The EDI Law Review **6**: 47–63, 1999.

The Authentication of Digital Legal Records

JOHN D. GREGORY[1]
General Counsel, Policy Branch, Ministry of the Attorney General (Ontario), Canada

Abstract. The nature of digital legal records makes their authentication a special challenge. Authentication describes a determination of whether a set of data is a record and where it comes from. It should not include assessing the record's integrity. The variety of uses of different classes of digital legal records ensures that no single legal rule will be appropriate to govern their authentication. In particular, digital signatures are not in themselves a particularly good tool of authentication, although they probably work better for public legal records than for private ones.

Key words: authentication, electronic records, electronic signatures, digital legal records, digital signatures, evidence

One of the challenges facing people who want to use information technology to create legal relationships is authentication of the records of those relationships. How do we know what any electronic message is, and how can we be sure where it came from? The theme of this presentation is that there is no single solution to this challenge, no "magic bullet" that can end all uncertainties. But the uncertainties can be reduced significantly.

To understand the possibilities, we have to look at what digital legal records are and how they may be used.

Digital Records

By "digital" we refer to something made up of bits, i.e. binary digits - a pair of digits, either one or zero. In a computer system, the 1s and 0s indicate the presence or absence of an electronic current, or instructions to let a current pass or not. Strings of these instructions can constitute a message. The digital instructions may be transmitted by electronic, magnetic, optical or other means. One often uses "electronic" when one means "digital", and this presentation will do so too.[2]

Bits do not care what they are.[3] There is nothing in the essence of instructions about 1s and 0s that make a collection of bits display a record, or play music, or operate a machine. One cannot tell by "looking" at the bits, or the electrical instructions, what their purpose is.

In the case of *United States of America v Thomas*,[4] the defendant was charged with distributing pornography across state lines to Tennessee by transmitting it by wire from a California electronic bulletin board. The defendant argued that all he transmitted was a collection of 1s and 0s, and if one were to write out the strings of bits on paper or on a wall, no obscene meaning could be detected. However, the defendant was convicted. So there must be something more to a digital record than 1s and 0s.

A number of organizations have examined how one can replace writing electronically. The common term these days in North America, at least, is "record". An American Bar Association study group proposed the term as best suited to represent a "media neutral" phenomenon, i.e. information on paper or in digital form or otherwise.[5] This definition has been used by the National Conference of Commissioners on Uniform State Laws, notably though not exclusively in recent revisions to the *Uniform Commercial Code*, produced by NCCUSL and the American Law Institute.

That definition of "record" is "information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form."

The United Nations Commission on International Trade Law (UNCITRAL) adopted in 1996 a Model Law on Electronic Commerce.[6] The Model Law works in two stages. First, it defines a "data message" as "information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy". Article 6 of the Model Law then describes how a data message can satisfy a legal requirement for writing: "if the information contained therein is accessible so as to be usable for subsequent reference."

The Uniform Law Conference of Canada has adopted a *Uniform Electronic Evidence Act* for use by Canadian provinces, territories, and the federal government.[7] It defines "electronic record" as "data that is recorded or stored on any medium in or by a computer system or other similar device, that can be read or perceived by a person or a computer system or other device." This definition builds on definitions of record in the *Canada Evidence Act*[8] and the definition of "computer system" in the *Criminal Code of Canada*.[9]

These definitions of record have some common elements, despite their divergences: they do not say what a digital record will look like, and they do not say how to retrieve it or to display it so it can be perceived or accessed. This is because there is no "natural" form of digital record. The question is how to make bits function as information in the right way. The person assembling the bits has to choose how to make them function in this way.

What the "right" way is depends on what the record is for. In short, what makes a collection of bits into a record is the intention of the creator of the collection. This intention may be expressed by a choice of hardware and software and sometimes of a mode of transmission.

In order for the intention to be communicated, it must be shared by the recipient or user of the record too. In the *Thomas* case referred to earlier,[10] the defendant's software was able to understand the bits coming through to it as images that the court found were pornographic. The shared intention of the creator and recipient turned out to be against the law in Tennessee.

One will note that this is different in kind, not just in degree, from paper. Marks on paper will readily be understood as a record, even if the marks are incomprehensible to the person who tries to make them out. The intention to make a record can be detected even if the content of the record is not. It is usually possible to tell quickly if the marks are random or meaningful.[11] One has dealt with paper for a long time and its conventions are understood. However, a collection of bits may not be information of any kind; it may just be static.

