International Lawyer

Volume 35 | Number 1 Article 7

2001

The International Chamber of Commerce's GUIDEC Principles: Private-Sector Rules for Digital Signatures

William F. Fox Jr.

The International Chamber of Commerce's GUIDEC Principles: Private-Sector Rules for Digital Signatures

WILLIAM F. FOX, JR.*

I. Introduction

Ensuring the authenticity of signatures is vital to all contracts. It is of special concern in the context of electronic commerce because e-commerce business ventures not only dispense with face-to-face dealings, but also lack the normal verification procedures that one can apply to, say, contracts by facsimile—where at the very least, the recipient of a document can see a specimen signature on a document even if that document is not what might be called an original in classic contract parlance. Without some technological mechanisms and legal principles for assuring the legitimacy of contracting parties' signatures, the legitimacy of contractual relationships in electronic commerce will never be firmly established.

Slightly over two years ago, the International Chamber of Commerce (ICC) promulgated an important set of legal principles for digital signatures, known as the General Usage for International Digitally Ensured Commerce (GUIDEC), that comprise an important step in dealing with parties' signatures and that go a long way toward developing that legitimacy that is so important for the future of electronic commerce generally.[1] This article describes the GUIDEC principles, makes some comparisons between the GUIDEC and other digital signature ventures, and offers some suggestions as to their utilization in various types of electronic contracts.

II. The International Chamber of Commerce and the GUIDEC

A. The ICC's Impact on International Business Transactions

The ICC is a body that is quite familiar to international business practitioners, but may be somewhat obscure for lawyers whose experience is mainly in domestic contracting. The

*Professor Fox teaches at the Columbus School of Law, Catholic University of America in Washington, DC. He is the author of, among other works, *International Commercial Agreements: A Primer on Drafting, Negotiating and Resolving Disputes* (3d ed. 1998). This article is a partial extract from his forthcoming book, *International Electronic Commerce: Resolving the Legal Issues.*

1. *See* INTERNATIONAL CHAMBER OF COMMERCE, GENERAL USAGE FOR INTERNATIONAL DIGITALLY ENSURED COMMERCE (2000), *at* http://www.iccwbo.org/home/guidec/guidec.asp [hereinafter GUIDEC].

ICC has had an enormous impact on a whole host of international business operations. For example, the ICC's Uniform Customs and Practices (UCP) provide the fundamental rules governing such things as international letters of credit and other types of documentary collections.[2] The impact of the UCP is so vast that even banks in the United States who might, arguably, utilize the provisions of Article 5 of the Uniform Commercial Code (Letters of Credit), apply the UCP in international letters of credit. The ICC's promulgation of so-called trade terms, such as F.O.B. (free on board) or C.I.F., through its now famous Incoterms, dominate the field of shipping terms for international sales contracts.[3]

Most recently, the ICC has launched an impressive venture known as the ICC Electronic Commerce Project (ECP).[4] Among other things, the not-yet-completed ECP is developing a set of foundation rules for electronic trade and settlement that are intended to "make trade more efficient by not only adapting rules to new technologies and media such as the Internet, but by taking advantage of these new tools to streamline trade transactions."[5] The ICC recognized, as early as 1997 that the key to successful international electronic commerce is the development of self-regulating business principles backed by a "sound framework of legal jurisdiction."[6] The ECP is broken down into various business sectors such as banking technique and practice, telecommunications and information technologies, financial services and insurance, transport, and international commercial practice.[7] Another document in the making, E-Terms, is an attempt to develop a standard set of definitions for all the factors that enter into electronic transactions. The E-Terms project is currently in what the computer experts might call beta testing.[8]

B. The GUIDEC Principles: Precursors and Technical Background

1. *Some Precursors*

The GUIDEC, as most readers will recognize, was not the first kid on the block. A number of U.S. state legislatures have enacted digital signature statutes.[9] The Commissioners on Uniform State Laws, working with a proposed addition to the Uniform Commercial Code, made a valiant attempt to promulgate U.C.C. Article 2B that is now being adopted in a somewhat piecemeal fashion by various states after the full-blown Article 2B was disavowed by the Commissioners.[10] The United Nations published a Model Law on Electronic Commerce that contains digital signature provisions.[11] The American Bar As-

2. *See* International Chamber of Commerce, Uniform Customs and Practice for Documentary Credit UCP 500 (1994).

