

**Public Record Office Standard
PROS 99/007**



Public
Record
Office
Victoria

Management of Electronic Records

**Version 1.0
April 2000**

Table of Contents

1.0	Introduction.....	2
2.0	Victorian Electronic Records Strategy	2
3.0	Electronic Records	3
4.0	Electronic Records Format	4
5.0	Common Structure for Electronic Records.....	4
5.1	Content.....	5
5.2	Metadata (Context)	5
6.0	VERS Compliance	5
7.0	Further Reading.....	5
8.0	Acknowledgments	6
9.0	Glossary	6
10.0	Establishment of standard	12
	Appendix One: Role and responsibilities of the Public Record Office Victoria	13
	Appendix Two: Electronic Records and the Law	14
1.	Paper Records.....	14
2.	Issues with moving from paper to electronic records.....	14
3.	Admissibility of Electronic Records	15
4.	Weight of Electronic Records	16
5.	Digital Signatures in Lieu of Handwritten Signatures	16
6.	Summary	16

Under section 12 of the *Public Records Act 1973*, the Keeper of Public Records is responsible for the establishment of standards for the efficient management of public records and for assisting public officers to apply those standards to records under their control. Officers in charge of public offices are responsible under section 13 of the Act for carrying out, with the advice and assistance of the Keeper, a programme of records management in accordance with the standards established under section 12 of the Act.

1.0 Introduction

Government recordkeeping provides a mechanism to support evidence of activity in a public office. It requires, particularly in the electronic environment, a thorough understanding of the functions and legislative requirements that may affect individual public offices and the particular recordkeeping needs of those offices.

The Victorian Electronic Records Strategy (VERS) is designed to assist public offices in managing their electronic records. The strategy focuses on the data or information contained in electronic records rather than the systems that are used to produce them.

VERS was developed with the assistance of CSIRO, Ernst & Young, the Department of Infrastructure, and records managers across government. The recommendations included in the VERS Final Report¹ issued in March 1999 provide a framework for the management of electronic records.

Under various provisions of the *Public Records Act 1973* Public Record Office Victoria and public offices share responsibility for the management of records in all formats and, where appropriate, their long term preservation. In order to assist public offices to meet their responsibilities under the *Public Records Act*, Public Record Office Victoria publishes Standards for the management of public records.² These include Standards for the creation and maintenance, management, destruction and transfer of public records. They apply equally to records in all formats, including electronic records.

The determination of disposal sentences for electronic records must be done in consultation with Public Record Office Victoria. PROS 97/003³ outlines the various means by which records disposal may be authorised. Determining which electronic records need to be kept for extended periods of time will enable the integration of disposal sentences into record keeping systems. This in turn will lead to greater efficiencies in the management of public records as the processes are readily automated, integrated and implemented in the electronic records environment.

This Standard should be used in conjunction with PROS 99/007 Specification 1: *System Requirements for Archiving Electronic Records*, PROS 99/007 Specification 2: *VERS Metadata Scheme*, and PROS 99/007 Specification 3: *VERS Standard Electronic Record Format*.

2.0 Victorian Electronic Records Strategy

The VERS approach provides a framework within which it is possible to capture and archive electronic records into a long term format that is not dependent on a particular computer system (hardware or software).

¹ *Victorian Electronic Records Strategy Final Report*, Public Record Office Victoria 1999. Available from the PROV website <http://www.prov.vic.gov.au/vers/>

² Available from the PROV website <http://www.prov.vic.gov.au/>

³ *Destruction of Public Records* PROS 97/003. Available from the PROV website <http://www.prov.vic.gov.au/>

The VERS model considers that **records exist within files**. It supports the aggregation of data (information) relating to a particular topic and advocates the management of this information at the file level rather than the individual record level. This is a continuation of the approach taken to records and files in the paper environment.

The approach relies on the use of published ‘standards’ for software and hardware (e.g. XML – eXtensible Markup Language – a text based standard) rather than the use of specific applications or programs which may change over time and become incompatible with requirements for record keeping.

The focus of VERS, whilst being primarily related to document type electronic objects, has applicability to other object formats and future developments may mandate standards for these.