While there is no "natural" form of an electronic record, there may be a narrow intent or a focussed intent of the creator. Consider the language of the *Provincial Offences Act*[12] providing for electronic tickets for minor offences such as speeding. Section 76.1 of the Act says that a document may be in electronic format if it is in a form permitted by regulation. The regulation says that a document in electronic format is permissible if it is "intelligible in a form prescribed under the Act."[13] The Legislature has intended to harmonize the physical appearance of electronic and paper records, at least at the time of this regulation. This may be useful for court administrators and judges who may look at paper and electronic tickets at the same time.[14]

In the absence of statutory direction, however, a digital record is not "better" because it "looks like" a paper record when displayed or printed. Some people argued in Ontario's photoradar team that each ticket when transmitted and stored should be part of a full word-processed file. They were wrong. Word processing program bits are no different from other codes or clues to the creator's intention. What was essential to the process was being sure of that intention. A speeding ticket was electronic information in a structured format; it was in fact very much like electronic data interchange. All that the photoradar project needed was enough bits to tell the relevant computers which standard form under the Act they were producing or receiving, plus the variable information: names of the defendant, date and place and nature of the offence, and so on.

Digital Legal Records

These tickets are clearly legal records, not just any records. What might distinguish a legal record from another type of record? The main feature is the intention of the creator that legal consequences should flow from the record. A second feature is the existence of some kind of authoritative interpreter of the record, in other words someone who can decide whose intent is communicated accurately and decide what legal effect the record has.

This latter feature may be important if parties dispute the alleged shared intention about the record. If I put the CD-ROM version of the Statutes of Ontario in a CD player, I will get neither statutes nor music. So do I have a record in some meaningful sense, even if the CD-ROM properly used will give me the statutes? At what point is the collection of bits not a record at all? This is to some extent the same as asking if the recipient or intended user should have been expected to share the intention. Is the recipient's failure to share the intention wilful, or negligent, or fortuitous? With legal records, someone – a court, an arbitrator – gets to decide.

Of course not all legal records are the same. One may divide them into three classes: public legal records, private legal records, and mixed, i.e. records with public and private elements.

Public legal records are those created by public authorities or under their direction: statutes, regulations, judicial decisions. For these records, the state can be said to impose its intent about the form of the bits to be understood as a record. The citizen must share the intent because the citizen must know the law. As a matter of practicality, of course, governments generally publish their legal records in accessible formats, to help ensure wide distribution.

Private legal records have legal effect for their maker or the parties to them. One thinks of contracts, or appointments like powers of attorney, but also of single-party records like wills. The parties to such records have to share the intent as to form. Indeed the trading partner agreements that underlie many traditional EDI relationships spelled out in detail the method of generating and communicating and storing the bits so they would be understood by both sides.[15]

Mixed legal records vary widely. Perhaps the most useful distinction for present purposes is whether the records must be placed on a public file, or submitted to government in some way. One thinks of tax returns, or applications for benefits of some kind, or documents to support registration or the grant of some legal status, such as incorporation. Some private documents depend on submission to a public authority for effect against third parties. Land transfers in many legal systems, or arbitrators' decisions submitted to a court for enforcement, are examples. In these cases, it is likely that government will prescribe the format: the intention to create a record derives from the legal duty and the intended format is essentially imposed.

Other "mixed" records may be created or communicated or retained pursuant to statute, and the statute may or may not prescribe form as well as content. For example, section 445 of the *Bank Act*[16] requires a bank to provide an account statement to its customers. It says that the information "shall be provided in writing or in such other manner as may be prescribed." Landlord and tenant statutes often require notice in writing of increases in rent, for example. To a large extent the intent needed to create a record will have to be shared between the originator and the recipient or user of the record, but the originator may have to answer to the government for its choices.[17]

Authenticating Legal Records

So far we have reviewed the nature of "digital" "legal" "records". What are the challenges of authentication of these records?

Authentication, in this context, means the detection and demonstration of the intention that created the record. Is the intention sufficiently clear and sufficiently shared that the recipient can rely on the collection of bits that it has received? Some of that question of course involves analyzing the legal impact of the record, which is different from authentication. Authentication is the first step; without it, one may not bother to worry about the legal effect. However, the intended legal effect will influence the degree of authentication one looks for in the record.

Put in a more traditional way, authentication is the determination of what a record is (is the collection of bits a record at all? What is it?), and where it comes from. Sometimes it is suggested that authentication requires demonstration of the integrity of the record as well. I am sceptical of this, as will be discussed later.

