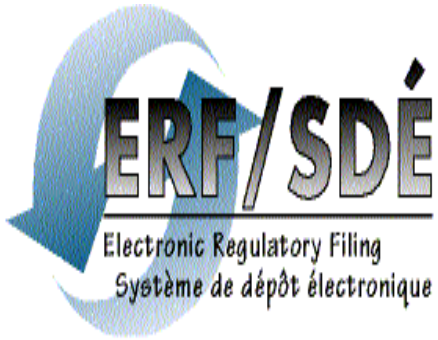
Electronic Regulatory Filing Project

a joint project of the National Energy Board and the Ontario Energy Board

Issues and Comment

January 15, 1999



National Energy Board
444 Seventh Avenue SW
Calgary, Alberta T2P OX8
(403) 292-4800
http://www.neb.gc.ca

Ontario Energy Board
2300 Yonge Street
P.O. Box 2319
Toronto, Ontario M4P 1E4
(416) 481-1967
http://www.oeb.gov.on.ca

CONTENTS

1. What is this report about?

The National Energy Board (NEB) and the Ontario Energy Board (OEB) are preparing to convert their information systems from paper to electronic form. Under the proposed Electronic Regulatory Filing system (ERF), all participants in the Boards' processes will deliver and receive regulatory information using computers. Paper documents will be the exception not the rule.

Note: This report has been prepared[1] to provide general background information pertaining to ERF. The legal discussion in it is of a general nature only and does not constitute legal advice. Readers seeking legal advice should consult their own advisors.

2. **What is the status of ERF?**

Beginning with a feasibility study completed in March 1993 , the Boards have proceeded carefully through cost benefit studies and progressive stages of analysis, design, and pilot implementation. During that time, regulated utilities, intervenors and others interested in the Boards' proceedings have participated in ERF workshops and planning sessions. A working prototype has already been demonstrated. Initial implementation is expected late in 1999.

3. **What questions have been raised about ERF?**

Two categories of questions include those that come from its relative novelty (like "How do I sign an electronic document?") and those that anticipate fundamental changes in the way the Boards operate (like "Will ERF lead to more written hearings?").

Questions of novelty will be resolved through training and familiarity. New technology invariably raises concern about risks. When photocopiers were introduced, for example, concerns were raised about accuracy of the reproduction. When fax machines were introduced, their use was scrutinized. Concerns were raised about the accuracy of fax copies, expense of faxing and the legality of facsimiles. Now both of these technologies, photocopying and faxing, are common, familiar and used almost without question, as are other familiar technologies like the telephone and television. That is, while there may still be problems with these technologies, most of the early concerns have been resolved not

[1] This report was written by Robin Nunn for the Ontario Energy Board and the National Energy Board (with special thanks to Stephen McCann, Charles Mathis and Claire McKinnon for their assistance).

through major changes in the technology but through better understanding of the technology and refining related processes.

Just as there are always concerns about potential risks in new technology, there is also a tendency to assume the opposite, that new machines, and in particular computers, are flawless. There is almost an expectation that if computers are not flawless then they are useless. Consider a common question: what is the possibility of losing track of a document among thousands of others in the computer system? This question is rarely asked about the present paper system. Everyone knows that paper can be lost. No practical computer system or paper system is without risk. Current systems used by the Boards, whether paper or electronic, are not flawless. A paper document may be misfiled or sent to a wrong address. The same errors can happen in a computer system. With proper design, however, errors may be tracked and corrected, whether the system is electronic or not. That is, risks of the proposed ERF system must be compared with the present system, not an abstract perfection that can never be achieved.

Between concerns about risk, on the one hand, and expectations of perfection, on the other hand, lies a middle-of-the-road issue: the danger of duplicating the present system with an electronic one. It may be possible instead, after examining the reasons for the present procedures, to adapt only necessary aspects to ERF. For example, handwritten signatures and affidavits are used now on documents filed with the Boards. Naturally there is a tendency to look for an electronic analogy such as a digital picture of a handwritten signature. Is this necessary? How is a picture, which can be duplicated by anyone, related to a handwritten signature that only the hand of the writer can make? Is a handwritten signature the only way to ensure that a document is “legal”? Are signatures examined and is forgery a likely event? These questions illustrate the opportunity both to avoid duplicating the present system and to design a better system. For more discussion of these specific questions, see the section in this report describing how documents will be signed in ERF.

Computers are impersonal. There is no human agent to act as a gatekeeper to information in a computer. The gatekeeper in a computer is a password or other technical device. Consequently there is a tendency to question how the impersonal machine will do all the things a person does to keep the system honest. Computers are also expected to measure up to their reputation for inhuman speed and efficiency. Consequently time becomes an issue where it may not be now. For example, users ask whether the computer system can be accessed twenty-four hours every day of the week. We do not ask this question about existing manual systems that are available only during normal business hours. Computers are expected to provide audited records and to confirm every step. In the present paper system, however, we often accept the risks of ordinary mail instead of registered mail. Computers also process huge amounts of information, yet the information is intangible and invisible until it is printed on a screen or paper. We implicitly trust a bound, typeset copy of a book because forgery would require skill and expense. Yet anyone can make words appear on a computer screen or printout. Who can say if they’re genuine? For all of these

reasons, questions are raised about computers that would not be asked if the processes were more personal and tangible, less technical and complex.

Whatever the reasons for concern, and whatever system is eventually implemented, all parties must have confidence in it. Legal concerns may be raised merely as a means to establish whether the new ERF system should be trusted. Indeed, trust is one of the underlying themes in this report (see for example the discussion of trusted third parties and public key infrastructure). Paper is a trusted technology. Paper documents are used to establish the truth. Computer technology is new and not as trusted, and so invites a reconsideration of how trust and truth come to exist.

As noted above, there is a tendency when thinking about computers to have unattainable expectations. Some people may envision hearings in which the participants communicate only by tapping keyboards in a futuristic regulatory control centre where paper has been outlawed. Instead, ERF is intended to improve regulatory processes in specific ways that are focused not on technology but on structured and standardized documents:

- The core improvements are based on the information repository of electronic documents. Using an international standard called Standard Generalized Markup Language ("SGML"), all information in the repository will be in a formal, documented structure. The formal structure required to store documents (defined in a Document Type Definition, a "DTD") is expected to provide efficient document exchange and management. Information is expected to be more complete and easier to find and use.

- With information in a central repository, participants can select relevant parts of the information. This is expected to save the costs of distributing all information to all participants while providing requested information more efficiently. Documents can be pulled from the system, not pushed at everyone.

- Building on the core system, automated information management systems can facilitate meetings and hearings. This is known as the automated hearing room. In its simplest form, the automated hearing room will permit everyone present in the hearing room to search and retrieve documents electronically. This should not be confused with computer-aided transcription to produce verbatim hearing transcripts. Verbatim transcripts are only one type of document that will be stored in the ERF repository. Additional technology will permit participation from remote locations. Other possibilities include use of software for groups to work together at different times and places. This latter concept is called the electronic hearing room.

- Another proposed improvement is the use of case management and work flow tools to process documents and improve scheduling.

- The architects of the ERF system also propose to provide comprehensive help, not only about using the computer system but also about the substance of the regulatory process.

It is important not to confuse ERF with other technological innovations. It is not a computer-assisted transcript (CAT) system for instant verbatim reporting. It is not an electronic document interchange (EDI) system as used in commercial transactions for automated purchase and sale with standard purchase orders and invoices. ERF is not an imaging system that stores pictures of documents. These and other techniques can be part of the proposed system but they are not essential. The greatest benefits of ERF are expected to come from routine document creation and handling. Electronic documents can be automated and they do not need to be printed, duplicated, bound and delivered.