3. *See* Incoterms 2000: ICC Official Rules for the Interpretation of Trade Terms (2000).

4. *See* International Chamber of Commerce, The ICC Electronic Commerce Project (2001), *at* http://www.iccwbo.org/home/electronic_commerce/electronic_commerce_project.asp[hereinafter ECP].

5. *Id.*

6. Press Release, International Chamber of Commerce, Making Rules for Electronic Commerce (Nov. 14, 1997), *available at* http://www.iccwbo.org/home/news_archives/1997/making_rules.asp [hereinafter Making Rules].

7. ECP, *supra* note 4.

8. *Id.*

9. *See, e.g.*, Utah Digital Signature Act, Utah Code Ann. § 46-3-1001 (2000).

10. *See, e.g.*, U.C.C. art. 2B (Proposed Draft 1998).

11. *See UNCITRAL Model Law on Electronic Commerce with Guide to Enactment*, U.N. GAOR, 51st Sess., Annex I, Supp. No. 17, U.N. Doc. A/51/17 (1996), *reprinted in* 36 I.L.M. 197 (1997), *available at* http://www.uncitral.org/english/texts/electcom/ml-ecomm.htm [hereinafter *Model Law*].

sociation has ventured into the fray by way of its Digital Signature Guidelines.[12] All these developments seek to fashion generally accepted principles for authenticating documents through the device of a digital signature. By and large, they attempt to do so without prescribing a particular technology for authentication. GUIDEC builds on all of these precursors.

When beginners venture into the realm of electronic commerce, things often appear murky, unsettled, and far beyond the powers of mere mortals to comprehend. In truth, electronic commerce is simply ordinary commercial dealings based on a new form of communication—the Internet. There are a number of existing electronically based practices that work quite well in ensuring the safety and security of commercial communication and practices. For example, international banks have long exchanged highly secure messages that transfer money from bank to bank under principles and techniques promulgated by the Society for Worldwide Interbank Financial Telecommunications (SWIFT).[13] Some companies have developed "virtual private Internets," which are electronic communications systems that exist as a closed, private system within the public Internet community.[14] These systems have a relatively strong track record. But the more pressing problem is how to develop sound, reliable, and legally enforceable techniques for transactions between merchants and consumers (so-called B2C commerce) or between merchants (so-called B2B commerce) that make electronic transactions as safe and legitimate as conventional paper-based transactions. As noted above, digital signatures lie at the heart of the problem.

2. *Some Technical Background*

There are a number of ways to deal with digital signatures as a matter of computer technology. A simple e-mail where the writer of the e-mail simply types his name is a type of digital signature. The problem with this kind of signature is how to verify that the originator of the e-mail is in fact the individual whose name is typed at the bottom of the e-mail. Most observers do not consider the mere receipt of an e-mail to be a sufficiently reliable guaranty of identity to be used as the basis for a contractual relationship.

A second possibility is to simply have the two contracting parties agree on a password that they believe is known only to the two of them to properly identify and confirm that the person with whom I'm communicating is the person with whom I wish to contract. In other words, I may exchange e-mails with someone and append the numbers "123" to my typed name. If I have made previous arrangements with the other person as to the nature of the password, my recipient may be wholly satisfied that he or she is hearing directly from me when my name includes the digits "123."

But once again, this does not really suffice because electronic commerce cannot be based either on extraordinarily loose and insecure e-mail where names are merely typed at the end of the communication. Businesses cannot be burdened with the need to exchange earlier communications that establish passwords known only to the two parties. At its optimum, electronic commerce should be a system where two persons who are complete strangers can complete valid transactions with only one or two exchanges of messages. Moreover, these messages should be subject to generally well-known and accepted secrecy devices so

12. AMERICAN BAR ASSOCIATION, DIGITAL SIGNATURE GUIDELINES, *available at* http://www.abanet.org/scitech/ec/isc/dsgfree.html (last visited Feb. 16, 2001).

13. SWIFT, http://www.swift.com (last visited Feb. 16, 2001).

14. See the discussion in *Responding to the Legal Obstacles to Electronic Commerce in Latin America*, 17 ARIZ. J. INT'L & COMP. L. 5, 9 (2000).

that there is simply no doubt that the communications are between the two actual contracting parties.