VERS is sufficiently flexible to support any electronic record in any format. The strategy is primarily focused on providing long-term preservation of electronic records but, where possible, day-to-day use of electronic records is also supported.

Record keeping requires a long term approach but computer systems and applications change or become obsolete very rapidly. Several issues have been identified as an impediment to the long term management of electronic records.

- Document formats change and become unreadable over time.
- Electronic objects can be subject to undetectable change thereby making it difficult to maintain the evidentiary and accountability status of the records.
- The context of an electronic record, and its relationship to other records, can easily be lost.
- Existing systems for managing electronic documents do not preserve the content, structure, context and evidential integrity of the record for as long as the record may be required.

Each of these issues has been addressed in the development of the Victorian Electronic Records Strategy.

3.0 Electronic Records

Electronic records are **evidence** of organizational activities and include policy documents, memos and letters, and database reports. They are generally the computerized versions of traditional paper records. Sources of electronic records range from desktop applications such as Word, Excel, and email, to corporate applications such as financial systems, human resource systems and corporate databases.

4.0 Electronic Records Format

An electronic records format must be able to support:

- *Long life.* Records must have an indefinite life. That is, the contents of a record must be capable of being viewed forever. This has four aspects:
 - *Preservation.* The records must be in a form that can be physically preserved (for example easily copied from one media to another without loss of quality).
 - *Accessibility.* It is useless to save records unless they can be found again.
 - *Readability.* Records must be able to be viewed as the creators and users originally saw them.
 - *Comprehensibility.* Records must be able to be understood in their context.
- *Evidence.* Electronic records must be admissible as evidence and given due weight in a court of law. This requires the ability to prove that a record has not been altered since creation, and to demonstrate who created the record and when it was created.
- *Disposal.* It must be possible to appraise (that is, evaluate and determine the record's status) and, where authorised, transfer or destroy records in a controlled manner.
- *Augmentation.* It must be possible to be able to augment or change the information **associated with** a record without disturbing the evidentiary integrity of the record. In VERS this process produces 'onion' records.

The VERS long term format (detailed in 97/007 Specification 3 *VERS Standard Electronic Record Format*) is able to support all these functions.

5.0 Common Structure for Electronic Records

The Victorian Electronic Records Strategy requires that electronic records of all types have a common structure to ensure their effective management. A common structure aids public offices, PROV and vendors by enabling a common interchange format for government information.

The following characteristics have been identified for all types of electronic records.

- Records must be **self documenting**. It is possible to interpret and understand the content of the record without needing to refer to documentation about the system in which it was produced
- Records must be **self contained**. All the information about the record is contained within the record itself
- The record structure must be **extensible**. It is simple to extend the structure of the record to add new metadata or new record types without affecting the interoperability of the basic structure.

5.1 Content

Content is the original information that is being preserved. There are many different types of content (for example, documents, databases, and images). Content types may be encoded in different formats. For example, documents in Portable Document Format (PDF) encoded as Base64, database tables directly encoded using eXtensible Markup Language (XML). The electronic record format must be sufficiently flexible to contain a variety of content encodings and types.

5.2 Metadata (Context)

Metadata is information associated with the record. Metadata can describe the record, describe the content of the record, document its relationship with other records and the organization (the record's context) and describe the encoding of the content. Metadata can also document the use and continuing management of the record.

PROS 99/007 Specification 1 *System Requirements for Archiving Electronic Records* describes a common record structure and the elements required for VERS compliance.

6.0 VERS Compliance

The specifications for electronic records attached are designed to ensure uniformity in record structure and management without limiting a public office's choice in systems and support processes for business activity. The first specification (PROS 99/007 Specification 1 *System Requirements for Archiving Electronic Records*) defines the formal system requirements and structure required for records produced in electronic systems compliant with this standard.

The second specification, PROS 99/007 Specification 2 *VERS Metadata Scheme*, defines the metadata requirements for electronic records.

The third Specification, PROS 99/007 Specification 3 *VERS Standard Electronic Record Format*, provides the recommended VERS long term format for VERS compliant systems.

Officers in charge of Public offices should ensure that record keeping systems in use now and in the future can support the common long term format for electronic records.

