Legally Binding Electronic Documents: Digital Signatures and Authentication

Christopher Reed*

I. Introduction

It is a fundamental requirement of electronic commerce that the transactions entered into via electronic communication should be legally binding on the parties. For a large class of business-to-consumer (B2C) transactions, this presents no real difficulty. The physical world carries out B2C transactions without any formalities at all; the most obvious example being the sale of goods for cash. In the online world, most traders simply require the consumer to click a button on a Web page to agree to the purchase, take details of the payment instrument (e.g., a credit card), and rely on their ability to prove this process in the event of a dispute. There is, admittedly, some risk that a consumer will repudiate a transaction by alleging third-party fraud, but most e-commerce traders find this risk is sufficiently small and that nothing more is needed to ensure the legal effectiveness of the transaction.

In business-to-business (B2B) e-commerce, however, this simple approach may be inadequate. Much larger sums of money are at stake, and an online business will wish to minimize the risk of repudiation by ensuring that its contracts with customers are legally binding on those customers. In this context, it is important to distinguish two distinct elements of bindingness—for most commercial transactions; an oral contract in theory would bind the parties, as would one entered into via a website without any formalities. However, if the transaction is to be binding in practice as well as theory, the plaintiff party will have to prove the existence and terms of the contract in litigation. Mere proof that some self-identified person completed a form on a Web page is not the most adequate form of evidence for a high-value contract.

This article, therefore, concentrates primarily on the evidentiary aspects of authentication, and, in particular, on the use of digital signature technology to achieve the required evidentiary effects.

*Christopher Reed is Professor of Electronic Commerce Law, Centre for Commercial Law Studies, Queen Mary University of London. Of counsel to Tite & Lewis, London.
II. Authentication

A. Basic Principles

Authentication of the record of an electronic communication requires that a court can, if necessary, be satisfied:

- that the contents of the record have remained unchanged since it was sent (the integrity of the record);
- that the purported sender of the communication is identifiable (the identity of the sender);
- that the identified sender agreed to its contents (attribution of the communication to the sender); and
- in some cases, that extraneous information, such as the apparent date of the transmission, is accurate.

All these elements are relevant to authenticating a communication as received.

Additionally, it is important to remember that a legal dispute will not come to court until some years after the relevant messages were sent, and in the meantime, they will have been archived by the parties. Because they could, in theory, have been altered intentionally, corrupted accidentally, or simply invented for the purposes of litigation, it will also be necessary to demonstrate an audit trail connecting the copy of the message before the court to the copy as originally sent or received.

Most of these records will be copies, and thus, there is a need to prove that each is an authentic copy of the message. The obvious way of doing this is to give oral evidence to that effect, and failure to do so may render the copy inadmissible.¹ In practice, this aspect of authentication may be easier than might be expected, and courts throughout the world have been prepared to accept non-technical evidence to prove the authenticity of computer records.² Authenticity is likely to be proven if:

- the user can produce a human witness to testify that the system (including the operational system used for archiving) was operating properly at the relevant time; and
- the other party to the litigation is unable to adduce evidence to counter this presumption.

In order to ensure that an appropriate audit trail exists, and to produce evidence that will tend to authenticate records of electronic messages, it has been common in B2B transactions to agree in advance what records the parties will keep, and whether particular categories of messages are to be acknowledged by the receiving party, including provisions on what form that acknowledgement should take. These records will assist in resolving disputes over the


2. For example, even under English criminal law, which imposes the high standard of proof beyond a reasonable doubt, computer records have been held admissible. In R. v. Spiby, [1990] 91 Crim. App. Rep. 186 (U.K.), the English Court of Appeal was prepared to presume that a computer was recording evidence accurately when its operator (a hotel manager) testified that he was unaware of any problems in operation, and in the absence of any evidence by the defendant that there was any question of malfunction. The House of Lords approved this approach in R. v. Shephard, [1993] AC 380 (U.K.).
existence or content of electronic messages. As online trading moves to open electronic commerce via the Internet, however, such pre-trading contracts become harder to establish.

B. AUTHENTICATION PROVISIONS IN CONTRACTS

Practicing lawyers seem generally to agree that it is worth including a provision in all e-commerce agreements that states that messages that comply with specified archiving and authentication procedures (and where appropriate, of any specified network provider's technical and operational requirements) are deemed to be admissible and prima facie accurate, and that the use of the specified authentication procedures constitutes a signature. Even if the use of the technology does not create what the courts would recognize as a valid signature, the contractual term, in some jurisdictions, would raise an estoppel argument in favor of the party seeking to rely on the document as authentic. But this estoppel will not bind a third party who will be able to plead the lack of a signature or other authentication as a defense. And, as a corollary, the party will not be able to base his own action on the estoppel; it would be ineffective if the result would be to declare valid a transaction that is in fact void according to the law for lack of formalities. Additionally, where one of the parties to the contract is a consumer, the term may be invalidated by consumer protection legislation.

3. See, for example, American Bar Association, Model Electronic Data Interchange Trading Partner Agreement § 1.5 (1990), which states:

Each party shall adopt as its signature an electronic identification consisting of symbol(s) or code(s) which are to be affixed to or contained in each Document transmitted by such party ("Signatures"). Each party agrees that any Signature of such party affixed to or contained in any transmitted Document shall be sufficient to verify such party originated such Document.

See Michael S. Baum & Henry H. Perrit, Jr., Electronic Contracting, Publishing, and EDI Law § 2.16 (1991). See also Benjamin Milbrandt & John Ciucci, Electronic Data Interchange: Trading Partner Agreement for Defense Transportation, MT901TR1 LOGISTICS MGMT. INST. § XIV (1990), which states: "Vendor will use a code as specified in each transaction set addendum as its discrete authenticating code in lieu of signature and as the equivalent of a signature."