To this end, electronic commerce specialists have enlisted a long-understood set of principles and practices that involve code breaking and encryption to resolve problems of identity. While avoiding a long digression into the different forms of cryptography, a short explanation is in order to set the stage for a discussion of the GUIDEC. Cryptography has been defined as the "art and science of keeping messages secure."[15] It has long been used as a device for protecting matters of national security and exchanging messages between, say, military forces in the field. The tensions that give rise to cryptography are simple: two people wish to exchange a message and wish to conceal the terms of that message from third parties.

Basically, cryptography involves a person sending a message in so-called plaintext who encrypts (i.e., scrambles) that message so that only the intended receiver of the message can decrypt (unscramble) the text of the message. Encryption involves the use of keys by which the scrambling takes place. In encryption there are always two keys—a public key that is typically distributed among a large number of persons and a private key that is known only to the specific individuals who are attempting to communicate with each other.[16] For our purposes, suffice it to say that there are many techniques and technologies that might be used to encrypt commercial messages.

Some digital signature statutes, most notably Utah's, require a particular type of cryptography to be utilized by the parties. But most proponents of electronic commerce take just the opposite approach and urge the development of rules that permit businesses "to choose the cryptographic systems that best suit their needs" and that avoid "any mandatory system based on a specific technology."[17] This is essentially the road taken by the GUIDEC.

C. The GUIDEC

1. *Underlying Goals and Concepts*

The ICC developed the GUIDEC by setting up a multi-disciplinary team of experts from a number of different countries[18] who reviewed a number of precursors (the UN venture and the ABA's pronouncements) to come up with the final GUIDEC text. The working party saw the key problem as one involving the lack of physical signatures in electronic messages.[19] But there were other goals: electronic commerce needed some commonly accepted terms and definitions and needed to be established in a context that would guarantee acceptance by the entire international business community.

Probably the most important precursor of the GUIDEC, and the statement of legal principles on which GUIDEC expressly builds, is the UNCITRAL Model Law on Elec-

15. Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C 1 (2d ed. 1996). *See generally* the general discussion in Cryptography's Role in Securing the Information Society (Kenneth W. Dam & Herbert S. Lin, eds. 1996).

16. F.L. Bauer, Decrypted Secrets: Methods and Maxims of Cryptology 25–26 (1997).

17. Alliance for Global Business, A Global Action Plan for Electronic Commerce 25 (2d ed., 1999). This report includes a great deal of the discussion set out in OECD's Cryptography Policy: The Guidelines and the Issues (1997), *available at* http://www.oece.org/dsti/sti/it/secur/prod/GD97-204.htm.

18. Mr. William Kennair, a notary in the United Kingdom, served as the Chair of the Information Security Working Party.

19. GUIDEC, *supra* note 1.

tronic Commerce.[20] The GUIDEC working party found the Model Law, promulgated by UNCITRAL in 1997, to be incomplete and insufficient in its treatment of digital signatures. The Model Law, for example, does not specify what method of signing a message might be appropriate under particular circumstances. Its express provision on digital signatures simply defines signature as any symbol executed or adopted by a party with present intention to authenticate a writing.[21] While the commentary deals, somewhat more elaborately, with the digital signature phenomenon, the commentary merely provides that the focus should be on a party's "intention to authenticate" rather than emphasizing the precise manner in which a symbol is affixed to the document.

Note that while the Model Law is salutary in avoiding the adoption of any particular technology, it is so broad that even an "X" placed at the end of an e-mail message would suffice as a legally valid and binding digital signature. The GUIDEC working party simply did not find this an acceptable practice for the international business community. The GUIDEC is much more explicit on the nature of the signature, the means by which a signature is ensured or authenticated, because, in the view of the working party, "digitally authenticated or ensured messages [must] retain their non-repudiable characteristics for evidentiary purposes."[22]

The GUIDEC text is divided into several chapters including a great deal of discussion of electronic commerce generally and of existing laws. As a threshold matter, the GUIDEC is applicable only to what the Uniform Commercial Code refers to as trade between merchants or B2B commerce. As the GUIDEC preface explains: the GUIDEC "assumes practices in which transacting parties are expert commercial actors, operating under the lex mercatoria. The [GUIDEC] does not attempt to define rights and responsibilities for transactions involving consumers."[23]

The GUIDEC sets out a glossary of terms, a section on best practices, and a section on certification. The policies that underlie the GUIDEC are straightforward and easily understood. They include a goal of enhancing "the ability of the international business community to execute secure digital transactions" and the establishment of "legal principles that promote trustworthy and reliable digital ensuring and certification practices."[24]

The GUIDEC places virtually all of its emphasis on open Internet-based commerce in systems that "offer access and communication between multiple parties not contractually obligated to systems managers [i.e., closed proprietary systems] thereby exposing businesses to trading partners with whom those businesses have no prior relationship."[25] In reaching

20. *Model Law*, *supra* note 11, at 70.