In my view authentication is done by the recipient or prospective user of a record, and not by its creator. Applying the term to something done by the creator of the record leads to unfortunate confusion. The creator does not need to discover his or her intention and may not know whether it will be shared. The range of possible uses of the record that leads to a range of possible methods of authenticating it are a matter for the relying party. Rules directed to the creator risk being too inflexible for potential relying parties to benefit from, or just irrelevant to the relying party. There is no question that the creator of a record can make authentication easier or harder at the time of creation, for example by signing the record. How this is done is a separate question from the nature of the process of authentication.

However, applying "authentication" to acts of the creator is well established, at least in the United States. For example, the definition of "signed" in the *Uniform Commercial Code* (UCC) includes the presence of "any symbol executed or adopted by a party with present intention to authenticate a writing."[18] The draft of Article 2B of the UCC on licensing uses "authenticate" instead of "sign" to refer to a process intended to give legal effect to a record.[19]

In the rest of this paper I will use the term "authentication" only as something done to an existing record by the recipient or prospective user.[20]

How one authenticates a purported record depends on the purpose of authenticating it and the nature of the legal record itself. For example, one would apply different standards to authenticating a statute than to authenticating a contract.

One may distinguish at least four classes of purpose of authentication.

– a general commercial or private purpose: Do I rely on this apparent offer to sell me something, or buy something from me? Is this my late uncle's will? We will return in more detail to this category.

- a governmental purpose: Will the government rely on the record, to accord status or to grant benefits? Standards may vary, depending for example on whether public funds are to be paid as a result.
- an evidentiary purpose: Can I use this record in court or with some other official decision-making body? The common law has developed standards for the use of documentary evidence, which must be authenticated. The Canadian test of authentication to have a record admitted in court is relatively weak: is there evidence capable of supporting a finding that the record is what it purports to be?[21] Once the proponent of the evidence shows that the record might reason ably be found to be authentic, the record is admitted, and the trier of fact – judge or jury – will weigh it with the other evidence to decide whether it is authentic and whether it matters.

  Some types of records are considered to be "self-authenticating". Because of their form or their origin, they are deemed to pass that first test without external evidence of identity or source. Examples are statutes and regulations printed by the official government printer[22] and records from public registers, certified by the public official who has custody of the record.[23] Another example is a document under the seal of a notary public.[24] For these records as well, evidentiary authentication gets them into the courtroom; it does not determine their legal effect after that.

  It will be noted that neither the standard test nor the self-authenticating process guarantees the genuineness or integrity of the record. They provide enough proof of these qualities that the court will deal with the record until contrary proof is made. To that extent they can be considered an "appropriateness" test of authenticity. It is appropriate to let the court deal with the record once these demonstrations of authenticity have been presented.
- archival or record-management purpose: People whose duty is to keep records may impose a lower standard of authentication before they admit records to the system, because they may be required to keep all records, of whatever origin or reliability. The rules will depend on the organization that keeps the archives.[25] On the other hand, as time passes from the creation of a record, the only indication of authenticity may be that associated with the archived record.[26] For example, the legal status of lands or the ability to carry on activity on lands in parts of Canada may depend on the interpretation of treaties signed between Europeans and the First Nations a century or two ago.[27] The presence of the record in the official archives may be the only way of authenticating it after such a time.

Records managers face a number of challenges in authenticating records submitted to them and in maintaining the records in ways that allow them to continue to be authenticated as storage media evolve. These matters are beyond the scope of this discussion.

In the interests of economy of space, this discussion will focus on the commercial and private uses of authentication, though of course the ability to use a record in court is one factor a business person will consider in deciding to rely on a record.

In particular we will consider the legal rules that support or should support authentication. Especially in commercial matters, the law should not go beyond the practical needs of its intended beneficiaries, those who want to give legal effects to digital records. The same principle may apply even to public law purposes in such a practical field as authentication.

Practical Considerations

Three practical considerations tend to limit the need for a comprehensive legal rule on authentication.

- One may detect the intention of the originator of a record in many different ways. One may find a lot of sources of evidence of intention to create a record, and of whose intention it is. A single rule about authentication is unlikely to work for all purposes, unless it is so broadly worded as to be practically useless. We will discuss some of the possibilities in more detail later.
- We should not require or expect more certainty from techniques or rules applied to digital records than we have for paper records. Do we always check a signature on a paper record? Does even a normally cautious business person ask for photo-identification when meeting a new client? Do people mail legal documents by ordinary post? If we are prepared to rely on such potentially insecure ways of doing legal business in the paper world, we should not demand the electronic equivalent of an armoured car to do business digitally.