4. This estoppel arises even if the parties know that their agreed electronic signature technology is ineffective as a matter of law:

The full facts may be known to both parties; but if, even knowing those facts to the full, they are clearly enough shown to have assumed a different state of facts as between themselves for the purposes of a particular transaction, then their assumption will be treated, as between them, as true, in proceedings arising out of the transaction. The claim of the party raising the estoppel is, not that he believed the assumed version of the facts was true, but that he believed (and agreed) that it should be treated as true.


5. See, e.g., Swallow & Pearson v. Middlesex County Council [1953] 1 All E.R. 580 (U.K.) (in respect of the formality of writing). Estoppel can arise, however, if the requirement for a signature is imposed by the law solely to protect the parties to the transaction, as opposed to the public interest. See Bower, supra note 4, at 142–44.

6. See, for example, Council Directive 93/13/EEC, art. 6(1), 1993 O.J. (L 95/29), on unfair terms in consumer contracts, which provides that unfair terms are not binding on the consumer. A term of this kind might fall within paragraph 1(q) of the Annex to the Directive as "excluding or hindering the consumer's right to take legal action or exercise any other legal remedy" and thus be regarded as prima facie unfair.

SPRING 2001
C. Authentication Through Third-Party Records

If communications are monitored by a third party, as might occur for transactions effected via a B2B exchange, the log of this monitoring could provide a useful level of authentication. The monitoring system should record sufficient information to prove: (a) the identity of the sender and recipient of the message, and (b) the message contents. So far as (b) is concerned, it should not be necessary to record the entire text of the message if sufficient information is retained to detect alterations. Monitoring by an independent third party provides strong authentication evidence.8

Where the parties communicate directly via an open network, such as the Internet, this evidence will not normally be available. This is because of the distributed nature of P/IP networks, which means that the route of a message and, thus, the identity of the organizations that will be handling it (in whole or in part) are not identifiable in advance. It is possible to route a message via an independent cybernotary9 who, for a fee, will retain the necessary evidentiary information, but this requires both parties to have agreed to the cybernotary's terms.

What is really required for truly open communications is some method of authenticating a message that permits both the sender and recipient to store it on their own systems and to use the stored copy for authentication purposes. The leading technology that achieves this aim is digital signatures.

III. Digital Signatures

The number of commercial transactions that actually require a signature in order to have legal effect is very small.10 But even where a signature is not strictly necessary, the parties to the transaction often want to have signed documentation. Clearly, a traditional manuscript signature is not feasible where the parties communicate via the Internet. Digital communication technology requires methods of electronic signature,12 which are necessarily very different from the manuscript signature.

---

7. Perhaps the message's hash function or even a simple checksum.
8. Examples of third party monitoring for authentication purposes include the SEADOCS project developed at Chase Manhattan Bank. See A. Urbach, The Electronic Presentation and Transfer of Shipping Documents, in ELECTRONIC BANKING: THE LEGAL IMPLICATIONS 111 (Royston Miles Goode ed., 1985). More recently the Bolero system, which also operates in the international trade arena. See Bolero.net, at http://www.bolero.net.
10. In common law countries, a signature requirement is now largely limited to dealings in real estate and contracts of guarantee. The U.S. Statute of Frauds requirement for written, signed evidence for contracts exceeding $500 in value is, in practice, almost never applicable. But some civil law states still retain equivalent rules that are generally applicable. See, e.g., C. Civ. art. 1341 (FR) (applying to contracts, other than those between merchants, exceeding Fr 5,000 in value).
11. The physical world concept of signature is the signatory's name, written in his own hand, on a paper document (a manuscript signature). This is so universally understood by lawyers and non-lawyers alike that it generally receives no special treatment in legislation or case reports.
12. From this point, electronic signature is used as the generic term because digital signature has gained a particular technical meaning, which is the use of asymmetric encryption techniques to authenticate the sender of an electronic document and the document's integrity. The term is also becoming identified with a particular implementation of encryption technology and signature infrastructure as defined in ANSI X.509.
A. What Is a Signature For?

A manuscript signature is accepted without question as legally effective in all jurisdictions, assuming it has not been procured by fraud, and it is rarely asked what effects such a signature is required by law to achieve. However, in those cases where the validity of alternatives has been considered, other methods of signing a document, such as signature by means of a printed or rubber stamp facsimile, have been assessed for validity. The most common approach is to define the functions that a signature must perform, and then to treat signature methods that affect those functions as valid signatures.

The primary function of a physical signature is to provide evidence of three matters:

- the identity of the signatory;
- that the signatory intended the signature to be his signature; and
- that the signatory approves of and adopts the contents of the document.

Manuscript signatures meet these functional requirements in a number of ways. Identity is established by comparing the signature on the document with other signatures that can be proved, by extrinsic evidence, to have been written by the signatory. The assumption is that manuscript signatures are unique, and that, therefore, such a comparison is all that is necessary to provide evidence of identity. In practice, manuscript signatures are usually acknowledged by the signatory once they are shown to him, and extrinsic evidence is only required where it is alleged that the signature has been forged.

Also, intention to sign is normally presumed because the act of affixing a manuscript signature to a document is universally recognized as signing. Intention to sign is normally only disputed where the affixing of the signature has been procured by fraud, and in those cases the signatory bears the burden of displacing the presumption that he intended to sign. Intention to adopt the contents of the document is similarly presumed because it is general knowledge that affixing a manuscript signature to a document has that effect. In both cases, the burden of displacing the presumption is on the signatory.