21. *Id.* art. 7.

22. GUIDEC, *supra* note 1, V.1.

23. *Id.* I.2.

24. *Id.* These are the first two principles. The other principles, somewhat redundant, are:

> (3) to encourage the development of trustworthy ensuring and certification systems,
> (4) to protect users of the digital information infrastructure from fraud and errors,
> (5) to balance ensuring and certification technologies with existing policies, laws, customs, and practices,
> (6) to define and clarify the duties of participants in the emerging ensuring and certification system, and
> (7) to foster global awareness of developments in ensuring and certification technology and its relationship to secure electronic commerce.

Id.

25. *Id.* II.5. The GUIDEC defines closed networks as those in which specific business entities "control physical access to the system, conduct communications according to written and approved procedures, maintain record systems designed to facilitate quality assurance, and create legal obligations between users and the organization responsible for operating the system." *Id.* II.2.

its goals, the GUIDEC recognizes the basic encryption techniques of public key and private key—resulting in what other promulgations call a digital signature and what the GUIDEC refers to as "ensuring a message." As the GUIDEC notes: "Because an ensured message is difficult to forge, its use binds the signatory, precluding a later repudiation of the message . . . [and] forms the basis for forming legally binding contracts . . . since [the ensured message] can provide electronically the same forensic effect a signed paper message provides."[26]

One of the primary contributions of the GUIDEC, as noted, is the development of a standard vocabulary for dealing with electronic signatures. Within the definitional structure, perhaps the central contribution is the use of the term ensure or ensuring a message in place of the more common digital signature. The drafters concluded that because of the differences in United States and European definitions of authenticate[27] and the concept of digitally signing a message, a new term was justified. In the GUIDEC glossary ensuring a message, means "(a) the ensurer had contact with the message and (b) the message has been preserved intact since it was ensured."[28] There are many other definitions in the GUIDEC glossary, but these terms are better understood in the context of the GUIDEC's best practices requirements.

The primary contribution of the GUIDEC is the development of some salutary principles for electronic contracts grouped under the best practices heading. Best practices is divided into several parts: ensuring a message and the legal significance of such ensuring; appropriate practices for ensuring a message; the scope of an ensured message; safeguarding an ensuring device; certification and the effect of a valid certificate; and suspension or revocation of public key certificates.

As the GUIDEC notes: a message is ensured as a factual matter if there is evidence to indicate (1) the identity of the ensurer; and (2) that the message has not been altered since it was ensured.[29] Moreover, a recipient or other interested person is required to attribute an ensured message to the person who actually ensured it. This provision has the effect of stability and predictability in that attribution is virtually automatic once a message is known to have been ensured. In the case of the use of an agent, the principal will be bound "if, under applicable law, the agent had sufficient authority to ensure the message."[30] Clearly, this provision contemplates a business executive permitting a secretary to transmit a binding ensured message. Finally, the person who creates an ensured message must, within the context of that message, "clearly indicate what is being ensured."[31]

The GUIDEC does not insist on any particular technology or protocol for ensuring messages. The best practices text merely provides: "An ensurer must ensure a message by

26. *Id.* III.3.

27. In the United States, the term authenticate seems to be used merely to associate a person with a message while in Europe authenticate has associations with the actual verification of a signature.

28. GUIDEC, *supra* note 1, VI.1.

29. *Id.* VII.1.

30. *Id.* VII.3.

31. *Id.* VII.5. This point may be somewhat obscure but is nonetheless important. As the GUIDEC commentary explains: "Since ensuring a message does not apply to alterations of the message, a person receiving the ensured message must determine whether the message arrives intact. Such a determination is only possible if the message has been clearly delimited and linked to when it was ensured." Because electronic communications are not necessarily standard as to margins, formatting, and the like, "[t]he parties should agree, in specifying the form for their messages, which variations are to be considered significant." *Id.* VII.5.

a means appropriate under the circumstances."[32] At first glance, this provision might be seen to contain the same seeds of ambiguity as the UNCITRAL Model Law. But the real meat in the GUIDEC is contained in the next section of best practices under the heading "Certification."