It is also important to distinguish an ERF document repository from a registration system. A land registry, for example, serves to register official documents. Documents are not accepted unless they fit in the prescribed format and only restricted types of documents are accepted. The information in a land registry directly affects legal rights. Contrast the registry model with the proposed ERF document information system that serves primarily to exchange information. Documents of many types are accepted so that participants can present their cases. Most documents filed with the Boards do not affect legal rights directly. Indeed, many documents are filed before a hearing begins and have no legal status until they are deemed to be admissible evidence. Even documents accepted as evidence do not usually have the force of registry documents that have direct legal consequences. These differences are strong influences in the design of the proposed ERF system (see also the discussion of other electronic systems).

The bottom line: ERF is a means of improving communication, not a change to the substance of the regulatory process.

4. **What is the legislative authority for ERF?**

When electronic documents were first encountered in legal proceedings, questions were raised about their status compared to paper records. In some instances, these questions have been resolved by legislation. For example, many statutes now give equal status to computer records and paper records (Access to Information Act, R.S.C. 1985, c. A-1, s.4(3), Canada Business Corporations Act, R.S.C. 1985, c. C-44, s. 22(1), Canada Evidence Act, R.S.C. c.C-5, s.30(12), Patent Act, R.S.C. 1985, c. P-4, s. 8(1)(1), Business Corporations Act, R.S.O. 1990, c. B.16, s. 139(1), Electronic Registration Act S.O. 1991 c. E.44, Land Titles Act, R.S.O 1990, c. L.5 , s.166(1), Registry Act, R.S.O

1990, c. R.20, s.16 (1) — see also the legislation in a growing number of American states that have followed the lead of Utah in passing statutes that say when corresponding with government, a digital signature is equal to a manual signature).

At the federal level, the Report of the Information Technology Security Strategy Steering Committee to the Council for Administrative Renewal, June 1995, made the following recommendations:

> "Although there is no legal impediment to the federal government using information technology, introducing the information technology security strategy, or implementing a public key infrastructure for digital signature and confidentiality encryption, the Steering Committee recommends *that legislation be reviewed, and possibly amended, in the following areas*:
>
> - The *Interpretation Act* and the *Canada Evidence Act* should be reviewed to clarify the evidentiary requirements for electronic records, particularly as they relate to statutory requirements for writing, original record, certified or notarized copy, etc.
>
> - Departments should review their own mandate and applicable statutes to ensure that the legislation provides for the use of these new information technologies.
>
> - The *Access to Information Act* and the *Privacy Act* should be reviewed to clarify requirements with regard to information technology, and in particular:
>
>   - computer searches and monitoring;
>   - smart cards;
>   - audit trails;
>   - central database and databases whose content changes frequently;
>   - formalities for exchanging information between government institutions.
>
> - Public key infrastructure legislation should be introduced to establish the many parties' roles and responsibilities, and to cap the federal government's financial liability. It is important that a lead Minister for such legislation be identified at an early stage.
>
> - The public should be consulted with regard to the issues of: the use of personal identifying information, for example, on government smart cards; the sharing of personal information among government departments, or between the federal and provincial governments, and; law enforcement access to encrypted information.
>
> - The legal responsibilities of operators of electronic bulletin boards and of persons who disseminate information on public electronic networks should be clarified.
>
> - Definitions of terms applicable in an electronic context is problematic, should be reviewed and possibly amended (eg. "private communications", "public place", "publication", "possession", "collection", and "disclosure")."

A proposed federal law, the Personal Information Protection and Electronic Documents Act (Bill C-54) would address some of these issues. Part 2 of Bill C-54 provides for

electronic alternatives to paper records governed by federal law. Instead of amending each individual federal statute, the Bill would amend the law generally. Federal government agencies will be authorized to use electronic means instead of paper, including electronic payments, forms and filings.

The NEB presently has the authority to make rules governing the conduct of its business (National Energy Board Act, R.S.C. 1985, C.N-7, s. 8). The National Energy Board Rules of Practice and Procedure, 1995 (SOR 95-208), refer explicitly to filing of documents. Section 9 authorizes filing in any form that the NEB has the facilities to receive. The same regulation, however, mandates filing of hard copy documents in addition to electronic filings. The rules are now being revised to accommodate electronic filings. The Ontario Energy Board also has authority over the conduct of its proceedings (Statutory Powers Procedure Act, R.S.O. 1990, c. S.22, s 25.1), and the information submitted to it (Ontario Energy Board Act, 1998, s. 13) and its rules too are being revised so that they will be neutral with respect to paper and electronic filings.

In the absence of more specific legislative provisions on electronic regulatory filing, general legal principles that evolved in a paper world must be reinterpreted for the electronic world.

5. **What criteria were used to design the ERF system?**

Early in the planning stages, a set of ERF principles and criteria was developed, including the following:

- Systems and processes which support the initiative must be effective, reliable and secure.
- Electronic documents must meet the following criteria:

  Electronic documents must have longevity, with documented information (including evidence) capable of being preserved over as long a time as appropriate for a court of record;

  Loading of documents into the system must be accurate;

  Loading of documents into the system (i.e. document repository) must be timely, and must require a minimum of handling;

  The presentation of a document (i.e. fonts and document layout) as intended by the author should, to the extent practicable, be preserved;

  Documents must be universally accessible, in other words, they must generally be retrievable and reusable regardless of the user's system or software that comply with open systems standards; and

  Exchange of documents should be possible using a variety of communication vehicles (e.g., E-mail, diskettes, Internet, file transfer, CD-ROM).

- To the extent practicable, the initiative will be based on an open, non-proprietary systems policy and standards.
- Systems supporting the initiative must be user driven, addressing and balancing the needs of all ERF participants and the general public.
- The systems and processes which support the initiative must enable long-term reductions in regulatory costs and process times.
- Where interim services are provided they must be cost effective in their own right and must contribute toward reaching the long term objective of ERF.

6. **How secure will the ERF system be?**

All computer systems require security measures. What kind of security is required and how much? The answer depends on subsidiary questions, including who has physical access to the computers and communication networks, who has electronic access, what are the incentives for someone to breach the security, what kinds of security breaches can be detected, what are the consequences of security breaches, what are the costs of protection, how secure is the present paper system in comparison, do security precautions interfere with normal use of the system and many other detailed questions.

The following topics must be addressed in any computer system:

- Authorization: authority to use the system (including not only authorized people but also authorized computers, that is, other computer systems that may also access the system)
- Authenticity: whether the users really are who they purport to be and whether the information they provide is what it is supposed to be
- Availability: whether the system is available and accessible when required
- Audit
- Confidentiality
- Integrity of information in the system
- Privacy

As noted earlier, no system is perfect. Current paper-based systems are not perfectly secure. Yet they have been deemed to be acceptable. Even locked filing cabinets behind locked doors can be breached by a determined intruder. Fire and water can damage any

records, whether paper or electronic. Abuse of an organization's information system may come not only from someone enabled by technology, such as the fabled computer hacker, but also from someone able to disrupt any system, such as a disgruntled employee. There is always a risk assessment, not an absolute guarantee of security.

Using reasonable computer security techniques, the proposed ERF system can be more secure than the present system. At present:

- Paper can be sent to the wrong address or be lost in the mail.
- Members of the public are permitted to handle original documents on the public record, which is therefore subject to damage, alteration or loss.
- Existing records may be incomplete.
- Old records may be difficult to retrieve.
- Present paper records are subject to error.
- There is no duplicate or backup system analogous to that provided by an electronic system for use after a disaster or during routine interruptions such as moving to a new location.
- Even documents given special status, such as signed affidavits, are not particularly secure now. It would be unusual for a tribunal to confirm the identity or authority of the person signing or to compare signatures on the affidavit with any other identifying document such as a driver's licence or passport.