7.0 Further Reading

Records Management Standards, available from the PROV website
<http://www.prov.vic.gov.au/>

- PROS 97/001 **Management of Public Records**
- PROS 97/002 **Creation and Maintenance of Public Records**
PROS 97/002 Specification 1 Storage of Public Records in Agencies
- PROS 97/003 **Destruction of Public Records**
PROS 97/003 Specification 1 Destruction of Records Covered by a Disposal Schedule

PROS 97/003 Specification 2 Destruction of Records Not Covered by a Disposal Schedule

- PROS 97/004 **Transfer and Storage of Public Records**
 - PROS 97/004 Specification 1 Documentation of Public Records
 - PROS 97/004 Specification 2 Transfer of Records to the Public Record Office Victoria
 - PROS 97/004 Specification 3 Transfer of Records to an APROSS
 - PROS 97/004 Specification 4 Access to Public Records
 - PROS 97/004 Specification 5 Processing and Listing Public Records

Victorian Electronic Records Strategy Final Report, Public Record Office Victoria 1999. Available from the VERS website <http://www.prov.vic.gov.au/vers/>

Keeping Electronic Records Forever, Public Record Office Victoria 1995-96. Available from the VERS website <http://www.prov.vic.gov.au/vers/>

8.0 Acknowledgments

Public Record Office Victoria would like to acknowledge the contributions of the State Records Authority of New South Wales, National Archives of Australia and the staff at the VERS@DOI project in the Department of Infrastructure in providing much useful feedback on this Standard. The Online Services Group of the Department of Employment, Workplace Relations and Small Business also provided comment as did the Unisys Information Management Program. Staff within PROV offered much helpful criticism and comment.

The original VERS Project team members (CSIRO, Ernst & Young, and PROV) were instrumental in devising the concepts and ideas which underpin this Standard.

PROV would like to thank the following people for providing their knowledge and expertise and helping to create this Standard:

Justine Heazlewood, Public Record Office Victoria
Brendan Hills, CSIRO
Ainslie Sefton, Public Record Office Victoria
Andrew Waugh, CSIRO

9.0 Glossary

agency: A [public office](#) as defined in the *Public Records Act 1973*. A government department or discrete public office (like a statutory authority).

algorithm: A precise rule (or set of rules) specifying how to solve some problem.

application: A complete, self-contained software program that performs a specific function directly for a user or group of users.

Archive System: The application or set of applications which manages [VERS Encapsulated Objects](#). See also [repository system](#), [Record Keeping System](#), [Capture System](#) and [Discovery System](#). This application has been functionally defined in PROS 99/007: Specification 1.

augmented record: *see* [onion record](#).

browsing: A method of searching for information by moving from one information resource to another via logical hierarchies or [links](#).

Capture System: A name for an [application](#) (or group of applications or part of an application) that obtains a [document](#) and/or [metadata](#) from an electronic environment (an application or group of applications which generate or manage the document and/or metadata) and creates [VERS Encapsulated Objects](#). See also [Record Keeping System](#), [Archive System](#) and [Discovery System](#).

certificate *see* [public key certificates](#).

certificate chain: To check the signature on a [public key certificate](#), you need the [public key](#) of the [Certificate Authority](#) that created and signed the certificate. This is obtained from a second public key certificate, the signature of which must be verified in turn. The resulting chain of public key certificates is called a certificate chain.

Certification Authority: An organisation that creates and signs [public key certificates](#).

computer file: An element of data storage in a computer file system. There is a distinction between a computer file and a 'file' in a records management sense where it commonly denotes a collection of paper documents grouped together in a paper binder.

controlled vocabulary: A simple list of valid terms or values.

digital signature: a security mechanism that demonstrates that a particular piece of data was created by a particular entity. See [Public/Private Key Security](#). *See also* [certificate](#), [Certification Authority](#), [private key](#), [public key](#), [public/private keypair](#).