  One sees this in the UNCITRAL Model Law on Electronic Commerce,[28] where Article 7 deals with electronic signatures. An electronic signature meets a legal requirement that a record be signed if it links the record with its originator and the "method . . . used to identify the person . . . is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement." Elsewhere in the IFCLA conference one heard Raymond Nimmer, the Reporter for the UCC Article 2B project, talk about "commercially appropriate" authentication. What is appropriate will vary according to the threat of compromise to the record, the gravity of the consequences of compromise, the benefits of proceeding anyway, and the cost of taking steps to reduce the risk. These are standard risk management principles, and they apply to digital communications as elsewhere.

– The digital medium of these records does create some new challenges of form and content, new threats to attribution and integrity of the record. However, the medium does not change the legal content of the record or its legal effect. To decide whether to rely on a digital legal record, the recipient or potential user will have to ask the same questions as arise for paper records: what is this? Do I trust the originator? What is my obligation under this record, and what are the obligations of the other party? And so on.

  We should not require of an authentication system that it give answers to all these questions. We should not be trying to give more legal effect to electronic legal records than they need to offset the difference in the medium of storage and communications. Doing so would violate the core principle of the Model Law, in Article 5: "Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message." Demanding more authentication than is strictly needed to compensate for the electronic medium would be to deny some element of legal validity because of the medium.

With these three practical themes in mind, we can look at the legal structure of authentication. The first question is whether what one has is a record at all. If the content is intelligible, one may safely conclude one has a record. Someone intended the intelligible content. The chance that a collection of bits is intelligible at random is infinitesimal. The legal effect of the intelligible information is not a matter of authentication, though of course it will be important to the person who has the record.

The next question is what the record purports to be. This is separate from understanding its legal effect; it is really a question of identification and no more.

The final and most difficult question is where or who did the record come from. This is essentially a question of attribution. Much of the discussion of authentication turns into a discussion of attribution, in my opinion.

The additional element that some people look for in authentication is the integrity of the record: is it the real thing, has it been altered? But the usual techniques for authentication do rather little in practice to ensure integrity. A signature on paper is very weak evidence indeed that the signed paper record has not been altered, yet a signature is often considered the principal means of authentication. The real link between authentication – often by a signature – and integrity is that reliable attribution is a strong incentive for the creator of the record to avoid error and fraud, because sanctions, such as civil or criminal liability, can be imposed when one knows who made the record. But that does not make the attribution technique itself a guarantee of integrity. Any attribution technique will promote integrity for the same reason. Whether one accepts it will depend on what incentive the creator of the record is thought to have to err or deceive, and how vulnerable the relying party is to error or deceit.

As a result, in this paper I will not discuss authentication as demonstrating the integrity of the record.[29] We will look a bit more closely at digital signatures later; they have distorted the discussion of authentication because of their strong ability to verify the integrity of the digitally signed record.[30]

Signatures and Authentication

It is important to note that authentication does not depend on a signature. The law may not require a signature at all (or even a writing) to produce a legal effect. At common law, many oral contracts are binding. Where there is a record, a potential relying party will need to authenticate it even if it is not signed. No one would rely on a record, give it legal effect, change one's position in accordance with it, without knowing what it was and where it came from or who was behind it.

A signature is certainly often an aid to authentication. The prospective relying party may as a practical matter demand a signature on a record as a good quick method of authenticating it. Likewise, the law sometimes requires that records be signed, presumably because the legislators took the view that a signature provided reliable authentication where authentication was needed to protect the relying party. (Other features of signatures might also have influenced that requirement, though, including the desire for a cautionary ceremony, the usefulness of a formality to ensure attention to detail, and so on).

Even on paper, however, there is no one signature. A number of techniques or processes or marks may be used to sign. An X on a document may be a signature (or in some traditions, it may be a kiss!) A handwritten name, or initials, may be a signature. Sometimes the recipient will want more: a witnessed signature, a signature certified correct by a trusted third party such as a bank or a notary, a signature executed before two witnesses both present at the same time (for a will in the common law tradition). Again, it depends why one needs a signature. What constitutes a signature to meet a statutory requirement that a record be signed may not be satisfactory to convey greater legal effect, and certainly may not be satisfactory to someone who is simply suspicious by nature. Some of this variation depends on different legal rules and some of it on the practicalities as estimated by the parties, and of course some on the intention of the parties, as noted at the outset.

Likewise in the digital world there is no one signature. The header of an e-mail message may be a signature; the name of the sender typed at the bottom may be a signature, or may be if it has "[signed]" or "/s/" or some other conventional mark attached. Or one may digitize one's handwritten signature and incorporate it into the message. Or one may use signature dynamics and have a computer record of the speed and weight and directions of one's handwriting on a pressure-sensitive pad. Or one may use public key crypto-

graphy, with or without certification by a third party or by members of a web of trust. No one rule of law is likely to be appropriate for each method of authentication.