Just as paper systems raise particular security issues (access to rooms, combination locks, keys) computer systems have their own issues (passwords, backups, power failure). A reasonably-constructed computer system will have as much as or more security than a paper system. As all documents will be electronic, identical copies can be provided as needed. Access to records can be controlled and audited. Computer verification techniques can reduce errors. Standard formats can improve data gathering and retrieval. Automation can minimize human errors.

Because computer systems can be made more secure than paper systems, computer security is often not a matter of whether the system is secure but how to balance security against ease of use. Too much security can be as inefficient as too little security. For example, a computer system could be made very secure if each document were given a unique password and a unique program for accessing that document. An intruder would have to know ten passwords and how to run ten programs to read ten documents. It is technically easy to create this kind of barrier. Unfortunately, legitimate users would also

face the same barrier. Nobody would want to use such a secure but inefficient system. Indeed, legitimate users would probably forget many of the passwords, or write them on paper and so create a new security problem in protecting the list of passwords.

Paper documents are so familiar that we rarely ask what are the required security elements. What gives us confidence in them? The same elements apply to digital documents. They include:

- authentication of the person— a document should show who signed it.

- authentication of the document— a document should show what the person signed.

Consider an ordinary letter signed by the letter writer. Many aspects of the letter could be used to prove it: a handwriting expert could testify about the signature, a materials expert could study the paper and ink, while the address, return address, postmark, stamp and the contents could all add to the ultimate confidence held in the document. Each of these elements, however, could also be forged. Handwriting can fool even an expert, or merely be illegible. Witnesses can lie.

In a computer system, authentication techniques should be designed to prevent forgery. The system should ensure that the person signing the document cannot deny doing so. Any commonly used technique should be efficient. Like a handwritten signature, it should be easy to do. Many of the techniques used in paper systems can be applied to computers, including acknowledgment of receipt (as in registered mail) and auditing of message traffic (mail tracking and logging).

Are electronic documents secure? Although no final decision has been made on the specific security programs to be used in ERF, the design of the proposed electronic document system includes provisions for software that will prevent unauthorized changes to documents. The system will be able to detect whether any information was changed, when the document was last changed and by whom. In this respect, paper documents which are easily changed are less secure than electronic documents under the proposed ERF system.

Are electronic documents vulnerable to forgery? In regulatory proceedings, forgery of documents is unlikely. The Secretary of the Board does not now examine the handwritten signature of the lawyer or witness filing a paper document to be sure it is a proper signature. An electronic document, by contrast, may have a secure code (digital signature, discussed elsewhere in this report) that serves the purpose of a handwritten signature.

An electronic system should also be able to ensure that the person sending a document cannot deny sending it and a person receiving a document cannot deny receiving it. Again,

the proposed ERF system makes provision for non-repudiation and auditing of transactions.

Authentication of a document is closely tied to verification of the contents. The techniques for signing documents should provide some means to verify not only what the signature attaches to but also that the signed document is complete and unaltered.

In some computer systems, even the security measures that protect the system are confidential and the location or perhaps even the existence of the computer systems is secret. A local example is the large unmarked suburban building that houses the computer systems of a major multinational company. There is no name on the building, just a street address. Any organization, even with such tight security, must be prepared to disclose necessary details about the computer system if required to prove computer records in court (see also the discussion of computer evidence).

Many organizations rely on the same computer security techniques including banks and law enforcement agencies which also need secure systems.

7. **What electronic formats will be used for ERF documents?**

In preference to proprietary formats, ERF uses open, international standards where possible. Consequently ERF does not accept formats specific to products like Microsoft Word or Corel WordPerfect. As the bulk of filings are text (that is, including words, tables, graphics and so on), the underlying architecture relies on the international standard text markup language, SGML. It is expected that XML and HTML will also be used to distribute information, although documents accepted in the repository must be in SGML. Some filings, such as high volume numerical data, may be stored in common relational database formats. Although document images produced by optical scanning or direct faxing may be used in exceptional circumstances, the architecture of ERF relies on searchable character formats. (See also the glossary in Appendix C for help with technical terms in this section).

There is no perfect document format. Nor is there a perfect way to search for information in a large repository. The Boards chose a format that permits contextual information to be encoded in the document itself. Such extra information, beyond the actual words in the document, can be used to search for documents, convert between formats or do other processing based on the extra intelligence encoded in the document. SGML permits individual documents to be used like databases, not merely stored.

Other formats can be searched word by word, but the familiar full-text search is subject to problems of noise and related concepts from basic information theory. Simply stated, when searching through a large repository, you get too much or too little information but

rarely the exact information required. Transcripts of testimony, for example, are difficult to search word by word given all the subtleties of human language. A witness may speak at length about “it”, for example, describing it in great detail, with only indirect reference many pages earlier to what “it” is. Keywords that appear frequently in an energy database, like “natural gas”, become no more useful in finding relevant passages than words like “it”. Many document formats can be separately indexed to improve searching but that index is not contained within the document format itself. Even keyword indexing has its drawbacks, especially if indexed mechanically. By contrast, an SGML document can be indexed as it is created, with the desired elements and attributes embedded in the document by the author.

Formats that meld appearance and content, such as word processing formats and Adobe Portable Document Format (PDF), were designed to make text and graphics look good on a page. They attempt to reproduce an electronic version of paper. But the formatting will be distorted if the rendering device, usually paper or screen, cannot reproduce the typeface and other features used by the creator of the document. They are also substantially larger than SGML documents, and consume more communication and storage resources. A corollary of the separation of form and content gained by use of SGML is increased reusability of documents– converting between SGML documents or from SGML to other formats such as PDF is much easier than converting from a format with less embedded intelligence.

SGML is a mature international standard unlike proprietary formats that change frequently. The Boards have observed the problems experienced by other tribunals plagued by so-called upgrades. For example, when a new version of the approved word processing software appears on the market, the rules of the tribunal and the computer systems of all participants may have to be altered to process the new format.

SGML is complex and that complexity increases the costs of analysis, design, development and maintenance. The initial cost of an SGML system may be significantly higher than one based on proprietary formats, in part for DTD (Document Type Definition) development, and SGML may require additional software tools to support its use, but SGML documents are independent of the software that created them. The tools may be common to no-one, but the documents at the heart of the system are available to everyone now and in the future regardless of the proprietary tools used by any specific participants. Moreover, SGML tools have been rapidly increasing in power and decreasing in cost.

HTML, although simple and portable, is not extensible and cannot adapt to specific content. Consequently, as discussed above, the ability to search a large document repository for a specific HTML document is limited. Other limitations: HTML can handle only simple fill-in-the-blank forms and one-way hypertext links. Although each new version of HTML adds more capability, software changes to incorporate new versions consume time and resources. In any event, all versions of HTML mix format and content in a one-size-fits all document type definition.

In contrast to HTML, XML offers many of the advantages of SGML. Again without describing these markup languages in detail, some reasons to prefer XML over HTML include separation of content from format, opportunity to use various style sheets, improved linking, freedom to define document types (DTDs) and growing industry support for XML. Because XML is simpler than SGML, XML software development will be correspondingly simpler.

Despite growing interest in XML as a replacement for HTML, the ultimate power to formalize document structure resides in SGML. As SGML is the metalanguage underlying these other formats, support for SGML implicitly includes support for HTML and XML. The Boards' SGML implementation will be XML compliant. Other supported open formats include JPEG, MPEG and CGM for storing a variety of graphic and multi-media information without compromising archival requirements. Additional open standards will be supported as required.