A difficulty arises, however, if the relevant law imposes specific requirements as to the form a signature must take. In the context of Internet communications, the thing to be signed, an electronic document, exists more as a matter of metaphysics than as a physical object. For this reason, it is very difficult for an electronic signature method to meet any physical requirement of form. For example, some of the English cases and statutes on

15. This is reflected in the jargon of the computer industry that often refers to logical entities, meaning entities that are treated by the technology as a single item even though they may be stored on or transmitted via multiple hardware devices, or may exist in multiple copies.
16. However, it is perfectly possible for the law to impose logical requirements of form. To date, the only requirement of form proposed for electronic signatures is that their validity should depend on compliance with particular technical standards. See, e.g., Utah Digital Signature Rules, Utah Code Ann. § 154-10-301(4)(a) (2000); Digital Signature Act (Signaturgesetz) § 14(4) 1997 BGBl. I 1872 (Ger.); Digital Signature Ordinance (SigV) § 16(6) (Ger.) (made under § 19 Digital Signature Act 1997, in force Nov. 1, 1997). Note, however, that logical requirements of form are imposed only in a minority of the current and proposed electronic signature legislation and that a move to technology-neutral digital signature laws can now be detected. See, e.g., Electronic Signatures in Global and National Commerce Act 2000, 15 USCA § 7001 (2000) (known as E-Sign). The majority of current legislation defines the validity of the signature in terms of the functions performed by the signature method.
physical world signatures appear to state that a signature must take the form of a mark on a document.\textsuperscript{17} A mark, in relation to a hard copy document, has the characteristics of visibility and physical alteration of the thing that is marked. None of the ways in which an electronic document communicated via the Internet may be signed are capable of producing documents that exhibit these characteristics. A distinction must be made between the information content of a document and the carrier of that information. In the case of a physical signature of a hard copy document, the signature makes both a physical alteration to the carrier (i.e., ink is placed on the paper) and adds to the information content of the document. By contrast, an electronic signature only alters the information content of the document. Any change to the carrier is merely incidental, and is not linked inextricably to the document in the same way as a hard copy signature is linked to the writing.\textsuperscript{18} Thus, although typing the signatory's name or adding a scanned signature image to a document makes a physical alteration to the storage medium on which the document is held,\textsuperscript{19} that alteration takes place at the microscopic level\textsuperscript{20} and is conceptually very different from the kind of physical alteration to the document envisaged in the case law—indeed, the bits that make up the document are not altered, merely added to.

However, if the relevant law defines the validity of a signature in terms of the evidentiary functions it achieves, an electronic document may be signed by the use of a mathematical function based on the document's data content.\textsuperscript{21} This process can meet all the law's evidentiary requirements for signatures, but can only be considered as a logical (or metaphysical) mark in that it is in many respects functionally equivalent to a mark on paper, primarily because it cannot easily be altered without leaving some trace. The process can be undertaken in a way that will easily produce evidence of the intention to sign and authenticate the signatory and the electronic document's contents, but the result is if anything less visible than and equally as metaphysical as adding text or an image.\textsuperscript{22}

\section*{B. How Electronic Signatures Meet the Law's Functional Requirements}

\subsection*{1. Evidence of the Signatory's Identity}

An electronic signature, by itself, cannot provide sufficient evidence of the signatory's identity. To explore this matter further, evidence is required that links the signature key or other signature device to the signatory himself. But the recipient wishes to be able to rely

\begin{itemize}
\item \textsuperscript{17} Morton v. Copeland [1855] 16 CB 517, 535 (Maule J) (signing "does not necessarily mean writing a person's Christian and surname, but any mark which identifies it as the act of the party"); \textit{In re Cunningham} 29 LJPM&A see also U.C.C. § 1-201(39) (1992). For statutes, see UK Law of Property (Miscellaneous Provisions) Act § 1(4) (1989): "In subsections (2) and (3) above 'sign', in relation to an instrument, includes making one's mark on the instrument and 'signature' is to be construed accordingly."
\item \textsuperscript{18} It is for this reason that the question that is occasionally asked by those unfamiliar with computers, "Can I place the digital document on a diskette and sign the label?" is nonsense. The digital document can be altered or substituted without any perceptible effect on the diskette itself, and thus the carrier has been signed, but not the document itself.
\item \textsuperscript{19} This is true even if the document is contained only in the temporary memory (RAM) of a computer.
\item \textsuperscript{20} In the case of magnetic storage media, such as disks or tapes, the magnetic polarity of particular areas of the medium is switched by moving electrons into new orbits.
\item \textsuperscript{21} Or, more normally, on a mathematical derivative (for example a checksum or hash function) of the document as a whole.
\item \textsuperscript{22} Although the document is altered (logically but not physically) in that it now consists of a different set of bits.
\end{itemize}
on the signature without needing to collect evidence for use in the unlikely event that the signature is disputed. For this reason, most electronic signatures used for e-commerce communications are likely to be accompanied by an ID Certificate issued by a Certification Authority. The Certification Authority\textsuperscript{23} takes traditional evidence of identity, for example, by examining passports, and, in the case of public key encryption digital signatures, checks that signatures effected with the signatory’s secret key are verifiable using the public key. Once the Certification Authority is satisfied as to the signatory’s identity, it issues an ID Certificate, which includes, inter alia, a certification of the signatory’s identity and of his public key.\textsuperscript{24} This certificate may be used by the recipient to prove the signatory’s identity.

2. Evidence of Intention to Sign and Adoption of Contents

Once identity has been proven, the very fact that an electronic signature has been affixed to a document should raise the same presumptions as manuscript signatures; that is, the signatory intended to sign the document and thereby adopt its contents. There is one difference, however. In the case of a manuscript signature, the signatory has to be present and must have the document to be signed in front of him. Electronic signature technology is a little different. There are essentially two options:\textsuperscript{25}

- the signature is effected by selecting from an on-screen menu or button, with the signature key stored on the signatory’s computer; or
- the signature key is stored on a physical token, such as a smart card, which needs to be present before the signature software can affix the signature.