Scenarios of Authentication

Let us work briefly through two scenarios of authentication. In the first case, the prospective relying party has a record from a named source. In the second, the record has no named source.

1. A record from a named source: One thinks of a private document like a contract, or an offer to purchase or sell something. If the recipient wants to authenticate it, what evidence will suffice to tie it to the purported originator, not in the eyes of a court but in the mind of the recipient?[31] A number of possibilities arise:

- the record contains a recognized signature, possibly protected against compromise or restricted in access. It may be an agreed code, like a privately-exchanged Personal Identification Number (PIN). It may be a digital signature with privately-exchanged keys. It may be (some day) an open-system digital signature resting on a certificate from a trusted third party.
- the record appears authentic because of internal evidence. The terms of the deal as negotiated are in order. In short, does the originator of the record appear to know what he or she or it is talking about? Is the content credible as coming from the purported originator?
- the communications system may be sufficiently secure that its products may be trusted. Using a private bilateral communications line may suffice. One may trust the headers and routing codes to show that a secure system has been used. If I get an e-mail note on my office computer purporting to be from my Director, the system security within the Ministry gives me confidence to rely on it, even if the only indication of source is the header on the screen, or a typed name at the bottom. (If the header differed from the name, I would start to ask questions).
- In short, the communications system itself is a source of authentication. As Raymond Nimmer wrote a few years ago, "the creation of system-based assurances of authenticity constitutes a condition precedent for continued expansion in the modern use of systems in important market-places."[32]

A frequent hypothesis of electronic commerce is that large-value transactions will occur between people or businesses unknown to each other before the transaction, and a reliable authentication technique (such as digital signatures with trusted certification authorities) will be needed for people to rely on the commercial records they will receive. The hypothesis may be more speculative

than real. In any event, the prospective relying party will want to know a good deal more than the name of the originator. For example, one would want to know creditworthiness (will he pay?), the quality of the goods and services expected (should I pay?), the authority and legal capacity of the originator to engage in the contract, the time at which the record was generated or transmitted, and so on. Some but not all of these matters could be conveyed by some techniques of authentication – but only by stretching the usual meaning of the term, as well as most current technologies.[33]

In short, even if one achieves authentication of the record by finding out who sent it, the relying party will need more information. The relying party will have to decide if the apparent originator or the system can be trusted. Who or what one trusts is a matter of individual choice, based on individual purposes or intentions. It is difficult for the law to prescribe one method of building or satisfying trust. One size, or one legal rule, will not fit all.

2. A record from an unnamed source: Such a record may be a private or commercial record. In this case the potential relying party will be able to look to some of the same factors for authentication as with the record from the named source: internal evidence from content, evidence from the communications system, and the like. A person might choose to rely on such a record without the name. In some cases, the important factor will be to determine the authority rather than the identity of the originator of the record. For some purposes, indeed, authority is a feature of identity rather than separate from it. Authority seems likely to be one of the earliest extensions of the standard digital signature certificate, because of its importance. A record showing clear authority to contract may be as good as a record showing a named source.

More frequently, perhaps, records from an unnamed source may be public records, such as statutes or proclamations. The relying party does not care who it came from; it does matter that it originally came from the government or at least an official source. Even official documents may nowadays come from private publishers, perhaps under contract with the state. Reports of courts and administrative tribunals often fall into that class in Canada and the United States.

In these cases one might find two influences on the authentication technique. The first is the trust the prospective relying party accords to the system and the participants in it. A public record may be satisfactorily authenticated if the relying party can trace its origin as far as a respected law publisher, or a law library, or a law firm. A trusted source need not be an official source, but for the purposes of the relying party the record may be sufficiently authenticated to act on it.

The second influence is the nature of the prospective user. Different users of the record may have different standards. For example, official users, such as government departments or agencies, or the courts, may insist on official texts, not those privately published or downloaded from an unofficial World Wide Web site. We saw earlier that courts accept public records if certified

by a public official or printed by a state printer.[34] Similarly an official recipient of a digital record may want to see a publicly known authentication technique associated with a public office, such as the digital signature of the court, or of the legislature. The recognized publication system is required to authenticate for these purposes.

Digital Signatures

Despite the frequently-expressed goal of keeping the law technology neutral, i.e. equally applicable to all technologies, many people continue to be attracted to legal rules to support digital signatures in particular, generally based on certificates of identity, because of the apparent strength of public key cryptography. However, it is arguable that digital signatures are not a universally good answer to the question of authentication.

