

Electronic Signature Comparison Between French & U.S. Law

By Laurence Birnbaum-Sarcy*

And

Florence Darques*

International Business Law Journal, April 2001

The international interconnection created by the Internet, and its impact on the global economy, has prompted international and domestic legislative effort to provide a legal framework for electronic commerce that serve the twin goals of encouraging electronic commerce and protecting on-line customers. To meet these challenges, France and the United States have enacted legislation on electronic signatures which they hope will achieve both goals not just domestically, but internationally as well. Both laws are designed to grant electronic contracts the same status as paper contracts.

France

On March 13, 2000, the French Parliament passed the "Loi portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique", Law No. 2000-230 (the "Loi"),¹ which became effective immediately. However, the draft of the implementing statute of the Loi (the "Décret"), which describes the conditions under which the Loi will apply, has been submitted to public debate. It is presently before the Conseil D'Etat and is scheduled to be adopted in the next few months.² As a member of the European Union ("E.U."), France will also have to conform, in the next few years, to the Directives of the European Parliament and Council on this subject.³

United States

In the United States, by contrast, on June 30, 2000, President Clinton signed the Electronic Signatures in Global and National Commerce Act ("E-Sign");⁴ most of its provisions became effective on October 1, 2000. Among the major concerns of E-Sign is how it will affect existing state law electronic signature requirements. E-Sign was enacted, in part, to promote consistency and certainty regarding the use of electronic signatures in the United States.⁵ At the state level, the National Conference of Commissioners on Uniform State Laws also approved the draft of the Uniform Electronic Transactions Act ("UETA")⁶ the application of which is specifically recognized in E-Sign.⁷ Thus far, however, fewer than half of the states (excluding New York) have enacted the UETA,⁸ and some have adopted it with significant amendments, which may counteract the effort to unify the legislation on this matter.

For example, New York has an electronic signature requirement which is set forth in the Electronic Signatures and Records Act ("ESRA").⁹ It is not clear what would happen to ESRA if UETA were adopted in New York. It is equally unclear whether E-Sign preempts ESRA.

Definition of Signature

In France and the United States, a signature has traditionally been defined as a writing or other mark which served to identify the person making the mark, which is placed on a document for the purpose of authenticating the document or giving it legal effect.¹⁰ As a legal matter, a signature also expresses the intent of the signatory to be bound by the terms of the contract.

In France and the United States, an electronic signature serves the same purpose, but may take different forms such as electronic sounds, symbols, or processes attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.¹¹ Therefore, as commentators in the field note, an electronic signature may be a simple one such as a name at the bottom of an email message or a more complex and secure one involving biometric technologies such as fingerprint or retinal scans.¹²

As is the case with handwritten signatures, fraud is a major concern with electronic signatures. Each of the countries recognizes authentication, certification and traditional forms of identification as legitimate protections against fraud.

Both France and the United States recognize authentication as a means to limit fraud. Authentication may also be used to provide further security to the electronic signature by imposing certain conditions before an electronic signature is recognized as valid. For example, authentication methods may include magnetic stripe cards with personal identification numbers, user names and passwords, public key cryptology, writing tablets with electronic pens, and even smart cards that generate a unique access code every few seconds.¹³

Certification is yet another method both countries use to limit fraud. Certification calls for a trusted third party, after verifying the data associated to the signatory, to guarantee the authenticity of the signature.¹⁴

Neither country has replaced the traditional methods of verification such as notarization and acknowledgment since both methods limit the risk of fraud. Indeed, both countries encourage traditional methods if the technology permits the use of those methods.¹⁵

Article 1316 of the French Civil Code

The Loi provides both a definition of an electronic signature and a prerequisite for its effectiveness. The recently enacted Article 1316-1 of the French Civil Code requires that the signatory be positively identified before the Code will recognize the validity of an electronic agreement.¹⁶ Once that signature is recognized as emanating from an identified signatory, then the electronic agreement is recognized as having the same force, validity and effect as its paper counterpart.¹⁷