In either case, a third party who had access to the computer or to the storage device would be able to make the signature. For this reason, an electronic signature should be

\textsuperscript{23} Or, more accurately, a Registration Authority; the commercial models adopted in the digital signature industry are increasingly separating the identification function, which is carried out by a Registration Authority, and the issue of the ID Certificate that emanates from the Certification Authority. The ID Certificate contains a statement that the person to whom it refers has been identified by the Registration Authority along with the effectiveness of the public key.

Annex II of Directive 1999/93/EC on a Community framework for electronic signatures, 2000 OJ (L13) 12, fails to recognize this distinction expressly, providing that one of the requirements that must be fulfilled by a Certification Authority if its ID Certificates are to obtain the legal advantages of being qualified (see infra note 67 and accompanying text) is that it must “(d) verify by appropriate means in accordance with national law the identity and, if applicable, any specific attributes of the person to whom a qualified certificate is issued.” Id. It is to be hoped that the implementation of the Directive in EU Member State national laws and any jurisprudence will recognize the use of Registration Authorities as amounting to appropriate means.

24. Of course, to operate effectively this certificate must be processable automatically, without human intervention. Thus, the certificate is authenticated not in a traditional paper-based way but by the Certification Authority’s electronic signature. A different Certification Authority will certify this signature, and that certificate will also be signed electronically. The theoretical circularity of this process is obviated in practice because a recipient will have identified some Certification Authority (e.g., his bank) whose electronic signature has been authenticated by some other means, and which is therefore trustworthy. Any other Certification Authority certified by that Certification Authority is also trustworthy, at least as to its identity, and so on. The user gradually builds up a database of authenticated electronic signatures, which reduces the amount of checking required.

25. A third option, that the signatory remembers the key and types it in to the software application, which produces the signature, is not practicable. Signature keys are too lengthy to be remembered reliably or keyed in without errors.
considered as more closely analogous to a rubber stamp signature. The party seeking to rely on the validity of the signature may need to adduce extrinsic evidence that the signature was applied with the authority of the signatory until the use of electronic signatures becomes so common that the courts are prepared to presume that a third party who is given access to the signature technology has been authorized by the signatory to sign on his behalf, or unless a statute introduces a presumption as to the identity of the signatory. In cases where an electronic signature that has previously been acknowledged by the signatory is effected by an unauthorized third party, however, the apparent signatory should be estopped from denying that it was his signature.

The objection that an electronic signature fails to meet the evidentiary requirements because a successful forgery cannot be detected is easily dismissed by pointing out that no such requirement is imposed for manuscript signatures. Indeed, signatures in pencil have been held valid under English law for such important commercial documents as bills of exchange and guarantees. In fact, electronic signatures are normally much harder to forge than manuscript signatures. Thus, the only function that electronic signatures cannot provide is that of making a mark on a document; a function that is unnecessary in the digital environment.

3. The Role of ID Certificates

Where the parties have had no previous dealings, the recipient will have no knowledge whether the public key does in fact correspond to the purported identity of the signatory. This is where the ID Certificate comes in. It contains:

- a copy of the signatory's public key; and
- a statement that the issuer of the certificate has checked the identify of the signatory, that the signatory does in fact possess the signature data that corresponds to the public key, and that the issuer has checked that the public key validates the identified person's electronic signature.

Thus, where an electronic signature is made on a document, the accompanying ID Certificate provides evidence from an independent third party that the person named in the certificate did in fact have access to the unique signature data so long as the public key included in the certificate validates the signature. In the absence of evidence from the alleged signatory that some third party forged his signature, a court should be satisfied by

---

26. See, e.g., Jenkins v. Gaisford & Thring, In the Goods of Jenkins (1863) 3 Sw. & Tr. 93 (rubber stamp signature).
27. This reasoning is found in cases on checks, such as Brown v. Westminster Bank Ltd., [1964] 2 Lloyd’s p. 187.
29. Lucas v. James (1849) 7 Hare 410.
30. See, e.g., RSA LABORATORIES, RSA LABORATORIES’ FREQUENTLY ASKED QUESTIONS ABOUT TODAY’S CRYPTOGRAPHY, VERSION 4.1, 80 (2000), available at http://www.rsasecurity.com/rsalabs/faq (last visited Jan. 10, 2001). This publication explains that in 1997, RSA Laboratories estimated that it would cost somewhat less than U.S.$1 million and take eight months to break a particular 512-bit RSA encryption key, and in 1999 such a key was broken in seven months. But breaking one person’s key does not speed up the time required to break any other person’s key. RSA now recommends 1024-bit keys for security encryption—these are theoretically 2 to the power of 512 times more difficult to break than a 512-bit key. These figures compare very favourably with the time and effort required for a skilled forger to copy a manuscript signature.
31. Or, more likely, a Registration Authority. See supra note 23.
the evidence that the purported signatory was responsible for the electronically signed document.

Electronic signatures are likely to be used for a wide range of transactions, which have legal consequences, including:

- the formation of contracts;
- transactions where the recipient of the communication is required to identify its customer, for example, funds transfers to which money laundering controls apply; or
- the provision of legally required information to government agencies where there may be a need to ensure that the information source is correct, or more commonly where there are penalties for supplying incorrect information, for example, on tax returns.