8. **How will documents be signed in ERF?**

For centuries, various statutes have required that words be written, signed, certified, notarized or perhaps be fit into a prescribed form. These requirements help to prevent disputes about what exactly was said. A writing requirement, however, is not necessarily the same as a signature requirement. Writing can be unsigned. Writing captures ideas for many purposes, including use as evidence. Signatures identify and formally bind a person to the writing so that, in the absence of forgery, the person cannot disavow the writing.

Documents with legal significance are often signed in handwriting. It would seem natural, therefore, to demand that the electronic system have an electronic analogy to a handwritten signature. Before doing so, however, it should first be noted that a personally handwritten signature is not the only or even the most common means of investing a document with legal significance. A signature in the form of a handwritten name is not always needed. A mark, such as an 'X', intended to serve as a signature, may be acceptable. A stamp or facsimile may be acceptable, as is common on cheques and other commercial instruments. A signature created by a machine can be treated in law like a human signature. Judicial decisions in Canada, the UK and the US have held that mechanical stamps and other reproduced signatures are legally binding. Even an illegible signature has been accepted (see for example R. v. Kapoor (1989) 52 C.C.C. (3d) 41). In addition, the principal person involved need not sign the document. An agent can sign on behalf of a principal. A power of attorney can be used to delegate broad authority for signing. In government, legislation may delegate authority for signing.

The law has generally been flexible enough to adapt to new technology by accepting new forms of writing and signing or even by avoiding the requirements altogether. At both federal and provincial levels, statutory requirements for writing have long been interpreted to include various media, as expressed in terms such as these:

> "writing", or any term of like import, includes words printed, typewritten, painted, engraved, lithographed, photographed or represented or reproduced by any mode of representing or reproducing words in visible form." (Interpretation Act, R.S.C. 1985 c. I-21, s.2).

As noted elsewhere in this report, a definition such as this may be too restrictive for computer media, but it illustrates the flexibility of the concepts.

Specific laws have also been passed to eliminate writing and signing requirements. The federal government and some provinces have implemented the United Nations Convention on Contracts for the International Sale of Goods which provides that sale contracts do not have to be written. Ontario, for example, has removed a writing requirement from its Sale of Goods Act (R.S.O. 1990, c. S.1, see also the International Sale of Goods Act, R.S.O. 1990, c. I.10).

In a computer system, as in a paper system, handwritten signatures need not be the only means of authenticating documents. Depending on the circumstances, the effect of a signature may be achieved with electronic tagging like the addressing information on electronic mail, or by a typed name in the text of the message or by a facsimile of a signature in the form of a digitized image, or by processes requiring passwords and personal identification numbers. In some electronic filing systems, such as SEDAR (described elsewhere in this report), the filer must keep a manually signed piece of paper to support the electronic filing. Revenue Canada uses a similar technique with electronically filed tax returns. The filer, who keeps a handwritten signature of the taxpayer, acts as an agent of Revenue Canada to authenticate the tax return.

For the purposes of this discussion, none of the above forms is considered to be a digital signature. A digital signature is not a visual concept but rather is the result of mathematical calculation applied to the document. In other words, a digital signature uses a “secret code”. The sender does not have to be a mathematician but merely needs software that does the appropriate calculation and attaches a signature to the document. The signature does not alter the contents of the document but rather is additional information. In some systems the code can be used to scramble (encrypt) the whole document to make it confidential, but document encryption is not a necessary part of a digital signature system. Whether the message itself is encrypted or not, a digital signature can nevertheless be used to determine if unauthorized changes have been made to the text of the message.

The concept of a digital signature is possibly confusing and certainly new for most people. For that reason it is discussed in this separate section although it is closely related to other issues like system security and admissibility of evidence.

To be effective, the signature code is calculated so that it identifies the signer, cannot be created by anyone but the signer and it can be verified by the recipient of the document.

Note that the recipient's software does not need the sender's secret code, called a private key, but only the corresponding public key used to check the signature.

Digital signature software usually relies on complex mathematical concepts such as the properties of prime numbers, hash functions and asymmetric cryptography, which are beyond the scope of this discussion. From the point of view of users of a digital signature system, a digital signature can be as simple as an added string of unintelligible characters at the bottom of an e-mail message. This string of characters is processed by the recipient's software to authenticate the signature and the message. The fundamental feature of a digital signature is that it can be traced to the person who made it. Only the person with the private key can make the signature. The non-mathematical forms of signatures listed above, such as a typed name or digital facsimile, cannot necessarily be traced because they can be reproduced by anyone.

More important than the mechanics are the fundamental reasons for using signatures. The purpose of a signature is to attest to the authenticity of a document. A signature provides evidence that the signer actively approved of the contents of the document and intended to be bound by the consequences. A valid signature cannot be repudiated by the signer. Any system, paper or electronic, must show who signed (signer authentication), what exactly was signed (document authentication) and do so efficiently so that the transaction cost of using signatures is minimal.

In regulatory proceedings generally, the signature on a document is not verified by the recipient of the document, although it is available if needed. Rather, the procedure by which the document is created and delivered to the recipient gives the document its authority. Pre-filed evidence, such as an economic forecast, for example, must be proved at a hearing. A signature on the forecast is of little value before a witness has attested to the document and has had an opportunity to explain, correct or update it.

Appropriate procedures can substitute for a handwritten signature. Familiar examples of procedure substituted for handwriting include:

- electronic home banking
- paying by credit card over the telephone
- online personal property security registrations
- purchase of securities from a broker

Each of these examples uses different safeguards to ensure that an authorized person or delegate is bound by the transaction despite the absence of a handwritten signature.

As there is currently no formal screening process at the Boards to detect fraud or forgery of signed documents, the proposed computer system cannot significantly increase the likelihood of fraud or forgery. Rather, the system can automate the process of verifying signatures. A general hardship provision can relieve a participant from the requirements of the system depending on the circumstances.

Together with digital signatures comes the need for a public key infrastructure (PKI) with trusted third parties or certifying authorities. A handwritten signature can be linked to a person by watching the person sign and by comparing handwriting samples. A digital signature is merely a stream of numbers. The digital signature can be linked to the person by having a third party keep records to verify that the stream of numbers has been issued to the person who claims to have that particular digital signature. That is, a third party can take responsibility for issuing and revoking digital signatures and generally monitoring the digital signature system.

Federal Bill C-54 (discussed elsewhere in this report) contemplates regulations deeming certain technologies to be acceptable for secure electronic signatures. Some of the issues that must be considered in making these regulations are stated in these terms:

> "The Governor in Council may prescribe a technology or process only if the Governor in Council is satisfied that it can be proved that
> (a) the electronic signature resulting from the use by a person of the technology or process is unique to the person;
> (b) the use of the technology or process by a person to incorporate, attach or associate the person's electronic signature to an electronic document is under the sole control of the person;
> (c) the technology or process can be used to identify the person using the technology or process; and
> (d) the electronic signature can be linked with an electronic document in such a way that it can be used to determine whether the electronic document has been changed since the electronic signature was incorporated in, attached to or associated with the electronic document." (s. 48(2)).

The proposed legislation also ties the concept of secure electronic signatures to the law of evidence in the following terms (see also the discussion of authentication):

> "The Governor in Council may make regulations establishing evidentiary presumptions in relation to electronic documents signed with secure electronic signatures, including regulations respecting
> (a) the association of secure electronic signatures with persons;
> (b) the integrity of information contained in electronic documents signed with secure electronic signatures; and

(c) the manner in which the matters referred to in paragraphs (a) and (b) may be proved." (s. 31(4)).

