AUTHENTICATION RULES AND ELECTRONIC RECORDS

John D. Gregory*
Toronto

The growth of electronic commerce and record-keeping has led to unique problems related to the authentication of electronic signatures and other key information. Electronic documents provide new challenges to the old paper-based legal authentication rules. The modernization of legal authentication regimes must accommodate electronic records, yet respond to concerns related to security and reliability. Time and technology will tell if new legislation promotes the traditional values of authentication rules or if it will need to continue to change to meet the true needs of the increasing numbers of users of electronic records.

Le développement du commerce électronique et de l'archivage électronique a entraîné des problèmes propres à l'authentification de la signature électronique et d'autres informations clés. Les vieilles règles juridiques sur l'authentification, conçues pour le papier, font face à de nouveaux défis devant les documents électroniques. La modernisation des régimes d'authentification doit s'adapter aux documents électroniques et en même temps répondre aux préoccupations concernant la sécurité et la fiabilité. Le temps et la technologie nous diront si la nouvelle législation favorise les valeurs traditionnelles de l'authentification, ou si elle devra continuer de changer afin de satisfaire les véritables besoins du nombre sans cesse croissant d'usagers de documents électroniques.

* John D. Gregory, General Counsel, Policy Branch, Ministry of the Attorney General (Ontario). The views expressed in this article are not necessarily those of the Ministry.

I. *Introduction*

This article discusses the legal status of authentication rules in the light of electronic records. It does so in three parts. First, it provides an overview of the nature of rules about authentication of records on paper, and why and how they have evolved. Next, it discusses the impact of electronic records on these rules, and how the rules have responded to them. Finally, it examines the principal methods of modernizing legal authentication regimes in order to accommodate electronic records, while maintaining the policies that led to the authentication rules in the first place.

The discussion deals throughout with the role and status of signatures, which are the focus of much debate in the world of electronic commerce and electronic government. It is not primarily devoted to authentication in the law of evidence, though the principles at issue are relevant to the courts as well as to business and government.

II. *Authentication Rules in Law*

A. *The nature of authentication*

Authentication is the decision whether a record is what it purports to be. It is, therefore, a question of evidence, though not always of the formal law of evidence.[1] It is a judgment of the credibility or reliability of a document.[2] As such it raises technical, policy and legal issues, all of which play a role in determining the appropriate legislative regime for electronic records.[3] Authentication is a separate question from that of legal effect; one judges the legal effect of a record after one knows how much one trusts it to have any effect, or whether authentication rules allow it to have any effect.

Three questions arise in the process of authentication: What is this record? Where or who does it come from? Has its content been altered, either intentionally or unintentionally?

1) **What:** The answer to the first question depends on the content and context of the individual document. A record may be anything capable of containing information: a contract, a letter, a statute, a laundry list, a bank statement, a picture, a ledger of transactions. This question is not generally the subject of legislation, since there is no right answer to what one might want a record to be. Legislation often, of course, deals with the form and content of particular records.

2) **Source:** There are many ways of deciding where a document came from. Its content is one: it may recite its origin, e.g. "This is an agreement made on [date] by [party X and party Y]." A business letter – one that may be part of a legal transaction - usually states the address from which it comes and the address to which it is being sent, along with the identity of the sender and addressee.

---

[1] While the article does not dwell on the law of evidence in particular, there is some discussion in a later part on recent reform of the law of evidence to deal with electronic records.

[2] A note on vocabulary: a) This article uses the terms "record" and "document" interchangeably. The former tends to be used in the United States, and the latter in Canada, especially in legislation. Archivists often distinguish them on the basis that a record is a document in the context of an organized method of storage and retrieval, i.e. record-keeping system.b) The term "authentication" is sometimes used, especially in the United States, to refer to the process engaged in by the creator of a record, to provide, along with a record, the evidence that will later be used to determine its credibility. Notably it is used as a near-synonym for "signing". The present paper uses the term only to refer to the process engaged in by the holder of a document who wants to estimate its reliability. The rules established to make this process work will of course affect the manner in which the creator of a record creates it.

[3] These three elements have been analysed by a public/ private working group on authentication principles sponsored by Industry Canada, of which the author has been an occasional member. The group is described *infra* note 18.

Other ways of determining the source of a record include the context (it may be part of an ongoing discussion shown by several records), physical evidence (a letterhead, a fingerprint), postal evidence (a postmark, even a stamp), or testimony of someone who knows (e.g. "this is the contract I made with party X last year".) There may be evidence created by a third party, such as a witness, a public official, a record-keeper, or a bank. (Sometimes such people make the originator's signature more reliable, rather than the document itself.)

A very common method of showing the source of a record is the signature of the person who created it, since the primary purpose of a signature is to link a person to a document.[4] A handwritten signature is relatively hard for someone other than the signer to duplicate accurately by hand, so it is a relatively good way to trace the document to the signer. It should be noted that one often needs additional evidence to use a handwritten signature – sometimes of the identity of the signer, since some signatures are not legible and unambiguous statements of the signer's identity, and sometimes of a genuine signature of the signer to compare with the one on the record to be authenticated, if the signature on the record is disputed.

The law does not require a signature to be handwritten, however. Mechanical signatures can be effective, and other people may be authorized to sign for the person to whom the document is to be attributed. A signature may be adopted by the person in whose name it was made, after the time of signing.[5]

Signatures may be supported by supplementary evidence as well, notably that of one or more witnesses to the signature, or the evidence of a public official such as a notary or clerk of a court. Making a document under oath, such as an affidavit, does not by that fact make its source more reliable. The oath goes to the truth of the contents, not their source or their permanence. However, the person before whom the oath is made – a notary or commissioner of oaths – may be a useful witness as to the source. Sometimes the laws of evidence provide that a document witnessed by (or sometimes sworn before) a public official is admissible in evidence without further proof of origin, i.e. it is "self-authenticating".

It is very important to note that a signature is just one way of determining the origin of a document. The document is what counts in law, not the signature. One authenticates the document, not the signature. A signature without a document is legally meaningless; it is just an autograph. A document without a signature may be very important legally. One can

[4] The legal effect of the signature beyond showing the link is not a question of authentication, but depends on the intent of the signer, which in turn is judged from the content of the signed document, the context of its signing and delivery, and a host of other factors.

[5] The form of a signature has no impact on its legal effect, though the fact that there is a signature at all may do so, if an authentication rule requires one.

authenticate an unsigned document and rely on it. A document whose origin is unknown is unlikely to be given legal consequences.

3) **Content:** The third element of authentication involves a judgment of the integrity of the record. A record can be altered intentionally or unintentionally (for example a page could be lost or torn or words become illegible). If the person relying on the record wants a legal relationship with the person who created it, then the two parties must have a common understanding, and the record of that understanding must also be the same for both of them. In short, the integrity of the document is important for obvious reasons.

Nevertheless the integrity of documents is often protected fairly casually. An original handwritten signature is some evidence of the integrity of the page on which it appears. It is common in some legal systems, notably common law systems, for multi-page contracts to be joined only by a staple. It is uncommon for parties who sign multi-page documents to initial every page, except for wills. Some legal systems require some kinds of document to be signed before a public official such as a notary, who may keep the original document in safe custody and make true copies for the use of the parties. Sometimes important documents must be deposited in a public registry, thus out of reach of those who might want to alter them, though usually public registries serve as public notice of the contents of the records as much as a means of keeping them secure.

A seal can help show the integrity of a document if it forms an impression through all its pages. This is more common with seals (and documents) of public officials than of seals used by private parties, which tend today to be impersonal and used on a single page.

One of the common ways of strengthening the likelihood of integrity of a document is to ensure that one has an original version of it. It is harder to tamper undetectably with an original than with a copy, which may be the copy of an altered original. For this reason notaries in Latin systems keep the originals of documents made before them, as mentioned a moment ago.

B. *The Process of Authentication*

One authenticates a document in order to decide whether or not to rely on it, that is, to change one's legal position or to enter into legal obligations. This decision is influenced by a number of factors, not all of them related to the technical nature of the document. The process can be described as a "threat-risk analysis", which involves an evaluation and a balancing of four factors: threats, risks, costs and benefits.

1) **The threats** to the genuineness of the source: who is interested in providing a false document? This involves considering the history of the relationship with the person providing the document: is the person trustworthy? Has there ever been any problem with a document from this person, transmitted

by the same method? Are there others who would benefit from a forgery or an alteration?

2) **The risks** to the person deciding whether to rely: what is the likelihood that the source of the document has provided a false document in this case? This involves the technical examination of the evidence of source and integrity.

3) **The costs** of relying on a false document: what is at stake if the document is not genuine? How much is lost? What is the cost of getting or asking for better evidence of source or integrity? Will the other person refuse? What are the technical costs of a better security system? Are the costs of more reliability higher than the costs of the loss from a false document?

4) **The benefits** of taking a chance on the document: are the potential benefits high compared to the risk of loss and the cost of loss?

Not all analyses of documents and not all relying parties will arrive at the same result. Different people will have different tolerance for loss and different estimates of the threats, risks, costs and benefits even in similar circumstances. High value transactions or transactions with strangers will produce different results than less important transactions with trusted partners.

In short, authentication calls for judgment, not just technical expertise. It is first of all a business judgment, in the case of commercial documents. However, the law has intervened in most countries to set conditions on the authentication decision, making it also a legal judgment.