Electronic signatures are also likely to be required for identification purposes where the user is requesting information that should not be released to third parties, such as information about the user's bank account. In addition, there are several types of commercial transactions where digital identification will be useful to one of the parties.

a. Information Licensing

One of the most important areas of commercial activity that the Internet makes possible is the direct supply of information. Most suppliers will not sell information; instead, they will seek to license it to the customer, so as to control use and further copying. Assuming that a license contract is concluded with the customer, there are two reasons why the supplier would wish to receive proper identification of the customer via an ID Certificate:

- If, at some future date, the supplier needs to enforce the license terms against the customer (e.g., the customer is found to be re-selling the information, in breach of the license), the ID Certificate will assist in proving that it was in fact that customer who purchased the information and agreed to be bound by the license terms.
- If the supplier requires ID Certificates from all its customers, the fact that a non-customer is found in possession of a copy of the information is strong evidence that the copy is unauthorized, and thus in breach of copyright. This will even more strongly be so if the public key of the original licensee is embedded in the copy supplied by the licensor, and the non-customer's copy is found to contain the same key.\(^{33}\)

The importance of identification in information transactions has been recognized specifically in section 213 of the Uniform Computer Information Transactions Act, which

\(^{32}\) Indeed, there must be some uncertainty whether information can be sold. A sale normally predicates the transfer of ownership rights. See, for example, Sale of Goods Act, 1979, § 2(1) (U.K.), which defines a sale as "a contract by which the seller transfers or agrees to transfer the property in the goods to the buyer for a money consideration. . . ." The main property rights in information are intellectual property rights, and even where the precise nature of the right transferred is not stated it is hard to imagine a court finding that a supply of information in return for payment was an assignment of those rights, at least in a mass marketing context.

proposes specific rules for determining when the person identified should have the transaction attributed to him. Section 213 specifically states:

a. An electronic authentication, display, message, record, or performance is attributed to a person if it was the act of that person or its electronic agent, or if the person is bound by it under agency or other law. The party relying on attribution of an electronic authentication, display, message, record, or performance to another person has the burden of establishing attribution.

b. The act of a person may be shown in any manner, including a showing of the efficacy of an attribution procedure that was agreed to or adopted by the parties or established by law.

c. The effect of an electronic act attributed to a person under subsection (a) is determined from the context at the time of its creation, execution, or adoption, including the parties' agreement, if any, or otherwise as provided by law.

d. If an attribution procedure exists, to detect errors or changes in an electronic authentication, display, message, record, or performance, and was agreed to or adopted by the parties or established by law, and one party conformed to the procedure but the other party did not, and the nonconforming party would have detected the change or error had that party also conformed, the effect of noncompliance is determined by the agreement but, in the absence of agreement, the conforming party may avoid the effect of the error or change.

Similar attribution provisions are found in section 13 of the Singapore Electronic Transactions Act of 1998.

b. Status Information

A third use of ID Certificates is to use them as a way to confirm the status of the user. Examples of the kind of status information that could be incorporated in an ID Certificate are:

• Information about the user's age. A supplier who wishes to enforce a contract with a customer needs to ensure that the customer does not lack capacity to enter into

34. UNIF. COMPUTER INFORMATION TRANSACTIONS ACT § 213 (1999), available at http://www.law.upenn.edu/bll/ulc/ucita/ucita200.htm (last visited Feb. 10, 2001). Section 112 sets out the rules for determining whether a person has assented to a transaction, a further aspect of attribution (in this case, agreement as opposed to identity):

(a) A person manifests assent to a record or term if the person, acting with knowledge of, or after having an opportunity to review the record or term or a copy of it:

(1) authenticates the record or term with intent to adopt or accept it; or

(2) intentionally engages in conduct or makes statements with reason to know that the other party or its electronic agent may infer from the conduct or statement that the person assents to the record or term.

(b) An electronic agent manifests assent to a record or term if, after having an opportunity to review it, the electronic agent:

(1) authenticates the record or term; or

(2) engages in operations that in the circumstances indicate acceptance of the record or term.

(c) If this [Act] or other law requires assent to specific term, a manifestation of assent must relate specifically to the term.

(d) Conduct or operations manifesting assent may be shown in any manner, including a showing that . . . a procedure existed by which a person or an electronic agent must have engaged in the conduct or operations in order to do so. . . .

Id.

35. Id. § 213.
contracts because he is a minor. Age information may also be used to reduce a host's liability risks, particularly if the host's site contains material whose supply to a minor might be unlawful. For example, the website http://www.hotsex.com requires visitors to confirm that "I am at least 18 years of age and have the legal right to possess adult material in my community" by clicking on a button on the site's home page but has to take the user's agreement to this on trust. Requiring an ID Certificate that shows the visitor is eighteen or over would enable the website's operators to prove to law enforcement agencies that none of the images on that site had been supplied to minors.

- Information about the user's credit status. This information could be supplied by the issuer of the ID Certificate itself if it is a financial institution that issues certificates to its customers, or the certificate could contain information supplied by a third party credit reference agency.

There is no technical reason why an ID Certificate should not contain a wide range of status information. Because the certificate is controlled by and disclosed by the person to whom it relates privacy and data protection issues are significantly less of a problem than would be the case if identity were confirmed directly to the other party.

C. LEGISLATIVE RECOGNITION OF ELECTRONIC SIGNATURES

Because of the uncertainties regarding whether courts would apply the principles outlined above in a consistent manner, there have been a number of legislative initiatives designed to validate the use of electronic signatures. The first of these was the Utah Digital Signatures Act of 1996, which was influenced by the discussions leading to the UNCITRAL Model Law on Electronic Commerce, also of 1996. At the time of writing, there are over 100 laws or proposals for laws regarding the use of electronic signatures. At present, three clear divisions can be seen in these instruments:

- Laws that validate the use of electronic signatures in a closed group of users, such as systems for transferring medical data between doctors, hospitals, and insurers. These laws are of no relevance to open Internet communications, and will not be considered further. This category includes EDI transactions, for which contract is often a potentially suitable mechanism for dealing with signature issues.