Bill C-54 distinguishes secure signatures in general from the specific technology of digital signatures. Future secure signature technologies, such as transmission of biological data, may also be prescribed. Bill C-54 defines both "electronic signature" and "secure electronic signature", the latter requiring the application of prescribed technology. A secure electronic signature would also satisfy a legal requirement for a seal.

The proposed law permits electronic documents to satisfy a writing requirement under scheduled laws. If an original document is required by law, the electronic version would need a secure electronic signature. Statements made under oath or affirmation, such as affidavits, could be made electronically using two secure electronic signatures, one of the person swearing the statement and another of the person authorized to take the statement. Similarly, signatures that must be witnessed could be made with two secure electronic signatures, that of the signer and that of the witness.

If secure signatures are more secure than handwriting, we now have new categories of trust. In a paper world, we now use a signature and occasionally the extra protection of a witness. Under some laws the witness may be anyone. Other laws require an official witness, such as a commissioner for oaths or a notary public. The secure electronic signature offers a new kind of witness, the certifying authority. Some situations may still require the electronic equivalent of an affidavit, but in many situations only a single secure signature may suffice. For example, the presence of an impartial witness may be needed to confirm the mental state of the signer. Where, however, the impartial witness is only confirming that the document was signed without inquiring into the intentions of the signer, only a single secure signature may be needed. That is, the idea of a witness's digital signature raises the question: what does the second signature witness?

Systems for handling electronic signatures are complex. One of the most effective ways to move from paper to electronic documents, then, is to remove any unnecessary signature requirements. Board rules may have to be examined to be sure that signatures are not required merely because they have always been required. For example, signatures under oath, on affidavits and notarized documents, may be a means of attaching criminal penalties to false filings. The same purpose can be achieved by a general rule or regulation deeming use of the computer system to constitute signing, with penalties for any false filing, without demanding individual oaths for each document (see for example the Employment Insurance Regulations SOR/96-332, ss. 90, 91).

9. **Will ERF documents comply with the rules of evidence?**

The evidence on which the decision of a tribunal is based should be relevant and reliable. If evidence is not relevant, it cannot assist the decision maker. If evidence is not reliable, or if

there is no way to tell whether it is reliable, it cannot be used to establish the facts of the case. Irrelevant or unreliable evidence is either excluded from consideration altogether or admitted but not given any weight in the decision. The question for the proposed ERF system, then, is whether the system will provide relevant, reliable, admissible evidence.

Among the various categories of evidence used to prove a case— such as oral testimony, written evidence, real evidence and so on —the category most relevant to the proposed ERF system is documentary evidence. Before a document can be admitted as evidence and made an exhibit, it must pass several tests. For example, the document must be authenticated, that is, shown to be genuine. The so-called best evidence rule also requires the original document if it is available. These and other evidentiary rules have many exceptions. Very old documents, for example, are generally assumed to be authentic.

Computer records have been admissible in court as documentary evidence under common law principles. In addition, there is a specific statutory provision for documents, including computer records, made "in the usual and ordinary course of business" (Canada Evidence Act, R.S.C. c. C-5, s.30, Evidence Act, R.S.O 1990, c. E.23, s. 35).

The language of the Evidence Act does not specify how to ensure that computer records are admissible. Even if the records are admissible, there is no specific standard for ensuring that the records be given appropriate weight in the tribunal's deliberations. The courts will look at the overall circumstances of making the records. In general, admissibility and weight of computer records depends on reliable processes for input, storage and retrieval of the information:

> "The nature and quality of the evidence put before the Court has to reflect the facts of the complete record-keeping process— in the case of computer records, the procedures and processes relating to the input of entries, storage or information, and its retrieval and presentation" (*R. v. McMullen* (1979) 47 CCC (2d) 499 at 506, 25 OR (2d) 301, 100 DLR (3d) 671).

In other words, there is no way to *guarantee* that a specific computer record will be admissible and given appropriate weight. Of course, a regulatory tribunal is not a court of law subject to every nuance of evidence law.

In any event, the focus of inquiry in a dispute about the validity of ERF documents would not be on the particular piece of paper or record. The inquiry would be about the record-keeping system that produced the record. That is, the ERF system— the complete record-keeping process cited above —must be reliable and meet industry standards.

Although federal and provincial evidence law refers to computer records, it does not refer to finer distinctions such as the difference between imaging and optical character

recognition. Imaging systems copy documents without separating individual parts of the image into letters and numbers. Imaging is subject to errors during input of the image and in the finite capacity of digital systems. That is, images in the real world may contain more information than can be captured in a reasonable storage space in the digital world. Unlike imaging, optical character recognition tries to separate meaningful parts of the image but is subject to interpretation, such as whether a dot is punctuation or merely a stray speck on the image. Yet another form of computer record is made when a computer file is copied from one disk to another disk. Unless the copy is verified byte for byte, the copy cannot be assumed to be exact, although it usually is. These different ways of creating computer records are all subsumed under the heading of computer records. Yet they vary in their trustworthiness. The latter type of copy is verifiably exact but few users of optical character recognition would expect perfect text every time. Imaging lies somewhere in the middle of the trustworthiness scale depending on the quality of the original paper documents, the sophistication of the imaging equipment, the imaging algorithms used (e.g. lossless or lossy compression) and the size and format of the stored images. (In this regard it is noteworthy that Revenue Canada issued an information circular for the purpose of including imaging as a method of keeping tax records. See Information Circular 78-10R2SR, February 10, 1995 which requires that records be kept according to standards set by the Canadian General Standards Board in Microfilm and Electronic Images as Documentary Evidence, (CAN/CGSB - 72.11-93)).

In regard to copies, there is no way to be sure what a court would say about destruction of original records used to make computer records. If destruction is the ordinary course of business, then the records might pass that test. If not, destruction might be deemed to be obstruction and deception (see also the discussion of professional practice issues). The Evidence Act has special provisions for destruction of signed documents that have been photographed (i.e. microfilmed) but does not specifically include digital documents (Canada Evidence Act, R.S.C. 1985, c.C-5, s.31, Evidence Act, R.S.O 1990, c. E.23, s.34).

Other evidentiary principles may apply in addition to the “ordinary course of business” discussed above. Underlying all of evidence law is the need to put accurate facts before the tribunal. To meet this need, courts prefer:

- records made contemporaneously with the events they describe (because human memory fades)
- records made from personal knowledge (not potentially unreliable hearsay)
- facts not opinions (the familiar “just the facts, please”, leaving opinions for experts and the tribunal)
- original records not copies (a principle developed in a paper world where copies are not identical to originals)

- records made routinely and because the maker had a duty to do so (not records concocted for self-serving purposes)

These apparently simple standards often cannot be met by computer systems. As described previously, computers are impersonal. Records are often maintained and manipulated by someone who has no knowledge of the making of the records. Records may be retrieved much later than the events recorded. Records in a computer system can be an amalgamation of information made within an organization and information from other computer systems outside the control, knowledge or accountability of any one person. Facts in a computer can be part of a system of software used to manipulate the facts, as in a spreadsheet that can produce countless variations from the same data. It is clear that the law of evidence will have to evolve to deal with electronic record-keeping.

The Uniform Law Conference of Canada has recently approved a Draft Electronic Evidence Act and Commentary. That document addresses numerous evidentiary issues such as authentication, the best evidence rule and standard procedures. For further information see http://www.law.ualberta.ca/alri/ulc/current/eueaa.htm.