C. *Authentication Rules*

Documents with legal effect are of course part of a legal system, a system of rules applicable to the relations of people and other entities, as devised by some institution of government.[6] Governments often decide to intervene in judgments about authentication, by making rules that influence the process.

1) **Purpose of authentication rules:** A number of purposes are at work in the rules respecting authentication. The government may decide that the consequences of particular transactions are so important to people that the transactions must be made less risky, by ensuring that some reliable forms of authentication are used. Sometimes only particularly vulnerable people – such as consumers – are made subject to such rules.

   Put another way, there is often a difference between what the law requires for validity and what people will choose to do out of prudence. The law may allow a document written in pencil on a piece of tissue paper to be valid, but

[6] The paper does not separately discuss court-based rules, either those imposed by common law on the authentication of documents in general – of which there are few, outside and even inside the law of evidence – or those created to govern the use of documents within the court system itself. The principles of such rules are arguably the same as those applicable to governmental actions. Evidence rules are discussed briefly *infra* at text accompanying note 88.

many people would consider it imprudent to accept such a flimsy document and they insist on something more durable. Sometimes government intervenes to move the legal standard closer to what prudence seems to require.

At other times governments act to protect a state interest in authenticity. Public records are often taken to be more important than records used only among private parties, because public records involve the official status of citizens, or the expenditure of public funds, or the documents making up the history of the community. Authentication rules applicable to public records are common.

2) **Nature:** Authentication rules generally require that documents be made in a particular form, or with particular formalities. Among the most common are:

- writing requirements: that a document made for a particular purpose or between particular parties must be in writing
- signature requirements: that a document must be signed by all parties to it, or by the party that will be subject to the obligations it creates.
- ceremonial requirements: that a document must be signed in certain circumstances, such as before witnesses, or before certain people, such as notaries or other public officials, or by applying a seal.
- originality requirements: that a document to have legal effect must be used or presented in its original version and not only as a copy.
- registration requirements: that the document be deposited in a public register. Requirements that the public have access to the register may be part of authentication – extra eyes to detect inauthenticity – or part of a public notice regime, for example to establish priorities of claims – that has nothing to do with authentication as such.[7]

Not all form requirements are based on concerns about authentication. They may sometimes serve to protect the signer of the document rather than to ensure its authenticity later. Some are created to produce evidence that certain procedures have been complied with, or that the transaction has been properly conducted. Requiring a consumer's signature on a contract may be a way of ensuring that the consumer appreciates the serious, or at least legally binding, consequences of what is being done.[8] It may be a way of ensuring, and proving later, that the consumer got to look at the terms of the contract before being bound to it. Neither of these motives shows any concern about identifying someone reliably.

---

[7] Registration priority systems are arguably designed primarily to avoid disputes among holders of documents admitted to be genuine, rather than to prevent the late introduction of a forged claim to an interest.

[8] C. Reed, in "What is a Signature?" (2000(3)) The Journal of Information, Law, and Technology (J.I.L.T.), online: http://elj.warwick.ac.edu.uk/jilt/00-3/reed.html, says (at s. 3.2.2) that this is rarely a motive for a signature requirement in law.

Because of the mixed motives for form requirements, as we will see later, laws affecting how electronic records can satisfy such requirements may not need to demand a highly reliable replication of their authentication function.

3) **Scope:** Authentication requirements typically affect documents with a serious impact on the affairs of the person making them. Some typical examples in Canada and the United States are wills, land transfers, contracts for high values or involving consumers, guarantees, family status documents such as marriage contracts, and personal care documents like living wills or powers of attorney

   It may be safe to say that most documents to be submitted to public authorities are subject to some requirements to show their source and integrity, whether the requirements arise from statute or administrative procedure, especially when personal status or entitlement to public benefits are in issue.

4) **Legal effect:** Rules affecting authentication can have one or more of several impacts on the documents subject to them.

   - validity: a document that meets the requirement is valid, or one that does not meet the requirement is invalid.[9]
   - enforceability: whether or not the document is valid, it may not be enforceable, for example against a party who has not signed it.
   - admissibility: a document not in proper form may not be admissible in judicial proceedings, particularly those involving its enforcement.
   - registrability: a document not in proper form may not be registered, and registration may be required to ensure certain rights or priorities concerning the subject of the document.
   - acceptability: a document not in proper form may simply be refused by a public authority subject to an authentication regime, or by a private party to a transaction involving the document.

III. *Authenticating Electronic Records*

In recent years many documents formerly made on paper have been appearing in electronic form. This has caused some concerns and some difficulties with the authentication process. This section of the article looks at the nature of electronic documents and how they may be authenticated in practice. It then turns to the application of existing authentication rules to electronic documents.

[9] Authentication rules may provide that an invalidly authenticated document has no legal effect, but as noted earlier, they say nothing of the legal effect of a record once it has been validly authenticated.

A. *The Nature of Electronic Records*

Electronic records are collections of instructions about electric current, to turn the current on or off. A bit is a yes-or-no (one-or-zero) instruction about current flow. With combinations of seven or eight bits (called bytes), one can give sufficiently complex instructions to make characters of most alphabets. Electronic documents commonly show the result of these instructions as words or numbers on a computer screen, or printed out onto paper. Despite their apparent understandability and the arguable relation to writing, people have been worried about the reliability of electronic documents. There are three main reasons for this:

1) **Uncertainty of storage:** The electronic instructions about current flow must be stored in some form of electronic medium, whether in a computer's hard drive, a diskette, a CD, or a magnetic tape (among others). These storage media may not be completely stable; some data may be lost or altered over time, without human intervention. The media themselves may lose power or data, or they may be affected by outside forces such as magnets or electrical power surges. Likewise if the data are transmitted from one storage place to another,[10] over wires or by wireless means, some of the data may degrade in the process. Finally, the technologies of data creation, storage and retrieval are evolving quickly, and data may have to "migrate" from one hardware support to another over its useful life, or be made processable by different software over that period. Data may be lost in those processes.

2) **Uncertainty of retrieval:** Sometimes data are created in one software or hardware system and retrieved in another. Data may be lost in doing so. In any event the display of the data depends on compatibilities and proper functioning of equipment, and it may be difficult to know if data are being lost in the process, or even if what is displayed is the (version of the) document that one intends to deal with. The format of information is often part of the information. Each time the process is repeated, there is an additional risk of loss.

3) **Ease of alteration, difficulty of detection:** Since electronic documents are just a collection of instructions, those instructions can be changed by anyone with the right software and access to the document. Once they have been changed, the resulting document may show no signs of the change. A copy of the instructions may be perfect, i.e. it may not be distinguishable in any practical manner from the version first created (unlike documents on paper). Further, evidence of origin – such as a signature – is itself electronic and thus subject to the same undetectable alterations as the signed text. Still further, bits are independent: they can be picked up and moved around, from one document to another as well as within a document. Thus the bits

[10] Or simply from the originator to the addressee, prior to any storage.

used to sign one document might be moved to appear in another document unknown to the person who created them.[11]

The result of these factors is a rebalancing of the threat-risk analysis that one does in authenticating any document. The risks are greater, the costs of avoiding them are different. On the other hand, the benefits of using electronic documents may be greater as well: flexibility, transferability, ease of retrieval, and others.

There are methods to reduce the risks inherent in the nature of electronic documents, arguably even to make such documents more reliable than their paper equivalents. This is not the place for a detailed technical description of them.[12] However, an indicative list shows practical methods to promote the authenticity of electronic documents. In authenticating someone else's records, one may wish to inquire about these matters, or even to require disclosure of them from a party proposing electronic records.

- Check the integrity of the storage process: when a document on paper is transferred to computer, have the resulting electronic text checked for completeness and accuracy. If this is not practicable for all transfers, check a representative sample.[13]
- Use trustworthy processes – i.e. know what the reliability of the technology is and use appropriate levels of it for the purpose.[14]
- Control access to the means of creating electronic records. Simple controls of physical access to the means of creating electronic documents may help ensure that only the right people get to them. Likewise electronic controls like passwords or higher level security can keep unauthorized people from the records.
- Use trustworthy people – i.e. ensure the skill and honesty of the people creating, storing and retrieving electronic documents are adequate.

---

[11] See D. Masse, "The ABCs of Authentication: A is for Atom, B is for Bit, and C is for Care", in Canadian Association of Law Librarians, *The Official Version: Proceedings of a National Summit to solve the problems of Authenticating, Preserving and Citing Legal Information in Digital Form*, (Kingston: Canadian Association of Law Librarians, 1997), online: http://www.callacbd.ca/1997summit/auth-masse.html.

[12] A brief but pointed summary of techniques for protecting one's system, and thus for increasing the likelihood of having authentic documents, appears in R. Jueneman, "What You Can Do to Counter Information Security Threats" (2002), online: http://www.jueneman.com/Recommendations.html.

[13] The New Brunswick *Electronic Evidence Act* of 1996, S.N.B. c. 52 provided for admissibility of certain electronic records if they were accompanied by affidavits of people knowledgeable about the reliability of their creation. See now the *Evidence Act*, R.S.N.B. c. E-11, ss. 47.1 and 47.2.