Under French law, apart from identifying its signatory, a valid signature guarantees that the signatory personally signed the document and further acknowledges his association with the content of the document.¹⁸ Article 1316-4 of the Civil Code states that a signature manifests the intent to be bound contractually.¹⁹

It is essential that the process of signing by electronic means be reliable. In fact, it is the use of reliable methods of identification that will guarantee the link between the signature and the document itself.²⁰ The process of identification under Article 1316-4 of the Civil Code is presumed reliable at the time the electronic signature is made if the process satisfies the conditions set forth by further implementing legislation.²¹

E-Sign

E-Sign's approach does not impose any conditions of identification for the validity and effect of an electronic signature to be recognized. It simply provides, in Section 101(a), that a signature, contract or other record relating to a transaction pertaining to interstate or foreign commerce may not be denied legal effect, validity or enforceability solely because it is in electronic form.²² Section 101 also provides that the use of an electronic contract should not be denied legal effect because an electronic record or signature was used in its formation.²³

E-Sign does not impose any conditions of identification for an electronic signature to be valid, nor does it provide that the electronic signature manifests the intent to be bound. E-Sign simply puts electronic signatures on the same footing as handwritten signatures without defining their purport.

Differences Between French and United States law

At present, several key differences exist between French and United States law. For an electronic signature to be valid under French law, the identification process needs to be satisfied. In order to do so, French law seems to imply that certification should be used. E-Sign, however, does not make any mention of certification. It does, however, address authentication in the context of the limits on federal preemption of state law.²⁴ Authentication may be used in the future by states as an additional tool to impose more security by imposing additional conditions to validate a signature.

The French Décret and the European Directive dated December 13, 1999 base the validity of the electronic signature and contract on certification.²⁵ They define a certificate as an electronic guarantee which links signature-verification data to a person and confirms the identity of that person.²⁶ The legislation contemplates that the certification provider will deliver the guarantee after verifying pertinent data.²⁷ The Décret outlines the conditions by which certificates are delivered and certificate providers are authorized to perform these services.²⁸ Under the Décret, the evaluation of the methods used to certify and the accreditation of the certificate providers, who are trusted third parties, are ultimately performed by the Office of the Prime Minister.²⁹ However, Article 4 of the Décret also permits this scrutiny to be performed by an organization selected by another Member State of the European Union.³⁰

E-Sign and the UETA do not even mention certification; ESRA, however, does provide for the use of certification.³¹ ESRA defines certificate authorities as trusted third parties or government entities who, through the use of cryptology, vouch for the authenticity of the individual or of the system in question by issuing certificates that are used for verification of electronic signatures produced by a corresponding coding device held by the parties.³² Here, through the use of certification, the electronic signature becomes a digital one.

The differences between France and the United States are quite salient on the issue of certification. On the one hand, French legislation requires certification to validate an electronic signature. In that regard, France has started to organize the framework in which electronic signatures are to operate. United States law, on the other hand, is silent on the issue of certification. Some commentators believe that silence on the issue of certification authorizes its use. Certification authorities in France may well ultimately be controlled by the government while, in the United States, certification authorities are likely to be private companies³³ such as Digital Signature Trust³⁴ or VeriSign.³⁵

Authentication may be the tool by which state legislation may impose conditions for a signature to be recognized as equivalent to a handwritten one. Section 102 of E-Sign allows states to adopt statutes regarding authentication of electronic signatures. The issue of authentication is not addressed as such in the French Loi. The European Directive of December 13, 1999 which France, as a Member State of the European Union, will have to implement in its law within the next few years, refers to authentication in relation to services allowing data authentication and the need to harmonize authentication methods.³⁶

E-Sign adapts traditional methods of verification such as notarization and acknowledgment of a document by a third party. It allows these verification methods to be accomplished electronically.³⁷ The presence of the notary is not necessary for the verification to be valid. E-Sign specifies that if a rule of law requires a signature to be notarized or verified, that requirement is satisfied if the electronic signature of the person authorized to perform those acts is attached to, or logically associated with, the signature or record.³⁸ The traditional concept of notarization is preserved but it can now be performed electronically.