Under federal Bill C-54, discussed elsewhere in this report, scheduled federal laws that require copies would be satisfied by a single electronic document. Bill C-54 deals with the issues of original documents by deeming electronic documents to be satisfactory if "the electronic document contains a secure electronic signature that was added when the electronic document was first generated in its final form and that can be used to verify that the electronic document has not been changed since that time." This language is open to various interpretations, including what constitutes "first" generation and "final form", with all the possible versions in between.

Evidentiary issues of authentication and best evidence are considered in Bill C-54 in these terms:

> "31.2 (1)The best evidence rule in respect of an electronic document is satisfied
> (a) on proof of the integrity of the electronic documents system by or in which the electronic document was recorded or stored; or
> (b) if an evidentiary presumption established under section 31.4 applies.
> (2) Despite subsection (1), an electronic document in the form of a printout satisfies the best evidence rule if the printout has been manifestly or consistently acted on, relied on or used as a record of the information recorded or stored in the printout.
> 31.3 For the purposes of subsection 31.2(1), in the absence of evidence to the contrary, the integrity of an electronic documents system by or in which an electronic document is recorded or stored is proven
> (a) by evidence that supports a finding that at all material times the computer system or other similar device used by the electronic documents system was

operating properly or, if it was not, the fact of its not operating properly did not affect the integrity of the electronic document and there are no other reasonable grounds to doubt the integrity of the electronic documents system;
(b) if it is established that the electronic document was recorded or stored by a party who is adverse in interest to the party seeking to introduce it; or
(c) if it is established that the electronic document was recorded or stored in the usual and ordinary course of business by a person who is not a party and who did not record or store it under the control of the party seeking to introduce it."
31.4 The Governor in Council may make regulations establishing evidentiary presumptions in relation to electronic documents signed with secure electronic signatures, including regulations respecting
(a) the association of secure electronic signatures with persons;
(b) the integrity of information contained in electronic documents signed with secure electronic signatures; and
(c) the manner in which the matters referred to in paragraphs (a) and (b) may be proved.
31.5 For the purpose of determining under any rule of law whether an electronic document is admissible, evidence may be presented in respect of any standard, procedure, usage or practice concerning the manner in which electronic documents are to be recorded or stored, having regard to the type of business, enterprise or endeavour that used, recorded or stored the electronic document and the nature and purpose of the electronic document."

The juxtaposition of evidence law and computers raises many questions. As more government institutions entrust their business records to computers, the issues discussed in this section will be resolved. Meanwhile the ERF system is being designed with these questions, including the unanswered ones, in mind.

10. **What will be the effect of ERF on confidential information filed with the Board?**

Confidential business information may be supplied to the Board (such as that specified in section 16.1 of the National Energy Board Act or part VII of the Ontario Energy Board Act, 1998). Other principles of general application, such as fiduciary duties, may also apply as they do now. The proposed ERF system is not expected to have any effect on confidentiality. Differences between the existing paper system and the proposed ERF system are primarily related to computer security compared to existing security, discussed elsewhere in this report.

11. **How will ERF affect natural justice and procedural fairness?**

The concepts of natural justice and procedural fairness are intended to ensure that affected parties know the case to be heard and can present their evidence and argument before an impartial tribunal. The specific procedural standards that will achieve these ends depend on many factors including the kind of tribunal and the effect of the decision. Courts have analyzed fairness and natural justice not as necessary requirements for every tribunal but as appropriate for the circumstances. Different tribunals do different things, from court-like determinations of individual rights on the one hand to broader policy decisions on the other hand. Less strict procedural requirements are applied to policy matters. Many lengthy treatises have been written on these concepts which will not be further defined here.

To the extent that ERF is simply automation of document creation, transmission, storage and retrieval, it should have no effect on procedural standards. In other words, the Boards will continue to have hearings, make decisions and so on. There are several aspects of ERF, however, that deserve specific comments.

The first is the question of fairness to individuals, small intervenor groups and those who do not now use computers. Will a system dependent on use of computers exclude anyone? No.

Most participants in the Boards' processes are represented by lawyers who have access to computers. A survey of participants showed that they are using various types of computer systems. The survey was completed early in the planning stages of ERF and undoubtedly would show even more technical sophistication today. There are also unrepresented intervenors, primarily concerned with issues such as construction on the intervenor's land, and a larger number of unrepresented individuals who do not intervene but who present their views through letters of comment.

Anyone who participates in proceedings under the present system must be able to read either official language, comply with Board rules and communicate by mail, fax or by attending personally. These requirements are not perceived to be unfair. In the proposed system, these requirements change little. Paper documents can be converted to electronic form compatible with Board standards. Even if an individual has only a pen and paper or a typewriter, the individual can submit the paper and the ERF system can store a digital version of it.

Conversely, to assist the public in getting documents from the system, computer access will be made available for online searching. Does this exclude members of the public who do not know how to search for documents in the computer system? Again, the baseline for comparison is the present system. Do members of the public know how to find documents in the present system? They must take the time to understand the rules, the process and the paper documents. Progress reports and studies of the proposed ERF system suggest

that document retrieval will be greatly improved under ERF. Moreover, the tribunal has the power to regulate its procedure and in particular to require that information be filed with indexes, executive summaries, cross-references and other techniques that can reduce the complexity of even the largest cases.

A related question is whether the use of computer technology will make the Boards more remote from the public. Computers are no longer specialized tools for experts— not in an era when public school children use the Internet in their classrooms, when telephone and cable companies make e-mail as available as telephones and televisions, and when many government agencies advertise their world-wide web sites. In many ways the proposed ERF system will make the Boards less remote: access to information will be improved not only through automated searching but also with more uniform filing and keyword tagging. ERF can also provide forms of access not available now for the disabled, including off-site computing, large-font display, Braille and speech synthesis. ERF will literally make the Boards less remote to participants in remote areas.

Indeed, electronic access may open the Boards to new audiences. An electronic document repository may provide public information to anyone with an Internet connection. The public record has always been open to the public, but only at Board offices. Instantly accessible and searchable public information is a new phenomenon, perhaps even a new category of public information.

Existing rules of practice and procedure may have to be revised to accommodate ERF. The rules now assume a paper world. For example, words like “original” and “copy” will have to be revisited in the context of electronic filings. Rules, guidelines and procedures will, of course, have to take into consideration the rights and needs of participants who do not own a computer or whose ability to use one is limited. The Boards will provide access to everyone as required whether by means of computers or traditional paper processes. Anyone without access to a computer will be accommodated.

One issue that merits special attention is that of notice. Natural justice and procedural fairness require that potential parties have notice of Board proceedings. Failure to give reasonable notice may invalidate a decision. Notice need not be personal delivery of a piece of paper (see also the discussion elsewhere in this report of document service generally). On the contrary, because so many parties may be interested, notice of Board proceedings is typically published in newspapers. No Canadian court has ruled on use of an Internet site or e-mail for public notice of proceedings. By analogy to existing rulings, however, it is likely that a court will inquire whether electronic means of notice are reasonable in the circumstances. Until the Internet and computer technology become as broadly and routinely consulted as the daily newspaper, however, the Boards will continue to give notice using traditional means in addition to any electronic means.

12. **How will documents be served in ERF?**

Today most documents are created electronically with word processing software, or other applications such as spreadsheet and e-mail software. They are then printed, filed and served as paper among the parties to the proceeding. Some parties may then scan the paper back into an electronic form for easier storage, searching and retrieval. The ERF document repository can eliminate some of these conversions and permit documents to be pulled from the system as required.