Public key cryptography is superb at ensuring the integrity of a record from the time it is signed to the time it is read (the signature is "verified"). One can rely on a digitally-signed record with complete confidence that it has not been altered in the specified time. For this reason, people have come to talk about assuring the integrity of a record as a feature of signatures.[35] Because of the usual association of signature with authentication, integrity is thought to be part of authentication. The argument of this paper has been, however, that authentication does not depend on signature but is a matter of attribution, and signatures are only one way of providing attribution (and digital signatures are only one kind of signature). Traditional signatures on paper are weak ways of showing record integrity, and other methods of attribution may be even weaker, while still appropriate for attribution itself. The advent of digital signatures has changed this character and started to influence the concept of authentication in general. In my view this risks misleading the inquiry about authentication into overly rigid technological paths, or suggest that only particular technologies can produce reliable authentication.[36]

It is ironic that digital signatures should be so influential in discussions of authentication, because public key cryptography itself does not perform the traditional function of a signature for authentication, namely attribution of a record to a person. Public key cryptography gives assurance that a message read with a public key was created by the corresponding private key. It says nothing whatever about who used the private key. Some additional element must be added to provide this information – the information at the heart of authentication.

The additional element is some kind of evidence of attribution, often from a trusted third party, a certification authority, though sometimes from the proposed relying party itself, sometimes from a more or less informal network

of contacts known as a "web of trust". How this kind of evidence is provided depends totally on the implementation of a public key infrastructure. It may be strong evidence or weak evidence. The market seems ready to offer a number of "levels" of certificate, depending on the authentication needs of potential relying parties.[37] But attribution to a person at any level of trust has nothing to do with the impressive mathematical technology of public key cryptography itself.

Digital signatures seem therefore a weak candidate for "magic bullet" authentication. However, if one is (still) looking for a general rule for authentication of legal records, it makes more sense to ask for digital signatures for public records than it does for private ones, for a number of reasons:

- the source of public legal records is not a stranger but the state, in some guise. The user knows who the source should be, and a trusted link to a name will probably be all that the user needs.[38]
- the public keys of public bodies can be very widely distributed, so the chance of someone risking falsification of the public key to deceive the recipient about the source of the record is small.
- likewise, the incentive to try to change the record is small, because the record will probably be available from other sources as well, making alteration easy to detect.
- the security techniques surrounding the integrity of the base or "original" record and the issuance of keys and the public key infra structure will be subject to public scrutiny so will probably be reliable (though some parts of the government may provide tempting targets to those who would like to cause disruption, just as the United States Department of Defence is subject to almost perpetual attacks on its computer security, mostly from "recreational" hackers rather than spies).
- since public legal records are not altered in normal use, the keys used to sign them can continue to be associated with them through several users. A statute with the digital signature of the legislature can be authenticated even if the electronic package has been transmitted through law firms and libraries and private hands over time. Private records passing through many hands would probably pick up alterations and a succession of private signatures, each of which would need to be verified to authenticate the record.
- official users of public legal records, such as other parts of the same government, can rely as well on their participation in a closed state communications system to add a level of confidence in the authentication.

In short, public legal records seem likely to be part of a trusted system that is still flexible to users of the records. Even using digital signatures as the means of authentication, the public system can be administratively less cumbersome than an open PKI in the private sector.

Conclusion

Where does this discussion leave us? We have seen that the nature of digital records requires that we determine the intention of the parties who use the record. The intention of the creator of the record sets its character. The intention of the user confirms that the digital message is a record and also influences the methods and standards for authenticating it. A lot of intentions are possible and a lot of legal effects may be given to these records.

As a result, the law should not prescribe a single method of authentication for digital legal records in order to give them legal effect. The potential users of such records should be allowed to assess their own risk, and to decide what they trust. Risk management in authentication is trust management. In some cases, "pretty good authentication" may be enough.[39] In other cases one may insist on the fullest possible security procedures, the best that current technology allows.[40]

Rarely will the legal system need to make such procedures mandatory. The role of legislation will more often be to ensure that the digital records do have their legal effect. Legislation and performance standards may support the development of authentication techniques but should restrict them as little as possible. This is the challenge facing UNCITRAL, the European Union, the OECD, and other bodies, public and private, trying to devise international standards for the authentication process. The trend is arguably towards less prescriptiveness and more flexibility, and the discussion in this paper indicates some of the reasons that this trend is the right one.