The French law also deals with the traditional concept of notarization when it distinguishes the "acte sous seing privé" from the "acte authentique".³⁹ The "actes sous seing privé" are agreements which are signed by the parties to the contract without third party acknowledgment.⁴⁰ The "actes authentiques" must receive the acknowledgment of public officers.⁴¹ The Loi modifies Article 1317 of the French Civil Code, and provides for the acknowledgment by a public official to be made electronically.⁴² Therefore, similar to a notarization in the United States, the obligation to have certain documents signed or "authenticated" by a third person persists, but the performance of such acknowledgment may be conducted electronically and without the presence of the official. The French

Loi specifies that such an acknowledgment may be effectuated electronically if it is executed and preserved according to the conditions set by further implementing legislation.⁴³

Consumer Protection

In her address before the National Assembly, Elisabeth Guigou, the then Minister of Justice, stressed that the development of electronic commerce is premised on the need for service providers and consumers to trust the system.⁴⁴ The Conseil D'Etat in its report presented to the National Assembly on July 2, 1998, dedicates an entire chapter to electronic transactions and consumer protection.⁴⁵ The Loi and Décret, however, do not specifically mention the consumer. Nevertheless, it is implicit that certification requirements are intended to protect the consumer.

E-Sign also contains a number of consumer protection provisions. First, E-Sign provides that if the law relating to the contract requires that information be disclosed in writing to the consumer, it may be disclosed in electronic form only if the consumer consents.⁴⁶ Second, the consumer has a right to withdraw his consent to receive records in electronic form.⁴⁷ Third, the consumer must be informed of his right and the procedures for exercising his rights prior to consenting.⁴⁸ Fourth, he must be advised of the conditions, consequences and even the fees resulting from his withdrawal of his consent.⁴⁹

United States State Legislative Actions

In the United States, several states have enacted electronic signature statutes and have developed pilot programs in collaboration with the private sector to further promote electronic transactions. The areas covered by these statutes will most likely not conflict with E-Sign which excluded from its scope of application a number of areas usually reserved to state law.⁵⁰ However, in states such as New York, the legislative effort may be curtailed due to some of the far-reaching implications of the provisions of its statute.

New York's ESRA provides a detailed framework in which electronic signatures and contracts are to operate. More importantly, ESRA creates an authority with broad powers, the Office for Technology, which is the ultimate body that will determine which technology is acceptable for the electronic environment.⁵¹

Colorado has also enacted recent legislation in the area with its launch of an initiative to enable the state's civil courts to accept legal filings electronically in civil, probate, water and domestic relations cases.⁵² Other types of cases including criminal cases will be addressed in the coming year. E-filing, in Colorado, began on July 31, 2000 and is expected to extend statewide by January 1, 2001.⁵³ Although, this initiative aims at electronic filings for judicial proceedings and not contract execution, it shows that states may legislate to promote electronic means for certain procedures and perhaps in the future, for certain types of contracts.

Another interesting case study is Florida, which, in addition to recently enacting the UETA, also became the first state in the nation to recognize a fully electronic mortgage loan closing. The real estate transaction was developed by a team of mortgage industry technology leaders and the Broward County Recorder's Office (Florida).⁵⁴ On the close of business on July 24, 2000 all closing documents were signed and the deed and mortgage were transmitted to the Recorder's Office, entirely by electronic means. The loan was closed, recorded and delivered to the secondary mortgage market in less than three hours.⁵⁵

Business and technological challenges

The challenge facing governments regarding the use of electronic signatures and records is the need to develop a secure system while providing a framework flexible enough to enable technology to guide the development of electronic commerce. Technology neutrality is either implied or specifically mentioned under both the French and the United States systems.

E-Sign specifically requires that, if state legislation adopts alternative procedures for use or acceptance of electronic signatures and records, they may not require or accord greater legal status to

a specific technology for receiving, communicating or authenticating electronic records or electronic signatures.⁵⁶ New York legislation also stresses this point in its introduction to the ESRA in which it states its intent to be sufficiently flexible to facilitate and promote the use of technological advancements.⁵⁷ Notwithstanding the introduction, some commentators believe that ESRA is too technology specific, and thus, will ultimately be preempted by E-Sign.