In a paper system, documents are not only filed with the tribunal but they are also served on interested parties. Filing and service ensure that parties know that documents exist and have access to them. Parties also cannot say they were unaware of the existence of the filed documents. This is an example of document "push" in which all documents are always delivered to all parties, regardless of their particular interests in the proceeding.

In an electronic system, automation makes it possible to provide different types of service, or eliminate service entirely. Parties could sift information according to their own interest profiles. They could receive documents by e-mail. Or rather than receive whole documents, they could simply receive notification that certain documents had been filed. Then they could pull documents from the repository as required. Or they could dispense with service altogether and check the repository for new documents, either manually or using an automated software agent for periodic updates.

No Canadian court has ruled on the legality of digital document service or eliminating service altogether in favour of document pull. Considering judicial decisions about technologies such as fax and telegraph, a court would be likely to look at the particular technology and the circumstances. In any event, the Boards have the power to control their own process, are not bound by the procedural requirements of courts and have prescribed their own filing and service requirements (National Energy Board Rules of Practice and Procedure, 1995, SOR/95-208, ss. 8 and 9, Ontario Energy Board Rules of Practice and Procedure, February 1997, ss. 11 and 20).

If, as in the present paper system, parties know about all filed documents and have access to them, with appropriate safeguards such as acknowledgment messages, then the objectives of document service could be achieved electronically. Although no final specification has been developed, the ERF system is being designed to meet these objectives.

13. **Has the Board considered the effect of ERF on legal practice?**

Consider these statements from lawyers published in the Ontario Lawyers Gazette, February 1997, by the Law Society of Upper Canada, the governing body for Ontario lawyers:

> "Law is very conservative . . . we're not going to be the first ones to test whether an electronic document is admissible in court."
>
> "It's like dragging the past in, but I'm not comfortable going to that fully electronic world if my career is going to turn on whether that fax I send from my computer really went out."

Law practice issues include whether instructions from clients must be signed on paper. Would e-mail instructions suffice? If so, how long should old e-mail be kept? Some lawyers may believe that only paper records will protect them against claims for errors and omissions and that all records must be kept forever. Issues like this between lawyers and their clients are not generally brought before a regulatory tribunal. Still, lawyers such as those quoted above may believe that they must exchange paper, not electrons, "out of an abundance of caution."

By the time ERF is fully implemented, it is expected that lawyers will be using computers in other areas of their practice and will have policies for electronic records and filing. In the meantime, any implementation of ERF will have to take some account of lawyers' professional responsibilities in relation to record-keeping.

14. **Does this mean that the Boards have answered every question about ERF?**

No. ERF is new. Until it has been implemented and tested, there will naturally be questions and problems to resolve. As noted at the outset, many questions will be resolved through familiarity with the new technology, which will only be gained over time. If there are unresolved questions, the Boards welcome comments and suggestions.

15. **Appendix A: Other Agencies and Jurisdictions**

Although ERF and its associated issues are new in Canadian energy regulation, the Boards are not alone. Other agencies and jurisdictions are also converting paper to electronic systems.

Canadian Federal Examples

The government of Canada has too many electronic programs to list here (see for example the list at http://www.gc.ca/programs/pgrind_e.html). They include:

CANADIAN ENVIRONMENTAL ASSESSMENT AGENCY (CEAA)

The Canadian Environmental Assessment Agency, pursuant to section 55 of the Canadian Environmental Assessment Act, operates a public registry system. The purpose of the registry is to facilitate public access to the records relating to environmental assessments, and to ensure convenient public access. The public registry includes the Federal Environmental Assessment Index (FEAI), departmental document listings and documents.

THE CANADIAN INTELLECTUAL PROPERTY OFFICE (CIPO)

The Canadian Intellectual Property Office permits online searching of the Canadian Patent Database. From the online description:

> "This database lets you access over 75 years of patent descriptions and images. You can search, retrieve and study more than 1,300,000 patent documents."

CIPO also offers the Canadian Trademarks Database, described online as:

> "enabling you to look up all pending and registered trade-marks in Canada. Trademark information found in the database can include designs, wares and services covered by the registration, owner's name and more."

DIGITAL SIGNATURES

The federal government is already using digital signature technology, as in the novel application described in these words:

> "On June 5, 1998, the Communications Minister of Singapore, Mah Bow Tan, used a digital signature to sign a Memorandum of Understanding between his country, Canada, and the State of Pennsylvania. The signing took place at an Asia-Pacific Economic Cooperation (APEC) Meeting on the Telecommunications and Information Industry. Canadian Minister of Industry John Manley and Pennsylvania Governor Tom Ridge, neither of whom was present at the meeting,

had both previously signed the document using private key technology. The signatures were delivered ceremonially to Minister Mah at the meeting by representatives. Minister Mah then placed a smart card containing his signature into a reader, and typed in his password to "sign" the document. The three signatures were then electronically authenticated to create an offical document. The document is the first digitally signed international government document and it creates a Global Learning Consortium between the two countries and the state to promote the use of telecommunications and information technology in education through a common website." (http://www.tas.gov.sq).

Examples from Ontario

In Ontario, examples of pioneering electronic systems include: personal property security registration, business names registration, land titles and land registry, civil trial procedure and securities commission filings.

MINISTRY OF THE ATTORNEY GENERAL, ONTARIO

A pilot project authorized under the Courts of Justice Act (O.Reg 223-97) permits lawyers to file a limited number of civil court documents electronically. Electronic filing is part of a larger civil case management project using proprietary software called Sustain to enter claims, schedule cases and produce statistical reports. Only designated law firms and legal departments trained in the use of the prescribed software may participate. In the pilot project, a lawyer uses Sustain client software to create and then e-mail a one-page word processing template to the court office. The software verifies the form, debits the filing fee directly from the lawyer's account, issues a court file number and sends a receipt to the lawyer. Service of documents between participating solicitors may be done through the computer system. The prescribed forms do not require a signature, although a signed proof of service must be kept by the lawyer. Public access to filed documents will initially be available at terminals in the court and later by remote access, and paper copies will also be made as required. Long term plans not part of the pilot project include filing of motions and trial records in addition to simple one-page documents.

The Sustain system, unlike ERF, uses proprietary software and data formats. A consortium of companies including Microsoft promotes the software as an electronic way to link lawyers and courts. The Ministry project is also associated with a separate administrative court management process.

MINISTRY OF CONSUMER AND COMMERCIAL RELATIONS (MCCR)

In partnership with a private company, Teranet, MCCR has developed an electronic land conveyancing system. MCCR also has an electronic system for filing personal property security registrations and one for business name registration. More than 90% of personal property registrations and 30% of business name registrations in Ontario are filed electronically. These systems use proprietary software and data formats. In most cases, only designated persons may participate. Under the regulations governing these systems, documents do not have to be signed. Unlike ERF, the registries are not primarily for document management in hearings and adjudication.

Cross-Canada Example

CANADIAN SECURITIES ADMINISTRATORS (CSA)

Canadian securities regulatory authorities have adopted an electronic filing system, the System for Electronic Document Analysis and Retrieval (SEDAR). SEDAR was developed to:

> "Facilitate the electronic filing of securities information prospectuses, continuing disclosures documents, etc.) and the payment of CSA filing fees as required by the securities regulatory authorities in Canada.
>
> Facilitate public dissemination of securities information collected in the securities filing process.
>
> Facilitate electronic communication such as E-mail between electronic filers, filing agents and securities regulatory authorities."
> (SEDAR Filer Manual)

Unless there are exceptional circumstances, all filed documents must now be in electronic form. Unlike the proposed ERF system, SEDAR does not use the standard generalized markup language, SGML. All SEDAR documents must be in one of three proprietary formats (WordPerfect, Microsoft Word, Adobe PDF).