[14] To a significant extent, the available technology has become more secure over the past few years. Secure Socket Layer (S.S.L.) security in web-based commerce (based on public key cryptography, described below) allows people to provide credit card numbers or other sensitive personal information with little or no fear of interception. Modern web browsers and word processing software often allow users to encrypt their electronic messages, either for storage in their own machines or for transmission to others.

Keeping strangers out is a help, but the people you know may also be a risk.

- Use secure communications methods, or if insecure communications are to be used (the Internet being a prime example), secure the data being communicated. The usual way to do this is encryption (as described in the next paragraph)
- Use a trusted third party to intervene in the decision-making about reliability, to attest to facts otherwise not readily ascertainable.

A good deal of discussion about protecting electronic records turns on uses of encryption. Encryption can increase dramatically the reliability of identifying the source of a document.[15] If only one person knows the encryption key, besides the person reading the document, then the person reading it can be sure where it came from. (Proving which of the two people who knew the key actually created the document can be harder, if that is disputed.) With dual-key cryptography (also called asymmetric or public-key cryptography), this advantage can be obtained for a system with many potential readers, as a different key is used for signing records (the "private key", known only to the signer) and for reading them (the "public key", available to be known to anyone who needs to know it).[16]

In addition, encryption allows for a test of the integrity of an electronic record from the time of encryption to the time of reading (also called "verification"). This process involves "hashing" the record, which means taking a mathematical digest or compression of it by a known formula. (Bits being numbers or digits, they are eminently suitable for mathematical processing.) When one hashes the received record by the same method that was used on the original record and the hash results match, then it is safe to say that the record has not changed from beginning to end.

When a private encryption key is used to encrypt the hash digest of a message, or the message itself, for the purpose of identifying the signer and generally to show the integrity of the signed text, it creates a "digital signature"[17] A system in which a trusted third party (known as a certification authority or provider of certification services) certifies the identity of the person who holds the private key linked to a particular public key is know as a Public Key Infrastructure, or PKI.

---

[15] Encryption is also used, of course, to protect the confidentiality of the document, a role irrelevant to authentication and not part of authentication rules.

[16] A very brief summary of public key cryptography can be found in J. Gregory, "PKI in a (Small) Nutshell", (1999), online: http://www.euclid.ca/pkishort.html. A tutorial appears in the American Bar Association's Digital Signature Guidelines (1996), online: http://www.abanet.org/scitech/ec/isc/dsgfree.html.

[17] Signatures created by any electronic means are described as "electronic signatures", of which a digital signature is one particular kind. Unfortunately the literature on signature technology does not consistently use "digital signature" in this restricted sense.

In sum, electronic documents are quite different physically and practically than documents on paper. The methods of keeping them from inappropriate change are often different too. One of the main challenges in authenticating electronic records is properly evaluating the effect of the differences, both in vulnerability and in protection. In other words, as noted, the threat-risk analysis is harder, and most people have less experience in doing it.[18]

This challenge has affected the legal responses to electronic records, a subject to which we now turn.

B. *Legal Responses to Electronic Records*

The first and still a very important legal response to authenticating electronic legal records is the private law method of contract. The parties to a transaction, or the users of electronic documents, agree among themselves what steps to take to make the documents reliable enough for them. A typical example of such contracts are the interchange agreements, also called trading-partner agreements, that are common among parties to Electronic Data Interchange (EDI). Such agreements often include descriptions of the procedures, the technology, and the intermediaries to be used in communicating electronically. They also prescribe or adopt a standard for the electronic form of traditional legal documents, such as purchase orders or receipts.[19]

This article has been dealing with rules for authentication laid down usually by the state, not just by private parties. It is a good question to what extent private parties can by agreement among themselves decide how such official requirements can be met. If the law requires that a document be signed, may the parties using a document decide by themselves, without any state authority, that their electronic signatures satisfy that rule? Can the parties simply decree that as between themselves, an electronic document will be considered to be "in writing" as required by law, so that no party may seek to invalidate the document later on ground that it is not in writing but electronic? Does it make a difference

---

[18] A number of public and private sector initiatives are under way to provide guidelines, best practices or standards for authenticating electronic records. They do not aim to change the law but they may work to say how to put into effect the legal rules described in later parts of this article. The Industry Canada authentication principles working group described *supra* note 3, is formulating principles on party responsibility, privacy, risk management and security, for publication in early 2003. American federal government work is described in "E-Authentication: Making Trust Possible", online: http://www.cio.gov/eauthentication/presentations.htm. Other public and private sector work in the US can be found at the National Electronic Commerce Clearing Centre, online: http://www.ec3.org and in the guidelines for evaluating public key infrastructure projects, published by the American Bar Association, online: http://www.abanet.org/scitech/ec/isc/pag/pag.html. See also the European Electronic Signature Standardization Initiative, EESSI, online: http://www.etsi.org/T_news/0005_ESI.htm.

[19] EDI Council of Canada (now the Electronic Commerce Council of Canada), "Model Form of Electronic Data Interchange Trading Partner Agreement and Commentary" (Toronto, EDI Council of Canada, 1990).

that the document is to be submitted to an agency of the state, rather than just between private parties? Can the parties make their own rules for admission of evidence? The difficulty in answering such questions was one factor that led to the legislative measures discussed in the next section of this paper.

It is arguable that an electronic document is "in writing" for the purposes of an authentication rule requiring writing. In use, many such documents are displayed in letters and numbers that we recognize as characters of writing. This argument runs into several counter-arguments, however, that have led to reluctance to accept electronic documents for this purpose without legislative support. The first is that writing requirements often appear in contexts that seem as a matter of policy to call for a degree of stability of the document, and electronic records do not all have this stability. Second, all Canadian jurisdictions have an Interpretation Act, which often defines "writing" or related terms in words that suggest if not state outright that some tangible medium must be present. One finds words like "printed" and "lithographed", though the closing language appears in broader terms.[20] Third, writing requirements often appear without the word "writing" itself, but rather terms that imply writing on paper such as "on a prescribed form" or "certified". Finally, not all documents whose users seek a legal effect do use the characters of writing. Machine-readable documents may also be suitable for the purposes of writing, but they cannot be said to resemble it. Many EDI forms are of this kind – codes recognizable by machines according to agreed standards, but not displayed in letters or numbers.

The courts have sometimes been willing to allow electronic records to satisfy form requirements that are rules about authentication. For example, a Canadian court a few years ago decided that a form of proxy faxed to a corporation for its shareholders' meeting was "signed" as required by the corporate statute.[21] Its status as a faxed document did not prevent the signature on it from satisfying the requirement. One wonders if the court would have been as confident if there had been any dispute about who had signed the proxy, and not only about its form. Since the source of the document in that case was not in dispute, the result is satisfactory for the case.[22]

The case shows the importance of distinguishing between the question of whether a document is signed and the question of who signed it. Often the form requirement demands only that one prove the former, the fact of signature. It requires the means of authentication but does not prejudge the result of the authentication process. The parties relying on the document are left to prove its

[20] See the *Interpretation Act*, R.S.C. 1985, c.I-21, s.35(1) – writing includes "any mode of representing or reproducing words in visible form", similar to much provincial legislation, for example the *Interpretation* Act, R.S.O. 1990 c.I.11, s.29(1).

[21] *Beatty* v. *First Explorer Fund 1987 & Co.*, (1988), 25 B.C.L.R. (2d) 377 (S.C.).

[22] In any event the law does not usually require any particular form for a signature, so it is arguable that electronic signals or codes qualify as a signature under the general law.

source, using the signature and other evidence – if it is disputed - just as they have to demonstrate its legal effect once it has been authenticated. The reasoning is the same for a paper as for an electronic document.

Rather than multiply examples of courts being more or less willing to find authentication rules satisfied by electronic documents, however, it is simply worth noting that court decisions govern only their own facts, however narrow or unusual. It is hard to derive advice on authenticating electronic records from the few cases available in any jurisdiction.

Many jurisdictions have therefore had recourse to legislation. Sometimes they simply authorize the state to use electronic documents for official purposes, or to keep official records in electronic form. Sometimes they spell out how to do particular things electronically. As electronic records have become more familiar, legislation about them has become more accepting and less prescriptive. In general, electronic records should not have to be more reliable than their paper equivalents.

However, states are still involving themselves in the authentication decision, and making a threat-risk analysis, or a prudence analysis, on behalf of their citizens. This is in part because people and their governments still trust electronic records less than paper records. It is also because electronic records present particular challenges to the interpretation of existing authentication rules. Some legislative assistance is necessary if the traditional rules are not to bar the use of electronic records even when the state and the citizens favour their use.

IV. *Legislation on Authenticating Electronic Records*

This section reviews legislation that applies broadly to electronic records. It does not include statutes that prescribe rules for particular documents or narrow classes of documents, or documents only for state use, because such statutes are as varied as the documents they deal with. The legislation described here is sometimes applicable on its face only to commercial applications, though Canada and some other countries have applied the principles more broadly. There are in any event fewer models for non-commercial records, such as in matrimonial matters, administrative law or criminal prosecutions. Legislators have to decide how much freedom parties should have to make their own arrangements or judgments about authentication, and how far any such freedom may be appropriate for different kinds of electronic documents.