In France, the Décret attempts to first answer the need to provide a secure system by establishing strictly controlled certifications. Yet, when submitting the project to the public, at least one legislator expressed his concern about not creating an overly burdensome system.⁵⁸

Security

The conclusion of commercial transactions without the physical presence of one of the parties is not new. For years, powers of attorney or facsimile signatures have replaced original handwritten signatures in business deals. The nature of an electronic signature, however, is to provide for an entire transaction to be concluded without the physical presence of any party or agent. Many commentators believe that this creates a heightened risk of fraud for those involved in commercial transactions and, in particular, for the consumer, who may engage in a business venture from his home.

Legislation in France concerning certification aims at preventing fraud and tackles the issue of forgery of signatures. Article 6 (2)(g) of the Décret requires certificate providers to develop means to prevent forgery of certificates.⁵⁹ Another level of control is further envisioned by the Décret through accreditation and control of the certificate providers by the government.⁶⁰ Section 105(b) of E-Sign requires the United States Secretary of Commerce to issue a report to Congress, within 12 months after enactment of E-Sign, to determine whether the absence of an electronic consent process would increase the incidence of fraud against consumers.⁶¹

E-Sign and the Loi represent more than just a symbolic change in the law regarding electronic signatures. Yet, if they are the guiding light, most consumers do not have the necessary technological equipment to complete transactions via electronic means. Pens and paper, as low technology as they may be, are not yet obsolete.

Laurence Birnbaum-Sarcy is now Manager in the Forensic and Litigation Services, KPMG LLP, New York and may be reached by telephone at: 212 872-5808 or by e-mail at: Lbirnbaumsarcy@kpmg.com

Florence Darques is now associate in the Pavia and Harcourt law firm in New York and can be contacted by telephone in: 212-980-3500 or by e-mail at the following address: fDarques@pavialaw.com

They are former associates in the New York office of Salans international law firm and they wish to thank Christiane Féral-Schuhl, a partner in the firm's Paris Office, and Jerome Walker, a partner in the firm's New York Office, for reviewing the article.

The contents of this article are the author's own and do not necessarily represent the positions of KPMG.

Footnotes

1. Law adapting evidence to information technology and relating to electronic signature, Law No. 2000-230 of March 13, 2000, J.O. 62, March 14, 2000, p.3968, JCP 2000, III, 20 259.

2. Projet de Décret d'application prévu par la Loi du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique(visited Feb.09,2001) <http://www.internet.gouv.fr/francais/textesref/pagsi2/signelect-projetdecree/projetdecree.htm>.

3. See, e.g., the Directive 2000 O.J.(L 13)17 (setting forth the Community framework for electronic signatures).
4. Pub. L. No. 106-229, 114 Stat. 464 (2000).
5. See Albert Gidari and John Morgan, *Internet Law and Policy Forum, Update: Survey of State Electronic & Digital Signature Legislative Initiatives* (last modified Sep.24, 2000)<http://www.ilpf.org/digsig/update.htm>.
6. The National Conference of Commissioners on Uniform State Laws, Uniform Electronic Transactions Act (UETA) (July 23-30, 1999)<http://www.law.upenn.edu/bll/ulc/uecicta/uetast84.htm>.
7. See E-Sign § 102(a)(1).
8. See Global E-Commerce Law, UETA State-by-State Comparison Table (last modified Nov. 6, 2000)<http://www.bmck.com/ecommerce/uetacomp.htm>.
9. Electronic Signatures and Records Act (ESRA), 9 N.Y.C.R.R. Part 540 (2000).
10. See Black's Law Dictionary 1381 (6th ed. 1990); Law No. 2000-230, supra note 1, at article 4 (C. Civ., New art. 1316-4).
11. See E-Sign § 106(5); UETA § 2(8); The Directive 2000 O.J.(L 13)14.
12. See Daniel J. Greenwood and Ray A. Campbell, *Electronic Commerce Legislation: From Written on Paper and Signed in Ink to Electronic Records and Online Authentication*, 53 Bus. Law. 307(1997)(also found at <http://www.civics.com/resume.htm#Publications>).
13. *Id.* at 2.
14. The Décret art. 2 (7).
15. See E-Sign § 101(g); Law No. 2000-230, supra note 1, at art.4 (C. Civ., New art.1316-4).
16. Law No. 2000-230, supra note 1, at art.1 (C. Civ., New art.1316-1).
17. *Id.* at arts. 1, 3 (C.Civ., New art. 1316-3).
18. *Id.* at art. 4 (C.Civ., New art. 1316-4).
19. *Id.*
20. *Id.*
21. *Id.*
22. See E-Sign § 101(a)(1).
23. *Id.*
24. See E-Sign § 102(a)(2)(ii).
25. See generally the Directive 2000 O.J.(L 13); the Décret.
26. See the Directive 2000 O.J.(L 13)14, 19; the Décret
27. See generally the Décret.