Examples from the United States

RULENET

An innovative experiment by the U.S. Nuclear Regulatory Commission (NRC), RuleNet was an electronic rulemaking forum on the Internet. The experiment involved the public in making performance-based rules related to fire protection. Anyone with a Web browser could observe, post comments and access related documents.
(http://nssc.llnl.gov/RuleNet/Help/Info.html)

FEDERAL COMMUNICATIONS COMMISSION (FCC)

In April 1997, the FCC started its electronic filing initiative with a Notice of Proposed Rulemaking (FCC 97-113):

> "In this Notice of Proposed Rulemaking (Notice), we propose to allow parties to file comments electronically in all FCC informal notice and comment rulemaking proceedings conducted under section 553 of the Administrative Procedure Act, except for broadcast allotment proceedings. These electronic filings would be given the same treatment and consideration as comments filed on paper. We tentatively conclude that this action will make it significantly easier for members of the public to communicate their views to the Commission, and to review comments that others have filed. We believe that electronic filing will also allow the Commission to improve the efficiency of its own processes, to the benefit of the public."

OTHER AGENCIES USING SGML

The following is a list from the SGML Web Page (http://www.oasis-open.org/cover/ as of November 1998) of government and industry SGML projects:

- The U.S. Department of Energy (DOE) Office of Scientific and Technical Information (OSTI)
- IRS (United States Internal Revenue Service)
- National Library of Medicine (NLM)
- Library of Congress - Encoded Archival Description (EAD) - Finding Aid Pilot Project
- SAE J2008 (and T2008) Automotive and Truck Standard
- SEC EDGAR Database
- IETM (Interactive Electronic Technical Manuals)
- TCIF/IPI (Telecommunications Industry Forum Information Products Interchange)
- Electronic Component Information Exchange (ECIX) - Pinnacles Component Information Standard (PCIS)
- ATA DTDs (Air Transport Association)

! Railroad Industry Forum: Electronic Parts Catalog Exchange Standard (EPCES)

! CALS: Continuous Acquisition and Lifecycle Support (formerly: Computer-aided Acquisition and Logistics Support; recently "Commerce At Light Speed")

! USAF SGML Repository

! MIL-STD-2167A: FOSIs and DTDs related to MIL-STD-2167A

! MIL-M-28001B SGML documents (Navy site)

! Army SGML Registry and Library (ASRL)

! Government Information Finder Technology - GIFT (Canada)

16. **Appendix B: Selected Further Reading**

Aspects of Public Policy Regarding Crown Copyright in the Digital Age, W.T. Stanbury, 10 Intellectual Property Journal 131, May 1996

Copyright and Confidential Information Law of Canada, G. F. Henderson ed, 1995 Carswell

Copyright and the State in Canada and the United States, David Vaver, 10 Intellectual Property Reports 187, May 1996

Copyright in Legal Documents, David Vaver, 1993 Osgoode Hall Law Journal Vol. 31 no. 4 p. 662

Crown Copyright In Canada: A Legacy Of Confusion, Barry Torno, 1981 Minister of Supply and Services Canada

Essentials of EDI Law, Peter Jones, Electronic Data Interchange Council of Canada, 1992

The Internet Changes Everything: Revolutionizing Public Participation and Access to Government Information Through the Internet", Stephen M. Johnson, Administrative Law Review, 50:2, Spring 1998, p.277ff;

Management of Recorded Information, Directive 7-5-8 June 1992, Management Board of Cabinet, Ontario

Microfilm and Electronic Images as Documentary Evidence, CAN/CGSB - 72.11-93, Canadian General Standards Board

Ontario Lawyers Gazette, January/February 1997, Vol. 1 No. 1, Law Society of Upper Canada

Open Access Same-Time Information System, 18 CFR Part 37 April 24, 1996 Federal Energy Regulatory Commission (FERC)

Policy, Practice and Who Gets to Own the Crown's Jewels: The Ownership of Intellectual Property in Crown Contracts, Martin P. J. Kratz, 10 C.I.P.R. 613

Practitioner's Guide to Electronic Filing in Utah Courts, April 27, 1995, Utah Administrative Office of the Courts

Recorded Information Fact Sheet # 6 on Electronic Document Filing Fundamentals, Archives of Ontario

Report of the Information Technology Security Strategy (ITSS) Steering Committee to the Council for Administrative Renewal, June 1995 (http://www.cse.dnd.ca/GOCITSTRATEGY/).

Revenue Canada Information Circular 78-10R2SR, February 10, 1995

SEDAR (System for Electronic Document Analysis and Retrieval) The Ontario Securities Commission OSC Bulletin November 15, 1996 Volume 19 Issue 46 Sedar Supplement

SGML Handbook, Charles F. Goldfarb, 1990 Oxford University Press

Standards For The Preparation, Distribution and Citation of Canadian Judgments in Electronic Form, May 1996, Judges Computer Advisory Committee of the Canadian Judicial Council

Survey of Legal Issues Relating to the Security of Electronic Information, Information Technology Security Strategy Legal Issues Working Group, June 1995, Treasury Board of Canada

Sustaining Dialog, Ministry of the Attorney General, quarterly newsletter for the Sustain court filing project

Who Owns Copyright in Law Reports? Gérard Snow, 64 C.P.R. (2d) 49

17. **Appendix C: Glossary**

Authentication: identifying legitimate persons and machines.

Byte: eight binary digits (bits, that is ones and zeroes); capable of representing 256 numbers or characters (between 0 and 255, represented as 00000000 to 11111111); a fundamental unit of information transmission or storage in a computer.

CGM: Computer graphics metafile, an image file format.

Cryptography: the science of securing messages.

Digital signature: computer process designed for the same purpose as a handwritten signature; an electronic means of associating a person with a document; the result of applying specific technological processes to authenticate a document.

DTD: Document Type Definition, a prescribed document structure, expressed in the language SGML (q.v.); all documents filed under ERF must be structured to conform to the prescribed DTD.

E-mail: electronic mail, sent as a stream of bytes (q.v.) from one computer to another, through the Internet (q.v.) or a private network; may refer to the system or individual messages.

ERF: Electronic Regulatory Filing, a joint project of the National Energy Board and the Ontario Energy Board, for conversion of paper processes to digital systems facilitating the creation, exchange, use and reuse of regulatory information.

HTML: Hypertext Markup Language, used to create Word Wide Web (or simply, web) pages on the Internet with links, called hyperlinks, to other web pages; HTML is one document type definition (DTD, q.v.) described by the metalanguage SGML (q.v.).

Internet: A network of computer networks using an agreed communication protocol called Transmission Control Protocol/Internet Protocol (TCP/IP) that facilitates common services such as electronic mail, web pages and file transfers.

JPEG: an image file format from the Joint Photographic Experts Group, also called JPG files, suitable for storing and transmitting photographs in a computer system.

MPEG: a digital video compression format from the Motion Pictures Experts Group used to store and transmit movies in a computer systems.

PDF: Portable Document Format, a proprietary document file format of Adobe Systems Incorporated.

SGML: Standard Generalized Markup Language, a metalanguage used to describe document types such as HTML and XML (q.v.); separates content and structure from formatting and appearance.

XML: Extensible Markup Language, a subset of SGML (q.v.); expected to be the next generation document standard for the World Wide Web (q.v).

World Wide Web: the interlinked documents stored on computers connected to the Internet (q.v.), also called the web, hence the expression web page referring to a single document; document addresses frequently begin with www, an abbreviation for World Wide Web, as in www.neb.gc.ca or www.oeb.gov.on.ca.