After the examination – the longest part of the text – of approaches to authentication rules for electronic records, the article looks more briefly at some other elements of legislation in this field that do not deal directly with the formalities of authentication but which contribute to the ways the relevant laws operate. In particular that part of the text deals with evidence, liability rules and recognition rules.

A. *Approaches to Formal Authentication of Electronic Records*

There are, roughly speaking, five general approaches to legislating authentication rules for electronic records. Each will be described in turn.

1) governmental discretion
2) closed systems
3) technology specific general rules
4) technology neutral general rules
5) hybrid rules – combining neutral and less neutral rules

1) *Governmental Discretion:*

This is the most open-ended approach. A government official, or government officials responsible for particular documents, is given the power to prescribe how particular documents are to be done. It is used generally where documents are to be filed with the state, so the state has a specific interest in the reliability of the document but also in the manageability of the process by which the documents are created and submitted. The discretion may be applied to remove existing authentication rules or to adapt them to the new medium of the document.[23]

2) *Closed Systems:*

A "closed" system of communication (i.e. of circulation of documents) is one in which all parties are linked to each other by contract or by admission or permission by someone with the power to control the system. This is often the government or a part of the government. At that point "system rules" will apply to authentication. The nature of the system rules will depend on the needs of the system. If everyone in the system is using the same trusted or officially approved hardware or software, or is identified automatically by accessing the system, then little other formal authentication may be required.[24]

---

[23] See for example Ontario's *Business Regulation Reform Act, 1994*, S.O. 1994 c. 32, s. 10. Several other provinces have similar legislation: for example, *Business Electronic Filing Act*, S.N.S. 1995-96 c. 3, *Business Electronic Filing Act*, S.N. 1997 c. B-12; *The Business Paper Reduction Act*, S.B.C. 1998 c. 26. See also s. 8 of the *Electronic Communications Act, 2000*, s.7 (U.K.), which allows the responsible minister to declare how form requirements can be satisfied electronically (subject to some Parliamentary control).

[24] See for example the Toronto E-Filing Pilot Project, 1996 – date (O.R. 223/97). Rules of Civil Procedure, R.R.O. 1990, c. 194, as amended, Rule 4.05.1. Private law firms using software provided by the Ministry of the Attorney General are allowed to file electronic court documents without the signatures needed on their paper equivalents. They may also pay the filing fees from their bank accounts by electronic means. All participants are known to and approved by the Ministry (and the bank).

EDI systems governed by trading partner agreements, as described earlier, are closed systems. To the extent that legislation recognizes the effectiveness of the contractual authentication devices to satisfy official requirements, they are logically included in the list of legislative approaches. We will see below that the more general legislative approaches usually make some room for private authentication systems alongside the statutory schemes.

3) *Technology Specific General Rules:*

Governments that have wanted to facilitate the use of electronic documents, generally or in commerce, have often moved cautiously to remove the barriers caused by existing authentication rules. They have spelled out the attributes of the technology deemed appropriate for commercial uses, for example, and have given special legal effect to it. Frequently the technology chosen for such statutes is public-key cryptography. This technology has the advantage of being well tested in theory and it has been thought predictably reliable.

It can have the additional advantage of offering a third party to make it more reliable. A signature on paper involves two people or classes of people: the signer and the person(s) relying on the signature. While an electronic signature may also involve only the same two classes, it may also involve an intermediary to establish the relying party's trust in the signature itself. An electronic signature is only bits, like any other electronic document. Many people believe that digital signatures will inspire more confidence if a trusted third party certifies to the relying party that the signature bits are in fact the signature of a particular person.[25] articles/trusted.htm. The authentication function can be fulfilled by this technology without constituting a signature in law, and thus without having to resolve questions of intent. SSL "browser certificates" are an example, by which computers identify themselves to web sites for secure e-commerce applications, such as paying by a credit card online. (The technology and not the third party guarantees the integrity of the electronic document supported by a digital signature.)

The technology has however two disadvantages, both arising from its technical complexity. First, it is hard for the general potential user of such a system to judge whether the technical or administrative requirements are being properly met. Second, it may be hard to demonstrate to a court just why the technology is reliable and should be accepted by the court.

Legislation has thus been devised to ensure that such third parties, known as certification authorities (CAs), follow trustworthy procedures. Some statutes offer to the relying party reinforced credibility of the identification in such certificates, by way of a presumption of attribution, and also a presumption of the integrity of the document involved. It is thought that such presumptions help

[25] A.M. Froomkin, "The Essential Role of Trusted Third Parties in Electronic Commerce", (1996), 75 Oregon L.R. 49, online:http://www.law.miami.edu/~froomkin/

the signer choose the technology with confidence, and relieve the relying party of having to get into the details of the technology before a court.

Much of the early conceptual work about the legal uses of such a system was carried out by the American Bar Association, whose Digital Signature Guidelines were influential.[26] The first legislation to this effect was the Utah Digital Signature Act of 1995.[27] It dealt expressly with public key cryptography as signature. It regulated certification authorities and exempted them from liability if they followed the rules. It also provided a presumption of attribution for signatures certified by licensed certification authorities. The Utah Act was followed in three other states (Washington, Minnesota and Missouri).[28]

However, this approach was severely criticized on several grounds.

- As technology evolved there were many different implementations of digital signatures, with different degrees of involvement and engagement by third parties and relying parties and thus different risks and degrees of reliability. The relationship among the participants was not always as contemplated in the legislation. Presumptions were not justified to the same degree for each implementation.
- Different uses of electronic documents needed different degrees of reliability, in fact, so having a single system designated by law was sometimes unhelpful or even risky to the users.
- The apparent advantage of not having to prove the technology in court was reduced by the need to respond persuasively to someone who attacked its reliability.
- Digital signature legislation was thought to impede the free development of electronic records systems, as it gave an unfair legal advantage to the technology of public key cryptography.[29]
- More recently, privacy advocates have attacked some features of PKIs as a threat to individuals' control over their personal information.[30]

---

[26] *Supra* note 16.

[27] *Utah Code Annotated*, Title 46-3, online: http://www.le.state.ut.us/~code/TITLE

[28] For a list of electronic signature legislation, with links to online texts, see the Baker & McKenzie firm website, online:http://www.bakerinfo.com/BakerNet/Resources/E+Commerce/

[29] B. Biddle, "Legislating Market Winners", (1997), onlineat:http://www.w3j.com/7/s3.biddle.wrap.html.

[30] See for example S. Brands, *Rethinking Public Key Infrastructures and Digital Certificates: Building In Privacy* (Boston, M.I.T. Press, 2000) - a summary is online: http://www.x4all.nl/~brands/#summary; and R. Clarke, "Privacy Rights of Public Key Infrastructures", (2000), 3 Internet Law Bull. 1, online: http://www.anu.edu.au/people/Roger.Clarke/DV/PKI2000.html. The relationship between authentication in general and privacy rights is one of some tension. Authentication systems, especially a temptingly handy "single sign-on" system for multiple uses, may give excessive information about the identity or attributes and entitlements of an individual to those who need to authenticate for more restricted purposes.

In the result, no further American states have followed the Utah example.[31]

The main place where PKI legislation is still actively under development is among governments for state use, in internal communications and in those with citizens and businesses. Many governments have decided that their electronic records require this technology, and for their own purposes are legislating the legal requirements for, and the results in law of, its use.[32]

4) *Technology Neutral General Rules*

The first task of legislation on electronic records has been to interpret existing form requirements in authentication rules, to say how electronic records may satisfy them. In contrast to the specific detailed statutes discussed above, and in response to the criticisms of them, a number of countries – and international bodies – have preferred a response to the authentication of electronic communications that will operate with whatever technology people choose to apply. The proposed legislation can be said to be "technology neutral" for this reason.[33]

The leader in this field is the United Nations Model Law on Electronic Commerce.[34] The Model Law sets out an electronic equivalent to various form requirements that are prescribed to support the authentication of paper records. It says how to satisfy electronically legal requirements that documents be in writing, that they be signed, and that they be presented in original form. It also has rules about evidence and about retaining records in electronic form. It also answers some questions unrelated to authentication concerns, on matters such as contracts and the time and place of sending messages.

For example, in the Model Law, a requirement for a signature of a person is satisfied if a method is used that identifies the person and indicates the

---

[31] In the wake of the Utah Act, Germany, Italy and Malaysia also passed digital signature legislation, with extensive rules about the creation of signatures, the role of the certification authority, and so on. Germany has since modified its law to conform to the Directive of the European Union on Electronic Signatures, which is discussed below in the section on hybrid legislation, and Italy will have to do so as well in due course. These laws too are listed on the Baker & McKenzie site, *supra* note 28.

[32] An important part of the motivation for such legislation is to set out the duties and liability of the parties when the technology is used, a topic discussed briefly later in this article. See *infra* text accompanying note 98.

[33] For a skeptical look at technology neutrality by a PKI advocate, see M. Baum, "Technology Neutrality and Secure Electronic Commerce: Rule-Making in the Age of 'Equivalence'", (1999: Exposure Draft 1.1). online: http://www.verisign.com/repository/techneutralityv1_1.doc.