- Laws that define validity solely in terms of the functions achieved by an electronic signature method.

37. "Certificates can be used for a variety of functions and can contain different pieces of information. The information can include conventional identifiers such as name, address, registration number or social security number, VAT or tax identification number, or specific attributes of the signatory for instance, their authority to act on behalf of a company, their credit worthiness, the existence of payment guarantees, or the holding of specific permits or licenses." Proposal for a European Parliament and Council Directive on a common framework for electronic signatures, COM(98)297 final at 5.
38. Credit for identifying this classification is due to Mr. Juan Avellan, PhD, researcher at the Information Technology Law Unit, Centre for Commercial Law Studies, Queen Mary University of London.

SPRING 2001
Laws that define validity by reference to the use of ID Certificates within the electronic signature method. These laws may be technology-neutral, in the sense that they do not prescribe a particular technical standard that must be adopted but merely describe the requirements, which a certificate and its issuing Certification Authority must meet. Some laws, however, mandate the use of particular technical standards.  

1. Functional Definitions of Validity

The starting point for most electronic signature laws is article 7(1) of the UNCITRAL Model Law on Electronic Commerce of 1996, which provides:

Where the law requires a signature of a person, that requirement is met in relation to a data message if:

a. a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and
b. that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

Further work is being undertaken by UNCITRAL with the aim of producing Uniform Rules on Electronic Signatures, but at the time of writing the Working Party has not determined whether to maintain the functional approach of the Model Law or to adopt rules based on ID Certificates.

In the meantime, a number of jurisdictions have introduced legislation. A few have taken a purist attitude, defining the functional requirements for an electronic signature but leaving it to the courts to determine whether those requirements are met on a case-by-case basis. Probably the most important example of such legislation is the U.S. Electronic Signatures in Global and National Commerce Act of 2000, which provides in section 101(a):

IN GENERAL—Notwithstanding any statute, regulation, or other rule of law (other than this subchapter and subchapter II of this chapter), with respect to any transaction in or affecting interstate or foreign commerce—

(1) a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form; and
(2) a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation.

The definition of electronic signature in section 106(5) is deliberately technology-neutral: "The term 'electronic signature' means an electronic sound, symbol, or process, attached

41. See, e.g., Utah Digital Signature Rules, Utah Code Ann. § 154-10-301(4)(a) (2000); German Digital Signature Act § 14(4); German Digital Signature Ordinance § 16(6).
to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record." 46 And section 102(a) only permits state laws to specify alternative requirements for the use or acceptance of electronic signatures if these "do not require, or accord greater legal status or effect to, the implementation or application of a specific technology or technical specification for performing the functions of creating, storing, generating, receiving, communicating, or authenticating electronic records or electronic signatures." 47

Many other legislatures, however, have adopted a two-tier approach to this issue; electronic signatures that meet the functional requirements are validated, but the law also makes provision for a greater level of legal acceptability for those signatures that are based on ID Certificates. The Singapore Electronic Transactions Act of 1998 and the EU Directive on electronic signatures clearly demonstrate this two-tier approach.

The Singapore Electronic Transactions Act of 1998 provides for a basic level of legal effect for an electronic signature in section 8:

(1) Where a rule of law requires a signature, or provides for certain consequences if a document is not signed, an electronic signature 48 satisfies that rule of law.

(2) An electronic signature may be proved in any manner, including by showing that a procedure existed by which it is necessary for a party, in order to proceed further with a transaction, to have executed a symbol or security procedure for the purpose of verifying that an electronic record is that of such party. 49

Additional legal privileges attach, however, to what the Act defines as a secure electronic signature in section 17:

If, through the application of a prescribed security procedure or a commercially reasonable security procedure agreed to by the parties involved, it can be verified that an electronic signature was, at the time it was made—

a. unique to the person using it;
b. capable of identifying such person;
c. created in a manner or using a means under the sole control of the person using it; and
d. linked to the electronic record to which it relates in a manner such that if the record was changed the electronic signature would be invalidated, such signature shall be treated as a secure electronic signature. 50

Secure electronic signatures benefit from a number of legal presumptions, which are examined below.

The EU Directive takes a somewhat more rigorous approach, imposing requirements similar to those for secure electronic signatures under the Singapore legislation as its basic test for validity. 51 Article 2 defines electronic signatures as follows:

46. Id. § 106(5).
47. Id. § 102(a)(2)(A)(ii). Alternatively, states may, under section 102(a)(1), adopt the Uniform Electronic Transactions Act requirements for signatures, which are themselves technology-neutral.
48. Electronic Transaction Act 1998 § 2 (1998) (Sing.). Electronic signature, as defined in section 2, "means any letters, characters, numbers or other symbols in digital form attached to or logically associated with an electronic record, and executed or adopted with the intention of authenticating or approving the electronic record." Id.
49. Id. § 8.
50. Id. § 17.
1. "electronic signature" means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication;

2. "advanced electronic signature" means an electronic signature which meets the following requirements:
   a. it is uniquely linked to the signatory;
   b. it is capable of identifying the signatory;
   c. it is created using means that the signatory can maintain under his sole control; and
   d. it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

The Directive proposes a two-tier system of electronic signatures:

- simple electronic signatures, which have merely to meet the definition in article 2(1); and
- certified advanced electronic signatures, where the identity of the signatory is confirmed by a certificate issued by an appropriate third party and complying with other provisions of the Directive (a qualified certificate) and the certificate is created by means of a secure-signature-creation device.

The distinction is important because the main purpose of the Directive is not to make provision for the validity of electronic signatures, but to ensure that national laws do not impose barriers to the free flow of certification services in the European Community.