Notes

1. This text was developed from an address to the meeting of the International Federation of Computer Law Associations in Oslo, Norway in June 1998. The views expressed are those of the author and not necessarily those of the Ministry.
2. The 1998 Annual Meeting draft of the *Uniform Electronic Transactions Act* in the United States defines "electronic" as "of or relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities". See http://www.law.upenn.edu/library/ulc/uecicta/98am.htm. The Act is being drafted by the National Conference of Commissioners on Uniform State Laws.
3. David Masse,"The ABCs of Authentication: A is for Atom, B is for Bit, and C is for Care", in *The Official Version: A National Summit to Solve the Problems of Authenticating, Preserving and Citing Legal Information in Digital Form*, Canadian Association of Law Librarians, 1998. See http://www.callacbd.ca/summit/auth.html, para. 22.
4. *United States of America v. Thomas*, 74 F.3d 701 (1996).
5. The committee's work is described by Patricia Brumfield Fry in "X Marks the Spot: New Technologies Compel New Concepts for Commercial Law," 26 *Loyola of Los Angeles Law Review* 607: 1993.
6. The Model Law is at http://www.un.or.at/uncitral/en-index.htm

7. The Uniform Act appears at the Uniform Law Conference's web site, http://www.law.ualberta.ca/alri/ulc/current/eeeact.htm. It was adopted by the Conference in August 1998.
8. The *Canada Evidence Act*, Revised Statutes of Canada 1985 chapter C-5, section 30(12) defines "record" as including "the whole or any part of any book, document, paper, card, tape or other thing on or in which information is written, recorded, stored or reproduced . . .". See http://canada.justice.gc.ca/STABLE/EN/Laws/Chap/C/C-5.html.
9. The *Criminal Code of Canada*, R.S.C. 1985 chapter C-46, section 342.1, defines "computer system", "computer program" and "function" as a related set. The system runs a program that makes the computer perform a function. See http://canada.justice.gc.ca/STABLE/EN/Laws/ Chap/C/C-46.html.
10. See above, footnote 4.
11. The creator of a paper record has to intend to create it, too, but the intention of the person who may use it or receive it is not relevant to its existence as a record. The variety of ways to create a written record is less than for electronic records – and the variety of purposes of writing other than to create a record is arguably less than the number of purposes for which one may assemble electronic bits. One thinks of law-school examples of legally effective cheques written on doors or car fenders, but they are obviously not mainstream practices.
12. Revised Statutes of Ontario 1990 c. p. 33, as amended by S.O. 1993 c. 31, s. 1(27). Ontario statutes and regulations are on line at http://legis.acjnet.org/Ontario/en/index.html.
13. Ontario Regulation 497/94, July 1994, section 1.
14. See for more detail John D. Gregory, "Electronic Documents in Ontario's Photoradar System", (1995), 6 *Journal of Motor Vehicle Law*, 277.
15. See Amelia H. Boss, "Electronic Data Interchange Agreements: Private Contracting toward a Global Environment" 13 *Northwestern Journal of International Law and Business*, 31: 1992.
16. The *Bank Act*, S.C. 1991 c.46, as amended by S.C. 1997 c. 15 s.48. See also http://canada.justice.gc.ca/STABLE/EN/Laws/Chap/B/B-1.01.html.
17. Singapore's new *Electronic Transactions Act*, passed on June 29, 1998, provides that record retention rules may be satisfied by electronic means if one meets standards that are essentially those of Model Law article 10, and if one has the consent of the government authority that created the retention requirement. See the Singapore statute, section 7. (The bill that became the Act, unaltered, is at http://www.ncb.ech.gov.sg/view/ech/ETBmain.html).
18. *Uniform Commercial Code*, section 1–201(39). There are proposals to amend this provision, among others, to remove the reference to writing and to make it consistent with other revisions to the Code. See http://www.law.upenn.edu/library/ulc for Article 1 draft revisions.
19. UCC draft Article 2B, section 2B–102(3) (1998 annual meeting draft, http://www.law.upenn.edu/library/ulc/ucc2b/ucc2bamg.htm).
20. The European Union's draft directive on electronic signatures uses "authentication" consistently as a process done by a potential relying party. See http://www.mbc.com/legis/eu-digsig-dir.html.
21. Schiff, *Evidence in the Litigation Process* (Carswell, Toronto) 3rd ed, 1988, page 728: ". . . the judge will admit the item [of real or demonstratrative evidence] if and when there is sufficient evidence rationally permitting a conclusion that the item is what the proponent claims". The *Uniform Electronic Evidence Act* codifies this standard. See above, footnote 7, section 3.
22. *Evidence Act*, Revised Statutes of Ontario 1990, chapter E.23, section 25.
23. *Evidence Act*, Revised Statutes of Ontario 1990, chapter E.23, section 29.
24. *Evidence Act*, Revised Statutes of Ontario 1990, chapter E.23, section 45.