[34] *Official Records of the General Assembly, Fortieth Session, Supplement No. 17* (A/40/17) (1996). The text and the very useful Guide to Enactment are online: http://www.uncitral.org/english/texts/electcom/ml-ecomm.htm. This text is sometimes referred to hereafter as the 1996 Model Law.

person's approval of the electronic record, and if the method used is as reliable as is appropriate in all the circumstances, including the existence of any agreement among the parties about the method to be used.[35] This function of a signature – to link a person with a document – is the same for a signature on paper or a signature associated with an electronic document. This means that existing authentication rules can be satisfied by an electronic signature under this formula.

A writing requirement can be satisfied under the Model Law by an electronic record "accessible so as to be usable for subsequent reference."[36] This is not very demanding, no doubt because the requirement that a document be in writing is not very demanding either. It can be more or less readable or durable or alterable.

A requirement to produce an original is more demanding. The Model Law recognizes this in providing that an electronic record may satisfy such a requirement only if there exist reliable assurances of the integrity of the record from the time it first took its final form.[37] It goes on to list details about what that may mean, and makes the standard of reliability depend on the circumstances of the proposed use of the record.[38]

The Model Law allows implementing countries to exclude particular requirements, signatures or documents from the scope of the permission, though it does not say what to exclude.[39] A state legislating on authentication of electronic records may choose to exclude on the basis of the type of document, the type of transaction, or the type of party. The motive of excluding would be to protect either the interests of the parties or the interests of the state in reliable authentication and prudent practices, in other words, the same motive that often underlay the creation of the authentication rule in the first place, before electronic documents came into the picture. The range of exclusions – of cases where authentication decisions cannot be left to the parties – is likely to be narrower when the documents and transactions are purely commercial. The more the enabling legislation extends to non-commercial matters, the more interest the state may have in involving itself in authentication decisions.[40]

---

[35] *Ibid.* art. 7(1). It is generally accepted that "approval" in this formula means only willingness to adopt the text as one's own, without necessarily restricting a signature to one used to assent to a contract.

[36] *Ibid.* art. 6(1).

[37] *Ibid.* art. 8(1).

[38] *Ibid.* art. 8(2).

[39] *Ibid.* arts. 6(3), 7(3), and 8(4).

[40] Likewise, the more detailed the rules are for electronic authentication, the fewer documents need to be excluded from the permission to authenticate electronically. Conversely, if a country excludes most sensitive documents from the legislation, then the remaining documents may well be left to be authenticated as the parties to them see fit.

Many of the countries implementing the U.N. Model Law,[41] including Canada,[42] have chosen similar exclusions. Typically land transfers, wills, powers of attorney, and negotiable instruments are excluded. Land transfers tend to have a public interest component, at least for the protection of third parties, often done through a public registration system. Powers of attorney and wills may be prepared by the parties themselves without professional advice, which increase the risk of insecurity in matters very important to the property of the makers.[43] Negotiable instruments carry in themselves the value they represent, and they therefore must be unique, i.e. exist in a single official version only. Electronic records are at present impossible to create in a way that they cannot be copied, if they are still to be transferable.

Authentication rules often aim to protect consumers. The Model Law does not itself exclude consumer transactions. However, its provisions yield to consumer protection laws in enacting states. Enacting states may have to decide if a requirement in their law that a consumer contract be in writing or signed should be satisfied by an electronic document that comply with the Model Law's rules, or whether further demands should be imposed. Canadian legislation on electronic documents likewise does not exclude consumer transactions. To protect consumers in electronic commerce, many jurisdictions are proceeding by regulation,[44] though Manitoba legislated on the topic in its general electronic commerce statute.[45] The essence of the texts so far is to prescribe content and disclosure rather than much detail on authentication practices. Though merchants must state who they are and where they can be found, electronic records need not contain any independent evidence of this information.

Three issues arise out of the Model Law's approach that cast light on legislation about authenticating electronic records: reliability standards, contracting out, and attribution rules. .

---

[41] International legislation is shown at the Baker & McKenzie site, *supra* note 28, and is analysed by the Internet Law and Policy Forum, online: http://www.ilpf.org.

[42] The principal Canadian document on implementing the U.N. Model Law on Electronic Commerce is the *Uniform Electronic Commerce Act*, [1999] Proceedings of the Uniform Law Conference of Canada 380, online: http://www.ulcc.ca/en/us/index.cfm?sec=1&sub=1u1. A chart showing its implementation by all the common law provinces and the Yukon, as well as federal and Quebec legislation, is on the same web site, online: http://www.ulcc.ca/en/cls/index.cfm?sec=4&sub=4b. There are minor variations in the implementing legislation. See J. Gregory, "Canadian Electronic Commerce Legislation", (2002), 17 B.F.L.R. 277.

[43] Some countries require the participation of notaries in these documents; if a system of electronic notarial documents can be devised, then this concern is lessened.

[44] A federal-provincial-territorial working group devised a "template" for consumer protection in "Internet sales", see the Industry Canada web site, online: http://strategis.ic.gc.ca. It has been enacted by Alberta in regulations under the *Fair Trading Act*, R.S.A.2000 c. F-2. The regulations are the Internet Sales Contract Regulation, A.R.81/2001.

[45] *The Electronic Commerce and Information Act*, S.M. 2000 c. E-5.5, online: http://www.gov.mb.ca/chc/statpub/free/pdf/b31-1s00.pdf . Part VI amends *The Consumer Protection Act*, C.C.S.M. c. C200. Ontario includes the new rules as ss.37-40 of its *Consumer Protection Act, 2002*, Schedule A to Bill 180, the *Consumer Protection Statute Law Amendment Act, 2002*, first reading 30 September 2002, online at http://www.ontla.on.ca/documents/Bills/37Parliament/Session3/b180e.htm.

- **Reliability rules**: Authentication rules generally aim to support the reliability of the record or at least of the evidence used to authenticate records. The 1996 Model Law has a range of reliability requirements for electronic records. The requirements for records to satisfy writing requirements and originality requirements have not been controversial; the implementing legislation in Canada has adopted them without serious variation.[46] The same is not true for signatures.

  Some implementations of the Model Law omit the reliability test entirely in the case of signatures, so that any electronic signature meets a signature requirement.[47] The e-signature would have to be made with intention to sign the document, so evidence would be needed of its nature. The Canadian[48] and American[49] uniform statutes, and the American federal statute[50] all take this approach.[51] The Quebec provincial statute also requires no particular reliability of an electronic signature.[52]

  The reason for the omission is that current law imposes no reliability test on handwritten signatures on paper. Anything that can be shown to be linked to a person with intent to sign a document can be a signature. As noted earlier, a signature is just one way to authenticate a document.[53]

---

[46] Quebec's *Act to establish a legal framework for information technology*, S.Q. 2001 c.32, does not track the Model Law, though it is largely consistent with it. It speaks at greater length of the need for stability of a "technology-based" document over its life-cycle. See ss. 3, 6 and 7. A detailed description of the statute and its background appears in French, with links to the text of the statute in English, French and Spanish, online: http://www.autoroute.gouv.qc.ca/loi_en_ligne/index.html.

[47] In other words, they do not create a new legal "thing" called an electronic signature: they apply the usual law of signatures to the electronic version.

[48] UECA, *supra* note 42, s.10. It defines "electronic signature" in s. 1.

[49] *Uniform Electronic Transactions Act*, s. 7(d). Compare its definition of "electronic signature" in s.1. The UETA was adopted by the National Conference of Commissioners on Uniform State Laws in 1999. The text is online: http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm. See http://www.uetaonline.com for background material, adoption record, and related documents.

[50] The *Electronic Signatures in Global and National Commerce Act* (E-SIGN), Public Law 106-229, June 30, 2000, online: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ229.106.pdf.

[51] The European Union Directive on Electronic Signatures prohibits discrimination against electronic signatures on the ground that they are electronic, but provides special rules for advanced electronic signatures, discussed below in relation to hybrid laws. See Directive 99/93/EC, December 1999, *Official Journal L013*, 19/01/2000, at 0012 – 0020. The text is online by searching under legislation – directives for 1999 document 93, at the E.U. web site, online: http://europa.eu.int/eur-lex/en/search/search_lif.html.

[52] *Supra* note 46.

[53] Compare the Quebec new technology statute, *ibid.* Section 38 says that the link between a "technology-based" document and a person may be shown by any method that allows the identity of the person to be confirmed and the link with the document to be confirmed, and of course the document itself to be identified. Section 39 says that one such method may be a signature, referring to the usual Civil Code definition of a signature (Civil Code of Quebec art. 2827).

If one can show with respect to any document, or any apparent signature, who created it, what it relates to, and what the intention was (a matter of context not form), then the task of authentication is complete.[54] Needing to show in addition that the form of signature met some kind of reliability test, independent of what one can actually prove toward authentication, seemed superfluous, if not simply a trap for the unwary, a risk of invalidity despite clear proof of authenticity.[55]

- **Contracting out – ability of parties to set standards:** Article 7 of the 1996 Model Law allows a court to take into account any agreement among the parties to a document when judging the reliability of a signature method. In doing so the court could presumably choose not to follow the agreement. Otherwise the parties cannot opt out of this standard for satisfying a signature requirement, or the other ways of meeting authentication rules with electronic records. The U.N. Model Law on Electronic Signatures of 2001[56] shows an evolution of this position. Article 5 of the newer text says that parties to a transaction may vary or opt out of any provision of the Model Law (i.e. of legislation implementing it) except where this is prohibited by law. This was intended to be the equivalent of saying that the power to opt out is limited by "mandatory rules" or considerations of "public order", in the language of international conventions. It was not intended to encourage countries to prohibit commercial parties from making their own arrangements across a range of documents. This is therefore a broader autonomy to make one's own arrangements than in the older text.