Article 5 lays out the circumstances in which electronic signatures are to be valid, enforceable, and legally effective. For simple electronic signatures, its provisions are entirely negative—Member States are to ensure that signatures of this type are not denied validity, enforceability, and effectiveness solely on the grounds that they are in electronic form or are not certified. And in this respect, the EU Directive resembles the U.S. Electronic Signatures in Global and National Commerce Act of 2000. But Member States are still free to refuse to recognize electronic signatures for any other reason. Certified advanced electronic signatures receive more favorable treatment, as explained in the next section.

2. Validity Based on Identity Certification

Older legislative initiatives made validity conditional on the use of an ID Certificate in the electronic signature method or, in the case of two-tier systems, granted additional advantages to certified electronic signatures. The Utah Act was the first example of such legislation, although its requirements are now overridden as incompatible with the Electronic Signatures in Global and National Commerce Act of 2000. The signature requirements of the Utah Act are:

(1) Where a rule of law requires a signature, or provides for certain consequences in the absence of a signature, that rule is satisfied by a digital signature if:

52. Id. art 2.
53. Id. art. 2(1). The terminology of simple and certified signatures is not found in the Directive, but is adopted here for ease of reference.
54. Id. art. 2(11). A “certification service provider,” defined in article 2(11) is a Certification Authority.
55. Id. art. 2(10). The certificate must fulfill the requirements of Annex I, and it must be issued by a certification service provider that meets the requirements of Annex II.
56. Id. art. 2(b). Under article 2(6), such a device must meet the requirements of Annex III.
57. Id. art. 5(2).
(a) that digital signature is verified by reference to the public key listed in a valid certificate issued by a licensed certification authority;
(b) that digital signature was affixed by the signer with the intention of signing the message; and
(c) the recipient has no knowledge or notice that the signer either:
   (i) breached a duty as a subscriber; or
   (ii) does not rightfully hold the private key used to affix the digital signature.

(2) Nothing in this chapter precludes any symbol from being valid as a signature under other applicable law, including Uniform Commercial Code, Subsection 70A-1-201(39).58

It should be noted that under the Utah system, licensing of the Certification Authority was a prerequisite for signature validity. But the essential point was the use of the ID Certificate, not the licensing per se, and many laws of this type are based on the American Bar Association Guidelines,59 which do not mandate licensing.60

In more recent legislation, the approach is not to make signature validity dependent on use of an ID Certificate, but to give additional legal effects or privileges where ID certification is used. Thus, section 20 of the Singapore Electronic Transactions Act of 1998 introduces a further concept of secure digital signature, which is by definition a secure electronic signature and thus receives the benefit of the presumptions explained below.61

The Act does not mandate licensing of the Certification Authority per se, but the wording of section 20(b) clearly indicates that in most cases licensing will be required:

When any portion of an electronic record is signed with a digital signature, the digital signature shall be treated as a secure electronic signature with respect to such portion of the record, if—

a. the digital signature was created during the operational period of a valid certificate and is verified by reference to the public key listed in such certificate; and
b. the certificate is considered trustworthy, in that it is an accurate binding of a public key to a person’s identity because—

   (i) a licensed certification authority operating in compliance with the regulations made under section 42 issued the certificate;
   (ii) the certificate was issued by a certification authority outside Singapore recognized for this purpose by the Controller pursuant to regulations made under section 43;
   (iii) the certificate was issued by a department or ministry of the Government, an organ of State or a statutory corporation approved by the Minister to act as a certification authority on such conditions as he may by regulations impose or specify; or

58. Utah Code Ann. § 46-3-301.
60. Id. Section 5.2 states:
   Satisfaction of signature requirements—
   Where a rule of law requires a signature, or provides for certain consequences in the absence of a signature, that rule is satisfied by a digital signature which is
   (1) affixed by the signer with the intention of signing the message, and
   (2) verified by reference to the public key listed in a valid certificate.
61. Electronic Transaction Act § 20 (Sing.).
(iv) the parties have expressly agreed between themselves (sender and recipient) to use
digital signatures as a security procedure, and the digital signature was properly ver-
ified by reference to the sender’s public key.62

By contrast, the EU Directive is specifically drafted in such a way that ID Certificates
from unlicensed Certification Authorities are still capable of producing a certificated sig-
nature. Under article 5(1), an electronic signature receives the benefit of a higher level of
validity if it is based on a qualified certificate, which was created using a secure signature
creation device.63 To be a qualified certificate, the certificate must link the signature veri-
fication data64 used by the signatory and confirm his identity,65 and be issued by a certifi-
cation service provider who meets the requirements of Annex II.66 Additionally, the certifi-
cate itself must comply with Annex I.67

To fulfill the requirements of Annex II, the certification service provider must, in essence,
be a fit and proper person to provide such services.68 The relevant criteria are that the
provider should operate a secure, efficient, and properly run business; take appropriate steps
to identify signatories to whom a certificate is issued; employ suitably qualified personnel
and use trustworthy computer systems and products; take measures against forgery and to
preserve the confidentiality of signature keys; have sufficient financial resources; maintain
proper records; not store the signatory’s signature-creation data; provide proper informa-
tion about the terms and conditions on which certificates are issued; and use trustworthy
systems to store certificates.69 In practice, compliance with Annex II is likely to be dem-
onstrated by acquiring a license from a European accreditation authority or one recogni-
zized70 by the relevant EU body.