25. *Archives Act*, Revised Statutes of Ontario 1990, chapter A.27, section 3 requires that "all original documents, parchments, manuscripts, papers, records and other matters" be turned over to the Archivist 20 years after they are no longer being used. Section 6 prohibits the destruction of "official" documents. The term is not defined, but it implies some degree of authenticating the character of the records. It is not clear why a different test applies to transmission and to preservation.
26. *Archives Act*, Revised Statutes of Ontario 1990, chapter A.27, provides in section 7 that a copy of an original document in the custody of the Archivist certified under the hand and seal of the Archivist is "proof of authenticity" of that document, in the absence of contrary evidence.
27. For example, *R. v. Badger*, [1996] 1 *Supreme Court Reports* 771. See http://www.droit.umontreal.ca/doc/csc-scc/en/pub/1996/vol1/html/1996scr1_0771.html.
28. The Model Law on Electronic Commerce was adopted by the United Nations in 1996. See http://www.un.or.at/uncitral/texts/en-index.htm.
29. Of course the relying party will usually care about the integrity of the record. The analysis of how one might be satisfied about its integrity differs from the analysis of authentication, and the methods will differ. Public policy will often care about record integrity too, but at least the common law world offers very few rules about the creation or use of records that aim to promote integrity (beyond strong attribution). Statutes requiring double (or more) witnesses to wills may be one example. If relying parties are left on their own to establish the integrity of paper records, the law should not be more intrusive or restrictive for electronic records.
30. Some people have seen potential in digital signatures to create an electronic parallel to civil law notaries, whose role does extend to ensuring the integrity of notarized records ("actes authentiques"). See for example the discussion of "cybernotaries" at http://www.abanet.org/scitech/ec/cn/home.html. However, one should not exaggerate the extent to which notaries are now used in international transactions, and the role of cybernotaries in global electronic commerce may turn out to be limited.
31. The recipient will not ignore what the courts will do, but it may have its own standards for what it will accept, higher or lower than the courts' rules. One recalls the test of Article 7 of the Model Law on signatures: as reliable as is appropriate in the circumstances.
32. Raymond Nimmer and Patricia Krauthouse, "Electronic Commerce: New Paradigms in Information Law", 31 *Idaho Law Review* 937, 945: 1995.
33. For this reason, some people distinguish between "identification" – finding out about the person sent a message – and "authentication" – confirming that a message came from a known source. Thus authentication would not be a feature of commerce among strangers. See http://www.garlic.com/~lynn/aadsover.htm
34. Above, notes 22, 23.
35. See for example the March 1998 draft of the *Uniform Electronic Transactions Act*, http://www.law.upenn.edu/library/ulc/uecicta/eta398.htm, section 102(20)(C). This aspect has been removed from the more recent draft (cited in footnote 2 above) but remains in the equivalent definition in draft Article 2B of the *Uniform Commercial Code* ("authentication", cited in footnote 19 above).
36. Some people say that digital signatures (or electronic signatures generally) are more like a seal than a signature, because they are attached mechanically to the record. Perhaps if one used the language of seals, one would be less likely to influence the concept of authentication than one does when using the more common but arguably too compendious term "signature".
37. See for example Stewart Baker, "International Developments Affecting Digital Signatures", http://www.steptoe.com/WebDoc.NSF/Law+\&+The+Net+All/International+Developments+Affecting+Digital+Signatures.

38. This may be a forceful, though non-commercial, example of the distinction made in footnote 33 above, between identification and authentication.
39. See the related discussion in John D. Gregory, "Electronic Legal Records: Pretty Good Authentication?", in *The Official Version: A National Summit to Solve the Problems of Authenticating, Preserving and Citing Legal Information in Digital Form*, Canadian Association of Law Librarians, 1998. Available at http://www.callacbd.ca/summit/auth-johngregory.html.
40. For lack of space, this paper could not explore some of the special considerations that apply to public/private electronic records, such as those created by business for submission to public bodies. In addition, techniques and standards of record management and signature management are very important to the development of trust. The challenges of maintaining electronic records over long periods, as the technology evolves quickly to systems incompatible with their predecessors, may make reliance on the legal effects of such records especially risky where permanence, or near-permanence, is needed. We are not yet in the fully paperless age.