  In addition, Article 3 of the new Model Law states clearly that the parties are free to decide what will be good enough among themselves, even if they choose a more demanding authentication technique than that which would be considered appropriately reliable under Article 6. They may also take advantage of any rule of law that would allow for a less reliable signature than the general standard of appropriate reliability.[57]

---

[54] Further, showing the fact of signature alone may meet the authentication rule, without showing who signed.

[55] Manitoba nevertheless included a reliability test in its signature rules: *The Electronic Commerce and Information Act*, *supra* note 45, s. 13(1). The UECA also allows enacting jurisdictions to make regulations imposing a reliability test for particular signatures: *supra* note 42, s. 10(2). No jurisdiction has made such regulations at time of writing.

[56] Adopted by the General Assembly, December 12, 2001, online: http://www.unictral.org/english/texts/electcom/ml-elecsig-e.pdf. A Guide to Enactment appears on the same site. It is sometimes referred to hereafter as the new Model Law or the 2001 Model Law.

[57] One does not contemplate legislation approving "inappropriate" reliability, but rather legislation setting a lower standard for a good reason, in the absence of which reason and legislation the signature technique could be considered insufficiently reliable.

Legislation based on the U.N. models, including Canada's, thus makes space for the trading partner agreements done for EDI, mentioned earlier, that spell out that the electronic signature or document authentication processes named in the contract will satisfy authentication rules of the applicable law. This is true especially for electronic signatures.[58]

This broad role for private contracts (what the Americans call "party autonomy") recognizes that authentication is more a matter of risk management than of legal duty. The law still plays two roles: first, it tells those without the power to negotiate standards how to get to a generally acceptable system. Second, it sets the important standards for authentication, those that cannot be derogated from, in other words those that are so important that parties are not allowed to make their own judgment. This power is given not only by the submission of private agreements to public order, but also by the power to exclude some kinds of signatures or records from the statutory permissions altogether. The exclusions leave electronic records exposed to the general law imposing form requirements for authentication. Sometimes, as we have seen earlier, electronic records will not be able to satisfy those rules for technical reasons, and they will suffer whatever the consequence is for not being authenticated under the rule.

In some cases the right policy response to this incapacity to authenticate electronic records under general rules may be special rules for those special types of records. For example, the province of Ontario has followed the general Canadian uniform statute in excluding land transfer documents from the permission to use electronic documents and signatures.[59] Nevertheless the province has established an electronic system of land transfers, with its separate statutory and technical security regimes.[60]

Legislation that leaves much autonomy to the parties to decide what evidence they need of authentication also exposes parties to the risk of wrong decisions. If this is done, then it is important to ensure that parties are free to decide not to use electronic records and signatures at

---

[58] The new Model Law does not address reliability under the other provision of the 1996 Model Law that referred to this quality, namely that on providing an original (article 8). A desire for clarification on the point has not made itself felt as it did with respect to signatures.

[59] The *Electronic Commerce Act*, S.O. 2000 c.17, s. 31(1)(4).

[60] *Land Registration Reform Act*, R.S.O. 1990 c.L.4, as amended by S.O. 1994 c.27, S.85. Other provinces, notably British Columbia and Manitoba, provide for some part of their real property processes to be done electronically, outside their e-transactions statutes. The Ontario regime was set up before passage of the general e-commerce statute, but the principle is the same regardless of the timing.

[61] UECA, *supra* note 42, s.6.

[62] UETA, *supra* note 49, s.5.

all. The Canadian[61] and American[62] statutes, among others, are very clear on that point. As the Canadian uniform statute puts it, "nothing in this Act requires any person to use or accept information in electronic form, but consent may be inferred by conduct."[63]

The power to say No is the power to say "Yes, if ..." and thus impose for particular transactions or classes of transaction the rules for reliable authentication that seem appropriate to that person. Since the relying party takes the risk, on paper or online, that the document or signature is not genuine, that party should be able to decide on the medium in which it will run that risk and the conditions that apply to it.[64]

- **Attribution rules**: Article 13 of the U.N. Model Law on Electronic Commerce provides that electronic records may be attributed to those who create them or who authorize their creation. This is of course the general law in most countries. The United States have legislated similar provisions.[65] Canadian legislators thought this went without saying, so did not say it.

  The 1996 U.N. Model Law goes on to provide a rule of attribution where certain agreed security procedures are used on electronic messages, or if an unauthorized person gets access to the security procedures through the fault of the authorized user.[66] These attribution rules are not directly connected to the electronic signature rules of the Model Law; they apply whether or not there is a legal requirement for a signature. They can be seen as recognizing that attribution is a key element of authentication, without any requirement of the intent element necessary in a signature. In a way they establish a rule of attribution by negligence.

  To date these rules have not been widely adopted by implementing countries, in part because the rules do not give enough flexibility in measuring the consequences of the attribution. The Canadian uniform statute did not try to follow the Model Law on this point,[67] although the federal government has given it some echo in its legislation,

---

[63] UECA, *supra* note 42, s. 6(1).

[64] Consent to use electronic documents is not the same as consent to the substance of a particular transaction conducted using such documents, of course.

[65] UETA, *supra* note 49, s. 9.

[66] 1996 Model Law, *supra* note 34, paras. 13(3) and (4).

[67] The American uniform drafting group attempted to devise similar rules, but they fell under severe criticism based partly on the fluidity of the technology available and partly on the likely lack of sophistication of its users, in short on the difficulty of setting a standard of care for negligence. Reports of the Drafting Committee meetings can provide details. They are online: http://www.webcom.com/legaled/ETAForum/mtgrpts.html, notably the meetings of September 1997 and January 1998.

[68] *Infra* text accompanying note 80.

discussed below.[68] The working group of the United Nations on electronic signatures aimed to give more substance to the provisions of Article 13 of the 1996 text, but there too, efforts to draft clear attribution rules ended up much narrower than originally hoped.[69]

Where legislation is silent on attribution, parties to electronic transactions will have to satisfy themselves of the origin of electronic documents and signatures in the usual way they authenticate any document. A technology-neutral statute can give little more help without hampering parties who choose their own communications methods. Statutes that say more about the technology may permit themselves to say more about attribution as well.

5) *Hybrid general rules:*

As the Utah model fell into question, attempts were made to find technology-neutral statutes that would nevertheless recognize that some kinds of e-signatures were more reliable than others. Likewise it was recognized that the test of "appropriate reliability" for electronic signatures under the 1996 Model Law gave little guidance to potential signers on whether their signatures would be upheld if challenged. The two motives have produced similar results: legislation that combines a general permission to use electronic signatures with special legal results for electronic signatures that met special rules. The latter class, often known as "secure electronic signatures", are generally described in terms first set out in the United States by the National Institute of Science and Technology (NIST) in the early 1990s.

The most solidly drafted of these was the Illinois *Electronic Commerce Security Act* of 1998.[70] It was followed by Singapore's *Electronic Transactions Act* in 1998,[71] and also in several other countries.[72] The U.N. Model Law on Electronic Signatures of 2001 uses similar terms to describe signatures that are presumed to be as reliable as required by the 1996 Model Law.[73] The E.U. Directive on Electronic Signatures[74] describes "advanced electronic signatures" in similar language as well.

---

[69] See the reports of the meetings of UNCITRAL's Working Group on Electronic Commerce, notably for July 1998 (A/CN.9/454, paras. 40-53); for February 1999 (A/CN.9/457, paras. 99-107, and Working Paper WP.79 paras. 31-33); for September 1999 (A/CN.9/465, paras. 68-77); and for February 2000 (A/CN.9/467, paras. 44-71). They are all online: http://www.uncitral.org/english/workinggroups/wg_ec/index.htm.

[70] Illinois *Electronic Commerce Security Act*, 1998, 5 Illinois Compiled Statutes 175, online: http://www.legis.state.il.us/ilcs/ch5/ch5act175articles/ch5act175artstoc.htm.

[71] *Electronic Transactions Act*, Singapore, 1998, online: http://www.cca.gov.sg/eta/index.html. It was the first to implement the U.N. Model Law on Electronic Commerce.

[72] Examples are Bermuda, Hong Kong and India.

[73] U.N. Model Law on Electronic Signatures, *supra* note 56.

[74] *Supra* note 51. The appendices on technical requirements for qualification are more detailed than in the other texts mentioned.

These characteristics were, in the words of the Illinois Act[75]:

- The signature is unique to the signer in the context in which it is used;
- It can be used to objectively identify the person signing the electronic record;
- It was reliably created by such identified person (e.g. because some aspect of the procedure involves the use of a signature device or other means or method that is within the sole control of such person and that cannot be readily duplicated or compromised);
- It is created and linked to the electronic record to which it relates, in a manner such that if the record or signature is intentionally or unintentionally changed after signing then the electronic signature is invalidated.