62. Id. § 20(b).
63. EU Directive, supra note 51, art. 5(1).
64. Id. art. 2(7). This definition would encompass any of the electronic signature methods discussed in this
article.
65. Id. art. 2(9).
66. Id. art. 2(10).
67. Annex I states:

Qualified certificates must contain:
(a) an indication that the certificate is issued as a qualified certificate;
(b) the identification of the certification-service-provider and the State in which it is established;
(c) the name of the signatory or a pseudonym, which shall be identified as such;
(d) provision for a specific attribute of the signatory to be included if relevant, depending on the purpose
for which the certificate is intended;
(e) signature-verification data which correspond to signature-creation data under the control of the sig-
natory;
(f) an indication of the beginning and end of the period of validity of the certificate;
(g) the identity code of the certificate;
(h) the advanced electronic signature of the certification-service-provider issuing it;
(i) limitations on the scope of use of the certificate, if applicable; and
(j) limits on the value of transactions for which the certificate can be used, if applicable.

Id. at Annex I.
68. Id. at Annex II.
69. These requirements, with minor differences to reflect the different nature of the services provided, are
very similar to those used to determine whether a banking license should be granted. See Banking Act c. 22,
70. The principles and procedures for recognition are set out in the EU Directive, supra note 51, art. 7.

VOL. 35, NO. 1
The effect of meeting these requirements is that the electronic signature is treated as equivalent to a manuscript signature. Article 5(1) provides that such signatures: "(a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a hand-written signature satisfies those requirements in relation to paper-based data; and (b) are admissible as evidence in legal proceedings." 71

3. Legal Presumptions

The purpose of laws validating electronic signatures would be defeated if the person relying on an electronic signature needed to produce technical evidence from which the court could make its own assessment of validity. For this reason, most laws introduce a number of presumptions about an electronic signature that meets the law's requirements. It will always be possible for the other party to adduce evidence to displace these presumptions if there has in fact been some technical failure resulting in a forgery or other defect in the signature. The most important of these presumptions are:

- that the apparent signatory did in fact make the electronic signature; 72
- that the apparent signatory intended to sign and adopt the contents of the document; 73
- that the signed document has not been altered since the time of signature; 74
- that the information in the ID Certificate is accurate 75 and the holder's public key in fact belongs to that holder; 76 and
- that the ID Certificate was issued by the Certification Authority whose electronic signature is contained in the certificate. 77

The Australian Electronic Transactions Act of 1999 simply provides that a signature that complies with section 10 meets any Commonwealth requirement for a signature, while section 7 of the UK Electronic Communications Act of 2000 simply states that such a signature is admissible in evidence as to the authenticity or integrity of a communication. 78

IV. The Future of Electronic Signature Law

The current trend in laws and legislative proposals is to link the question of signature validity with certification of identity. It seems likely that, as commercial activity on the Internet increases, businesses will increasingly require their customers to identify themselves through ID Certificates and will demand electronic signatures that are validated by those certificates. Use of uncertificated electronic signatures will probably be confined to non-commercial transactions; as these will rarely have legal consequences, the evidential issues of proving signatory identity will be unlikely to trouble the courts.

71. Id. art. 5(1).
72. See Electronic Transactions Act § 18(2)(a) (Sing.).
73. See id. § 18(2)(b).
74. See American Bar Association, supra note 59, at § 5.6(3); see also Electronic Transactions Act § 18(1) (Sing.).
75. See American Bar Association, supra note 59, at § 5.6(1); see also Electronic Transactions Act § 21 (Sing.).
76. See American Bar Association, supra note 59, at § 5.6(2).
77. Id. at 5.6(4).
78. Under English law this makes it de facto equivalent to a manuscript signature, as a signature under English law is primarily an evidentiary matter only. See Chris Reed, Digital Information Law: Electronic Documents and Requirements of Form ch. 5 (1996).
There is also a clear trend towards introducing accreditation schemes for certification authorities, for two main reasons:79

- persons relying on ID Certificates need to trust and have confidence in the issuing Certification Authority, and this trust and confidence is engendered by adherence to the accreditation scheme's requirements and auditing (where required by the scheme rules); and
- ID Certificates need to work for cross-border transactions, which means that an ID Certificate issued in, say, Singapore, needs to be recognized for legal purposes in the UK (and vice versa). While it is impractical for the UK tScheme80 to accredit every Singaporean Certification Authority, it is perfectly feasible to recognize Singapore's single accreditation scheme, and thus provide legal recognition in UK for all Singaporean Certification Authorities accredited thereafter.

This does not mean that laws that do not require electronic signatures to be supported by ID Certificates from accredited Certification Authorities, such as the U.S. Electronic Signatures in Global and National Commerce Act of 2000, are in some way defective. These laws do not forbid the use of ID Certificates, and a local Certification Authority will be at liberty to seek voluntary accreditation from some local or foreign accreditation body so as to achieve acceptance of its certificates under foreign laws.

Even where accreditation does not form part of the law's requirements for a valid electronic signature, it is likely that online traders will require their trading partners to use signatures supported by a certificate from an accredited Certification Authority. Such signatures avoid the difficulties inherent in proving that the signature method achieved the evidential functions discussed above, and will also benefit from reciprocal recognition in those jurisdictions that make the use of accredited Certification Authorities compulsory as a condition of electronic signature validation.

---

79. Regulation of Investigating Powers Act c. 23, § 51 (2000) (U.K.). A third reason for accreditation, now largely abandoned, was that governments hoped to impose key escrow requirements on Certification Authorities as a condition of accreditation. In essence, key escrow obliges a Certification Authority to retain a copy of the signatory's private key and make it available to law enforcement and national security bodies. Key escrow is both technically and commercially impracticable, and most governments have abandoned attempts to introduce it. The U.K. Home Office has fought a rearguard action in the Regulation of Investigatory Powers Act, which requires that any person in possession of a private key should disclose it when requested in accordance with the Act, but Certification Authorities are likely to deal with this by refusing to retain copies of private keys.

80. The tScheme is a self-regulatory body that is likely to take on the role of accreditor of UK Certification Authorities—further details are available from Federation of the Electronics Industry at http://fei.interliant.com (last visited Jan. 6, 2001).