Discovery System: A name for an [application](#) (or group of applications or part of an application) that allows a person to search for [electronic records](#). The person is able to search on [metadata fields](#), document text, or [record linkages](#). The resultant [records](#) are represented to the user exactly as captured. See also [Record Keeping System](#), [Archive System](#) and [Capture System](#).

disposal: The process of appraising records. Within the Victorian public sector, records are appraised to determine their significance (business, legal or historical) and then judged to be either of temporary or permanent value to the state.

document: In its widest sense a document may be a sound [file](#), an image, a digital video or any other recorded information format as well as the more traditional word processing document or email. A paper document. Any [computer file](#) which may be printed.

In this Standard **document** can also mean that part of the [VERS Encapsulated Object](#) containing the electronic [computer file](#) which must be preserved in [VERS Long Term Format](#).

Document Type Definition: The definition of a document type in [XML](#), consisting of a set of mark-up tags and their interpretation.

DTD *see* [Document Type Definition](#).

electronic pointer: An automated [linking](#) reference within a system to an object either within the system or external to the system.

electronic record: A [record](#) communicated and maintained by means of electronic equipment. A record stored in a form that only a computer can process.

encapsulation: The process of creating a [VERS Encapsulated Object](#) by combining: [Standard Format Metadata](#), [Standard Format Documents](#), and [Integrity Assurance Metadata](#).

encoding: The physical representation of a [document](#). The data that forms a document. The file format of a document. The part of the [VERS Encapsulated Object](#) containing a representation of the actual document data.

encryption: Any procedure used in cryptography to transform a transmission in order to prevent any but the intended recipient from reading that data.

ERMS: the abbreviation for electronic records management system.

evidentiary integrity: An intangible property of an [electronic record](#) that determines the value of the record as evidence. It needs to be protected by the [Record Keeping System](#) and/or the [Integrity Assurance Metadata](#) in the [VERS Encapsulated Object](#).

file record: A special type of [VERS Encapsulated Object](#) that does not contain any [standard format documents](#), but contains [metadata](#) which describes a [file](#).

file: A logical collection or accumulation of records. An object in the [Record Keeping System](#) that “contains” ([linked](#)) [VERS Encapsulated Objects](#). All VERS Encapsulated Objects must be “contained in” ([linked to](#)) a file. The file is itself a VERS Encapsulated Object.

finding aid: Any guide such as an index, list, inventory, or catalogue that is descriptive or analytical with respect to a body of [records](#), and having the purpose of clarifying the subject content and organization of the records in order to facilitate their use.

government agency: a [public office](#) as defined in the *Public Records Act 1973*. A government department or discrete public office (like a statutory authority).

hash function: A computer [algorithm](#).

hash value: Part of the process of creating a [digital signature](#) is to turn the message to be signed into a number known as the hash value which is then [encrypted](#) to form the digital signature.

hypertext link: A [link](#) from one (usually text based) resource to another. The link is usually from a piece of text in one resource to another resource but it could also mean a link from a piece of text in a resource to another part of that same resource.

inheritance: The process of filling in [metadata fields](#) automatically from information obtained from the system, [application](#), or other [records](#).

integrity assurance metadata: [Metadata](#) that is part of a [VERS Encapsulated Object](#) that allows verification of the integrity of the VERS Encapsulated Object using [digital signatures](#).

key: In [Public/Private Key Security](#), this is simply a very long prime number. Common key lengths are 40 bits, 128 bits, and 1024 bits. A [private key](#) must be kept secret and be held by only one user. The [public key](#) is published so as to be accessible to all users of the security system.

link: Any connection between or within [records](#) or [files](#). These connections may be textual (e.g. a ‘see also’ reference) or by means of [electronic pointers](#) (e.g. a URL).

long term electronic record: A [record](#) which has been designed to survive for a long time. *See also* [VERS Encapsulated Object](#).

media: Physical storage media. A means of storing data. A piece of media allows data to be copied on to it which can then be read back by a computer. Some types of media allow data to be recopied (destroying the original data in the process) while other types of media will only allow data to be copied to the media once. Common types of media are CD-Rom, magnetic tape, floppy disk.

media migration *see* [media refresh](#).

media refresh: The copying of the contents of a piece of [media](#) to fresh media (possibly using a different storage technology or density).