Ensured messages are transmitted only under the auspices of a certificate that is defined as "a message ensured by a person, which message attests to the accuracy of facts material to the legal efficacy of the act of another person."[33] The basic concept of certificate under the GUIDEC is not terribly different from the notion of a certificate that might be issued by, say, a notary public, who acts to authenticate a particular document. But in the specific context of electronic commerce, the notion of certificate mainly contemplates a public key certificate issued by an appropriate certifier whose authority to issue such certificates is carefully policed.

The concept of certification is vital to the GUIDEC. As the working group explains:

> The use of public key cryptography for digital signature purposes require that a trusted third party establish that holders of public keys are indeed who they purport to be. Without a trusted third party certifying that a given individual is in fact the holder of a public key, it is impossible for other transacting parties on the network to know for certain that the holder of the public key is not an imposter.[34]

As the GUIDEC explains further: "This third party, known in the GUIDEC as a Certifier, will form the trust backbone for all types of commercial and non-commercial transactions taking place over open networks."[35]

To begin with, a certifier must use "only technologically reliable information systems and processes, and trustworthy personnel in issuing a certificate."[36] A technologically reliable certificate is one that is "reasonably secure from intrusion and misuse;" and provides "a reasonable level of availability, reliability, and correct operation."[37] The certifier commits to using only "technologically reliable information systems and processes, and trustworthy personnel in issuing a certificate."[38] As the GUIDEC commentary points out, "[t]he trustworthiness of a certifier is central to the whole concept of certification."[39]

To become a certifier is not necessarily easy or inexpensive. For example, a certifier "must have financial resources sufficient to conduct its business and bear the reasonable risks resulting from the certificates it issues."[40] A certifier must keep detailed records.[41] A certifier must notify affected persons of any problems with a particular certificate.[42] And certificates are subject to suspension or revocation.[43] While these principles are somewhat broadly stated, the GUIDEC envisions the development of additional laws and regulations that will "prescribe clear rules and liabilities for certifiers."[44]

32. *Id.* VII.4.
33. *Id.* VI. 2.
34. *Id.* Preface.
35. *Id.*
36. *Id.* VIII.3.
37. *Id.* VI.16.
38. *Id.* VIII.3.
39. *Id.* VIII.3, commentary.
40. *Id.* VIII.5.
41. *Id.* VIII.6.
42. *Id.* VIII.4.
43. *Id.* VIII.8, .9, .10, .11.
44. *Id.* III.4.

III. Some Brief Predictions and Prognostications

The GUIDEC is an excellent beginning to one of the thorniest problems in electronic commerce. Until and unless merchants can approach electronic commerce with the same understandings of stability, predictability, and security that they now enjoy using paper contracts, the Internet will never be the earth-shattering development envisioned by so many recent commentators. Perhaps the fundamental premise of the GUIDEC is its strongest advantage: in international business it is generally much better to permit the merchants to make—and abide by—their own rules rather than having meddlesome—and often inexpert—governmental bodies establish basic principles of conduct. This point is well borne out by the success of the UCP and Incoterms. In this respect, the prestige of the ICC will be instrumental in adoption of the GUIDEC by international merchants.

In this author's opinion, it is also vital that rules governing digital signature be truly international in scope, reflecting the profound international consequences of electronic commerce. A "Balkanization" of electronic commerce rules will inhibit e-commerce for many years in the future. The GUIDEC is truly international.

But the GUIDEC has not yet been universally accepted. Currently its provisions conflict in many respects with other similar sets of rules, each of which has its own proponents and detractors. Further, it is highly doubtful whether individual national governments will be able to keep their hands off such fundamental principles of international commercial practice. The UCP and the Incoterms function mainly because they are relatively obscure rules of conduct that do not have terribly important consequences for national governments. That may not be the case for digital signatures. Finally, it may have been a mistake for the GUIDEC to restrict itself only to B2B commerce. Does it make sense to have one set of digital signature rules solely between merchants and conceivably a different (and potentially conflicting) set of rules for trade between merchants and consumers? This author believes that solid, comprehensible, and enforceable principles can be worked out for both B2B and B2C commerce within the same rules structure. If various governments and other bodies develop wholly different rules for consumer transactions, the GUIDEC may never be fully accepted.

At the time of this writing, the jury is still out on the GUIDEC. Whether the GUIDEC succeeds or fails will only be apparent with the passage of time.