Illinois allowed the Secretary of State to designate electronic signature systems that met these criteria, so that litigants would not have to prove compliance with them in every case. Article 7 of the 2001 Model Law does the same; it contemplates a declaration by an authorized body that a particular method of creating an electronic signature is reliable.[76] Although the article does not intend for countries to designate how reliable e-signatures *must* be done, only particular ways that are deemed to be reliable, there will be much pressure in practice for signers to use the approved methods.[77] .doc. Any such accreditation must be in accord with recognized international standards, to reduce the chances of this: 2001 Model Law art. 7(2). The recognition rules discussed below also bolster this approach.

Where the criteria for a secure electronic signature were present, the Illinois Act provided a presumption of attribution, i.e. that the signature actually came from the person who apparently made it. The 2001 Model Law does not provide presumptions, except that the signature meets a legal requirement.[78] The same result follows under the E.U. Directive: the advanced electronic signature is to be given the same legal status as a handwritten signature.[79]

The Canadian federal government has adopted the *Personal Information Protection and Electronic Documents Act* (PIPEDA), Part 2 of which deals with

---

[75] *Supra* note 70, s. 10-110.

[76] This body may be in the public sector or may be a private body authorized by the public authorities to give such accreditation. 2001 Model Law, art.7, and Guide to Enactment, para. 135.

[77] Some concerns have been expressed that countries will introduce disharmony in what is acceptable, by accrediting inconsistent signature methods under this article. See Steptoe & Johnson LLP, "Commentary on the UNCITRAL Model Law on Electronic Signatures", May 2001, online: http://www.steptoe.com/webdoc.nsf/Files/UNCITRAL/$file/UNCITRAL

[78] Article 6(3). Article 6(4) says that this reliability may be challenged by any means, i.e. it turns the rule into a presumption. To date no country has adopted the Model Law on Electronic Signatures.

[79] *Supra* note 51, art. 5.

electronic documents.[80] It is a hybrid statute as well. Some of the signature provisions simply allow signature requirements to be satisfied electronically by use of an e-signature in the form to be prescribed by regulation.[81] However, several sections contemplate the use of a "secure electronic signature".[82] For example, one can use a secure electronic signature to create a certificate signed by a minister or public official that is proof of a fact or admissible in evidence. A secure electronic signature may serve as a seal, if the seal requirement has been designated under the Act. Affidavits may be made electronically if both deponent and commissioner of the oath sign with a secure electronic signature. Declarations of truth may be made with such signatures, in similar circumstances. Witnesses may sign under similar conditions. It is worth noting that unlike most of the hybrid statutes, the Canadian federal law gives no choice about whether to use a secure electronic signature. To sign electronically and validly within the meaning of the provisions named, people must use the secure electronic signature.

A "secure electronic signature" is not defined in the Act, except as "an electronic signature that results from the application of a technology or process prescribed by regulations made under subsection 48(1)". That subsection sets out the usual provisions for signatures of this type, as we have discussed above. The intention is that in the first instance the only technology to be designated will be that of digital signatures certified by the Government of Canada, or those from systems cross-certified with the Government of Canada Public Key Infrastructure.[83] At time of writing, regulations on secure electronic signatures were still at the drafting stage.

Hybrid legislation reflects the nature of authentication among private parties: different weight is given to different documents and to different technologies. Business people, at least, are likely to prefer the simpler part of the hybrid statutes, that any electronic signature meets a legal requirement. Once that requirement is met, going on to show just who signed it and why one's attribution is reliable is a separate issue. The party seeking enforcement must prove fact, not compliance with a vague or complex legal standard. Proving fact is easier, and a better basis for the authentication process, which is a judgment about the acceptability of risk.[84] As noted in the earlier discussion of the

---

[80] S.C. 2000 c.5, online: http://lois.justice.gc.ca/en/P-8.6/index.html.

[81] One will have to see the regulations to know if technical standards will be imposed even where secure electronic signatures are not needed under the Act.

[82] PIPEDA, *supra* note 80, ss. 36–46.

[83] Cross-certification allows two or more public key infrastructures to recognize each other's certificates and thus signatures. More on the Government of Canada PKI can be found online: http://www.cio-dpi.gc.ca/pki-icp/index_e.asp. Some provincial governments are developing public key infrastructures as well, and they hope to be cross-certified with the federal PKI.

[84] This argument can be tested by examining practices under the European Electronic Signature Directive, *supra* note 51. How many businesses use the advanced electronic signature to achieve equivalence to a handwritten signature, and how many rely on other electronic signatures that the Directive protects against discrimination within the E.U. solely because they are electronic?

function of a signature, the presence in fact of a signature is only one way in a commercial transaction to provide evidence of attribution. Business parties may in practice choose to satisfy themselves about attribution through procedures that do not qualify as a signature at all, and certainly not as an advanced or a secure signature.[85]

It is arguable that the detailed requirements in the hybrid legislation will not be easy to meet, judging from the difficulties in setting up public key infrastructures in Canada and the United States.[86] Even when the requirements are met on their face, the assurances of identity of the signatory are vulnerable, depending on the design of the system. Presumptions of attribution are risky outside the context of a state-supported or at least state-regulated system, where the technical standards and trustworthy procedures are well known and expertly applied. But it is important that the hurdles to using electronic documents for legal effect should not be set too high for all purposes. One will recall that most of Canada[87] and the United States, at least, have done without any specific reliability test for electronic signatures, at least in commercial documents. The need for the technical part of hybrid legislation does not appear to be overwhelming.

B. *Other Rules Affecting Authentication*

Some legislation on authenticating electronic records has gone beyond the strict requirements of authenticity. The three most notable topics affect evidence, liability and the recognition of foreign electronic documents or signatures. While such provisions are not necessary to a sound authentication regime, they are not irrelevant. As authentication is a matter of evidence in the everyday sense, so it affects the rules in the courtroom sense. Liability rules may push all the parties to electronic records to conduct themselves in a way that will maximize the chances that the records they produce will be reliable. Recognition rules generally increase the confidence with which one may deal with foreign

---

[85] Indeed, the identity of the other party is often less important than its solvency or the quality of its goods or services. For this reason one distinguishes sometimes between identification – who is this person? – and authentication – is this the person it purports to be? This paper uses the term "authentication" to cover both aspects, however.

[86] An anecdotal account appears in S. Berinato, "Only Mostly Dead", in CSO Online, May 23, 2002, online: http://www.csoonline.com/alarmed/05232002.html. While the detailed parts of most hybrid laws do not expressly require digital signatures and a PKI, many people have thought that this technology was the most likely to fulfill the statutory requirements.

[87] As noted earlier, the Manitoba Act has a reliability test for electronic signatures: *supra* note 45, s. 13(1). To date the part of the provincial statute on signatures is not in force, and no regulations have been made about them. Prince Edward Island's *Electronic Commerce Act*, S.P.E.I. 2000 c.31, defines electronic signature in terms similar to those of PIPEDA's secure electronic signatures, but without any other consequence to meeting or failing to meet the standard: ss. 1(1)(b) and 9.

electronic documents, which promotes international commerce. The rules ensure that foreign methods of authentication are accepted where the documents are to be used, while protecting the country of use by requiring that the reliability of the foreign methods be equivalent to those in the country of use.

1) *Evidence Rules*

At common law, documents need to be "authenticated" before they are admitted in evidence. This means that they must be supported by evidence capable of supporting a finding that the documents are what they purport to be.[88] Generally this process is not demanding; it can be met in most cases by having a sworn witness testify to the identity and source of the document. In proposing its Uniform Electronic Evidence Act, the Uniform Law Conference codified the common law authentication test, without making special provision for electronics.[89] The statute modified the means of satisfying the "best evidence" rule for electronic records, and the Conference considered that no additional hurdles to admission should be included in the process of authentication.

Thus it can be said that the law of evidence does not demand of documents, electronic or not, processes of authentication as rigorous as those of other areas of the law. This is understandable, as authentication in evidence merely gets the document in the courtroom or tribunal door, after which a trier of fact must decide whether the document is really taken for what it purports to be, and what result follows. In commercial or public law matters, authentication is more closely related to actual reliance on the document with legal effect. The need for protection by authentication rules is greater.

In general the common law does not give signatures or signed documents any special status as evidence, except for documents signed by public officials, which may be "self-authenticating", i.e. admitted without proof of origin beyond that signature. As a result, most of the U.S. and Canadian statutes on electronic records discussed here say very little or nothing about evidence questions. The UECA is silent on evidence, and the Uniform Electronic Evidence Act also says nothing about signatures. The UETA, like the 1996 Model Law, says only that evidence of a record or signature may not be excluded solely because it is in electronic form.[90] The U.S. federal statute on electronic signatures is silent on evidence.

---

[88] S. Schiff, *Evidence in the Litigation Process*, 3rd ed. (Carswell, Toronto, 1988) at 768.

[89] The *Uniform Electronic Evidence Act*, [1998] Proceedings of the Uniform Law Conference of Canada 164, online: http://www.ulcc.ca/en/us/index.cfm?sec=1&sub=1u2, s.3. The Uniform Act has been implemented in most jurisdictions. See the implementation chart for the UECA and the Uniform Electronic Evidence statute online: http://www.ulcc.ca/en/cls/index.cfm?sec=4&sub4d.

[90] UETA, *supra* note 49, s. 13. 1996 U.N. Model Law, *supra* note 34, art. 9.