28. See generally the Décret.
29. The Décret art.4, 5.
30. The Décret art.4.
31. See generally ESRA.
32. See ESRA § 540.2(b).
33. See *Certification Authority Services and Policies*, ILPF, Appendix 4 (visited Oct.03,2000) <http://www.ilpf.org/work/ca/app4.htm>.
34. Digital Signature Trust Co. (visited Nov.02, 2000) <http://www.digsigtrust.com/>.
35. Verisign (visited Nov.02, 2000) <http://www.verisign.com/>.
36. The Directive 2000 O.J.(L 13)13.
37. See E-Sign § 101(g).
38. *Id.*
39. See CHRISTIANE FERAL-SCHUHL, *Cyberdroit, Le Droit à l'Epreuve de l'Internet* (Daloz, 2nd Ed. 2000), and in particular Chapter 7, *L'Internet et la Sécurité*.
40. C. Civ., art. 1322.
41. C. Civ., art. 1317.
42. Law No. 2000-230, supra note 1, at art. 2 (C. Civ., New art.1317).
43. *Id.*
44. See Elisabeth Guigou, Garde des Sceaux, Ministre de la Justice, *Intervention devant l'Assemblée Nationale*, (Feb. 29, 2000) <http://www.justice.gouv.fr/discours/d290200.html>.
45. Conseil D'Etat, Section du rapport et des études, *Internet et les réseaux numériques* (Jul.2, 1998) <http://www.internet.gouv.fr.francais/textesref/rapce98/accueil.htm>.
46. See E-Sign § 101(c)(1)(A).
47. *Id.*
48. *Id.* at 101(c)(1)(B)(i)(I).
49. *Id.* at 101(c)(1)(B)(i)(II).
50. See E-Sign § 103.
51. See ESRA § 540.3.
52. See Justice Link News Room, Press Release, *Colorado Courts First in Nation to Offer Statewide E-Filing in Civil and Domestic Cases* (Aug.7, 2000) <http://www.justicelink.com/>.
53. *Id.*

54. See eOriginal Press Release, *eOriginal, Inc. Announces First Totally Consumer Mortgage Closings, Time to Close, Record and Deliver Mortgage to Investor Reduced from 45 days to 5 Hours* (Oct. 7, 1999)<http://www.eoriginal.com/news/press/prempoc1099.htm>.

55. See Kate Marquess, American Bar Association, *Sign on the Dot-com Line*, (visited Sept.22, 2000) <http://www.abanet.org/journal/octoo/octtkate.html>.

56. See E-Sign § 101(c)(1)(B)(i)(II).

57. See ESRA, 9 N.Y.C.R.R. Part 540(1)(c).

58. See Consultation Publique sur le Projet de Décret (25 July-15 September 2000) <http://www.internet.gouv.fr/>.

59. The Décret art. 6 (g).

60. The Décret art 4, 5.

61. See E-Sign § 105(b).