law, few people use e-signatures. CNet News, April 17, 2002. Retrieved January 2004 from <http://news.com.com/2100-1017-884544.html>

Zachary Tumin (2002), The Future Technology of Money. Financial Services Technology Consortium. Retrieved January 2004 from <http://www1.oecd.org/publications/e-book/0302011E.PDF>