Many of the uses of secure electronic signatures in the Canadian federal legislation support an evidentiary use, however.[91] PIPEDA amended the Canada Evidence Act[92] to allow the creation by regulation of presumptions of the association of secure electronic signatures with persons, and of the integrity of information in documents where a secure electronic signature is used. No such regulations have been made to date.

In Quebec, an electronic signature is approved where made "by means of any process that meets the requirements of article 2827 of the Civil Code",[93] which is part of Book VII of the Code on evidence. No special rule of admissibility is provided. The Quebec statute did amend one article of the Civil Code on the use of electronic documents as evidence,[94] without mentioning signatures in particular.

By contrast, the E.U. Directive on Electronic Signatures provides that advanced electronic signatures must be admissible in evidence, and that other electronic signatures may not be denied admissibility on grounds of their electronic form or because they are not qualified in one element or another.[95] To the extent that documents are more readily admissible when signed, and that courts will be hard to satisfy in practice with less than an advanced signature, compliance with the requirements for an advanced signature would be more important in European law than in Canadian or American jurisdictions.

That said, the choices for private and public parties may be made easier by the development of technical standards for electronic signatures.[96] The Uniform Electronic Evidence Act expressly allows courts to consider conformity with applicable standards in determining the admissibility of electronic records.[97]

2) *Liability Rules*

For documents used between two parties, there seems to be little desire to legislate on the liability of the parties. The usual rule is that the relying party takes the risk of inauthenticity, subject to whatever rights it may be able to enforce against negligent or deceptive trading partners. Traditional authentication rules are more likely to invalidate non-compliant documents than they are to impose liability on their users. For three-party systems, with a certification authority between the signer and the relying party, some countries have wanted

---

[91] See the items requiring a secure electronic signature listed above, text accompanying note 82.

[92] R.S.C. 1985 c. C-5, new section 31.4. Manitoba made similar amendments; see part 7 of its statute, *supra* note 45, s.38, creating new section 51.5 of the provincial *Evidence Act*. No regulations have been made under that provision.

[93] *An Act to provide a legal framework for information technology*, *supra* note 46, s. 39.

[94] *Ibid.*, s. 77 repeals and replaces article 2837 of the *Civil Code of Quebec*.

[95] E.U. Directive, *supra* note 51, art. 5.

[96] Some work in that direction is mentioned *supra* note 18.

to legislate to ensure that parties knew what their responsibilities were. Another aim was to allocate liability in a way to promote activity of trusted third parties, who have sometimes been considered essential to the development of reliable e-commerce.

This latter motive was strongly evident in Utah, which relieved the third party of liability if the rules were followed. The Utah system was however much criticized on its liability (and attribution) rules: it was said to distort the true value of the technology to legislate liability. The real risks would in any event become apparent and would be reflected in insurance premiums and the prices of services. Essentially the digital signature statutes were said to be allocating risk by law differently than how the real risk fell.[98]

The U.N. Model Law on Electronic Signatures says that parties must "bear the consequences" of failing to comply with the conduct set out in the Model Law.[99] This adds little to current law. It is however worth noting that the responsibility of the relying party may be different from that of the signer and of the certification authority, called in the 2001 Model Law (and the E.U. Directive) the certification service provider (CSP). Negligence of the signer or CSP is very likely to harm others. Negligence of the relying party harms only the relying party, who may end up with a contract with the wrong person, or with no one. The consequences of the relying party's negligence is thus not to be liable to someone else but to be unable to blame anyone else for the loss (though liability could be shared in some cases.)

The E.U. Directive on Electronic Signatures requires member states of the Union to ensure certain liabilities of the CSP but also provides for CSPs to limit their liability by appropriate disclosures. Otherwise there are no standards or values for liability.

The Quebec statute on information technology is essentially a technology-neutral statute but nevertheless makes detailed provision for the activity of persons who certify the identity of signatories of technology-based documents,[100] and it sets up a voluntary accreditation scheme for them.[101]

Concerns have been raised about liability provisions even of the level of generality of the U.N. Model Law on Electronic Signatures. They are drafted with a three-party model, really a digital signature/PKI model, in mind, but apply on their face to any electronic signature. The conduct they promote may be too demanding for some kinds of signature. In addition, the terms are sufficiently general that inconsistent implementation is likely, and this will be confusing for commercial parties – in any of the three roles – that want to operate

---

[97] *Uniform Electronic Evidence Act*, *supra* note 89, s.6.

[98] See Biddle, *supra* note 29.

[99] 2001 U.N. Model Law, *supra* note 56, arts. 8, 9, and 11.

[100] Quebec statute, *supra* note 46, s.47ff.

[101] *Ibid.* ss. 51ff. Further, Quebec provides for the liability, or the exemption from liability, of communications intermediaries like Internet service providers: ss. 22, 36, 37.

internationally. The responsibilities of the parties may often be better determined by contract among themselves. It also needs to be clear whether the party autonomy permitted by such legislation allows parties to change the rules of conduct and liability or whether these rules are mandatory in all cases.[102]

3) *Recognition Rules*

The use of electronic documents and especially the Internet has stimulated the need for consistent rules for recognizing foreign or interprovincial documents. One country's authentication rules are not applied only to its own residents' records. The more consistent these rules are, the more confident people will be to trade across borders by electronic means.

Where different countries are using third-party certification processes to authenticate electronic records, one hears of "cross-certification" to ensure the use of the records in another country. A certification authority in one country certifies a document on the strength of the certificate of a certification authority in another. Cross-certification depends on very detailed technical coordination of certification standards and operations among participating CAs. (The concept appears for use within countries as well as across borders.) While national cross-certification agreements exist, they seem more at a demonstration level for the moment.[103] 01_12_98_124.htm. They also are restricted to certification models, i.e. they are technology-specific.

It has become more common to speak of "cross-recognition", or simply of "recognition", of foreign electronic records. "Cross" suggests a mutuality: A recognizes B's records if B recognizes A's records. Given the speed and unpredictability of electronic commerce, it is likely to be more productive for a country to recognize electronic records from anywhere that meet its standards, without concern for reciprocity.

The U.N. Model Law on Electronic Signatures makes the location of the origin of an electronic signature or certificate irrelevant to the recognition of the document.[104] Likewise the place of business of the issuer of the certificate or of the signer is irrelevant. Implementing states are to give the same legal effect to a foreign signature or certificate that a domestic

---

[102] See the Steptoe & Johnson LLP article, *supra* note 77.

[103] See for example the cross-certification agreement published between Canada and Singapore of June 1998 – announced with some fanfare at the time, it is hard to find a trace of it now. Government of Singapore, "E-Commerce Timeline", online: http://www.ec.gov.sg/singapore/timeline.html; Entrust Technologies, "Entrust Technologies Announces Participation in First-Ever International Public-Key Infrastructure Cross-Certification Agreement", December 1, 1998, online: http://www.entrust.com/news/files/

[104] 2001 Model Law, *supra* note 56, art. 12(1).

signature or certificate would have, if they have substantially equivalent reliability.[105] (Exact technical conformity is not required.)

This language is chosen to allow for a range of degrees of reliability. Thus the domestic rules on authentication can be respected. If a country insists on high reliability for particular kinds of documents, it can insist that foreign electronic records demonstrate equivalent reliability at that high level. Lower levels of reliability may be met by lower level foreign records.

However, the rules on reliability are to meet "recognized international standards" for reliability.[106] This important provision intends to prevent a multiplicity of standards, including those that might be imposed as non-tariff barriers to trade. The Guide to Enactment of the 2001 Model Law points out that such standards may originate with public or private bodies and may be « standards » adopted by official standard-setting bodies, or guidelines.[107] No doubt there will be some kind of unofficial hierarchy in favour of public standards, if an accreditation authority found that applicable standards varied when it needed to decide about signing methods.

Finally, the new Model Law allows parties among themselves to agree to their own standards, which are to be recognized unless they are invalid under applicable law.[108] This language echoes the limits to party autonomy on domestic signatures, discussed earlier. Implementing countries should be slow to intervene in such private decisions, but if their authentication rules are particularly important to them, they are allowed to do so.

While the language of the U.N. Model Law deals only with signatures and certificates, its principles (non-discrimination against foreign records, equivalent reliability and broad though not limitless party autonomy) are readily applicable to any other rules affecting the authentication of electronic records.

V. *Conclusion*

Authenticating a document is an exercise of judgment, of balancing the risks of reliance against its benefits. Sometimes the state intervenes to require certain forms to be observed, in order to protect the interests of parties or of the state itself. Electronic documents present new challenges, in part to estimate if the current rules are sufficiently strong for them, and in part, conversely, to see how the current rules can be made flexible enough to accommodate them.

An increasing body of legislation and international models for legislation exists to guide parties that deal with electronic records. Most of the laws leave

---

[105] *Ibid.*, art. 12(2)(3).

[106] *Ibid.*, art. 12(4).

[107] *Ibid.*, Guide to Enactment, para. 159.

[108] *Ibid.*, art. 12(5).

an appropriately broad scope for varied security processes among commercial parties, while spelling out more details for dealings with public bodies. The trends of minimalism and technology neutrality dominate but do not hold the field exclusively. Time and technology will tell if the legislation promotes the traditional values of authentication rules or if it will need to change to meet the true needs of the increasing numbers of users of electronic records.