metadata augmentation: The process of adding to or modifying the metadata of a [VERS Encapsulated Object](#) without degrading the [evidentiary integrity](#) of the original [document](#) or [metadata](#). This is effected by wrapping an existing VEO within another VEO containing the altered [metadata](#) or additional [documents](#). This produces an [onion layered VEO](#).

metadata element: A container for specific information about the [document\(s\)](#) contained in a [VERS Encapsulated Object](#). *See also* [metadata field](#).

metadata field: *see* [metadata element](#).

metadata schema: The organization and structure of the [metadata](#). *See* PROS 99/007: Specification 2 for the specific VERS Schema.

metadata: Metadata is information associated with a [record](#). Metadata can describe a record, describe the content of a record, document its relationship with other records and the organization (a record’s context) and describe the [encoding](#) of the content. Metadata can also document the use and continuing management of a record.

onion record: A [record](#) which has been modified by the addition or alteration of [metadata](#) or [documents](#). This is effected by wrapping an existing [VERS Encapsulated Object](#) (VEO) within another VEO containing the altered [metadata](#) or additional [documents](#). This produces an onion layered VEO. *See also* [metadata augmentation](#).

PDF: Adobe’s Portable Document Format.

private key: A [key](#). One half of a [public/private keypair](#). A private key is kept secret and is used to sign or encrypt objects. *See also* [public key](#).

public key: A [key](#). One half of a [public/private keypair](#). A public key is published and is used by other parties to verify digital signatures or decrypt objects. *See also* [private key](#).

public key certificate: A container for a [public key](#). A certificate contains information about the public key (e.g. its period of validity), and is signed by the organisation that issued the certificate to demonstrate its authenticity. *See also* [Certification Authority](#), [digital signature](#).

public office: As defined in the *Public Records Act* means:

- (a) any department, branch or office of the Government of Victoria;
- (b) any public statutory body corporate or unincorporate;
- (c) any municipality or other body constituted by or under the *Local Government Act 1958*;
- (d) any other local governing body corporate or unincorporate; and
- (e) a State owned enterprise within the meaning of the *State Owned Enterprises Act 1992*.

public/private key authentication: The process of showing that some data was actually created by the purported author. This is achieved by creating a [signature](#) from the data and the author's [private key](#). This process does not obfuscate (or [encrypt](#)) the original data, but allows data integrity verification using the author's [public key](#).

public/private key security: A technique used for [authentication](#). It requires two [keys](#), one of which must be kept [private](#), and one which is [publicly](#) available. A mathematical [algorithm](#) is used to ensure that the data is authentic or secure to a very high degree. The greater the key length, the higher the security of the system.

Up to two signatures can be used to protect the [VERS Encapsulated Object](#) from forgery. A [record](#) is normally [signed](#) separately by the creator of the record and by the system itself. These two signatures protect the record from forgery by any one party acting alone. The creator's signature ensures that a forgery cannot be perpetrated by a system administrator or by a third party. The system's signature ensures that the creator cannot forge the record after the event.

public/private keypair: A pair of linked [keys](#). One key is the [public key](#), the other key is the [private key](#). The keys are linked such that anything [encrypted](#) or [signed](#) using one key can be decrypted or verified using the other.

record linking: A system with the appropriate functionality can [link VERS Encapsulated Object\(s\)](#) to other relevant VEOs in the [Record Keeping System](#). Examples of this are linking a VEO to the [file record](#) it is associated with, or linking a VEO to the previous VEO in the same [transaction](#).

record: Evidence of organizational activity. A record can take many forms and is defined under the *Evidence Act 1958* to mean:

- a document in writing;
- a book, map, plan, graph or drawing;
- a photograph;
- a label marking or other writing which identifies or describes any thing of which it forms part, or to which it is attached by any means whatsoever;
- a disc, tape, sound track or other device in which sounds or other data (not being visual images) are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced therefrom;
- a film, negative, tape or other device in which one or more visual images are embodied so as to be capable (as aforesaid) of being reproduced therefrom;
- anything whatsoever on which is marked any words figures letters or symbols which are capable of carrying a definite meaning to persons conversant with them.

Record Keeping System: The application or set of applications which captures, manages, exports and controls access to [VERS Encapsulated Objects](#). See also [repository system](#), [Archive System](#), [Capture System](#) and [Discovery System](#). This application has been functionally defined in PROS 99/007: Specification 1.

repository system: Any application which stores and manages records. See also [Record Keeping System](#) and [Archive System](#).

search: The process of seeking for [records](#) in the [Record Keeping System](#). This may be done by means of [metadata](#), free-text, classification structures or other means.

signature block: The part of a [VEO](#) which contains a [digital signature](#) and the [metadata](#) related to that signature.

standard document format: The long term format used to store [documents](#) within a [VERS Encapsulated Object](#).

standard format document: A [document](#) in [standard document format](#) (i.e. after the document has been transformed).

standard format metadata: [Metadata](#) that conforms to the VERS [metadata scheme](#) as outlined in PROS 99/007 Specification 2.

transaction: A unit of work. Consists of one or more [VERS Encapsulated Objects](#) that were created as the unit of work was performed.

universal unique identifier: A [metadata field](#) that allows unique identification of an [electronic record](#). Within the VERS [metadata scheme](#) this is known as the **VEO Identifier**.

VEO: See [VERS Encapsulated Object](#).

VERS Encapsulated Object: A record which has been encapsulated using [XML](#) as outlined in PROS 99/007 Specification 3 and which conforms to the VERS [metadata scheme](#) as outlined in PROS 99/007 Specification 2 and which may contain [standard format documents](#).

VERS long term format: The format used to securely store [standard format document\(s\)](#) and associated [metadata](#), [encapsulated](#) together.

VERS standard format *see* [VERS Long Term Format](#).

XML: eXtensible Markup Language. A standard language that defines the structure of a set of documents using a [Document Type Definition](#).

10.0 Establishment of standard

Pursuant to section 12 of the *Public Records Act 1973*, I hereby establish these provisions as a standard applying to the records of all public offices, courts or persons acting judicially in Victoria. This standard as varied or amended from time to time, shall have effect for a period of ten (10) years from the date of issue unless revoked prior to that date.

Keeper of Public Records

Ross Gibbs

Date of Issue:

26 April 2000

Appendix One: Role and responsibilities of the Public Record Office Victoria

Public Record Office Victoria (PROV) was established under the *Public Records Act 1973* for the better preservation, management and utilisation of the public records of Victoria.

Public records include any records made or received by a person employed in a public office in the course of his or her duties, or by a court or person acting judicially in Victoria. Record is defined to mean any document within the meaning of the *Evidence Act 1958*, and includes information whether on paper, film, magnetic tape or disc, or any other media.

The term “Public Office” is defined in sub-section 2(1) of the Public Records Act to mean:

- (f) any department, branch or office of the Government of Victoria;
- (g) any public statutory body corporate or unincorporate;
- (h) any municipality or other body constituted by or under the *Local Government Act 1958*;
- (i) any other local governing body corporate or unincorporate; and
- (j) a State owned enterprise within the meaning of the *State Owned Enterprises Act 1992*.

Appendix Two: Electronic Records and the Law

1. Paper Records

In introducing records into evidence, Victorian courts make two decisions: admissibility and weight.

Admissibility addresses the question of whether the record can be introduced at all.

Admissibility is subject to a variety of rules built up over centuries. Of particular relevance to electronic records is the 'best evidence' rule. Among other things, this states that the 'original' is the best evidence. It is possible to introduce a copy, but only if the original is no longer available, and only after appropriate explanations. However the *Evidence Act* allows certain types of copies to be treated as originals (e.g. microfilm, photographs). The last revision of the current *Evidence Act* predates the widespread use of modern copying technology and the widespread use of computers.

Weight is only considered if the record can be introduced (i.e. is admissible) and reflects how reliable the court judges the record. Clearly weight is a subjective decision and depends on the record's perceived authenticity.

The highest weight would probably be given to documents that are signed, dated, and witnessed. In practice, however, the legal system accepts that the degree of formality associated with a document will depend on the importance of the record. Very formal records, such as wills, are formally signed and dated. At the other extreme, file notes may be accepted even though they have neither a signature nor a date. The courts may, of course, give different weights to documents with different degrees of formality.

Business records are an exception to the hearsay rule, and are assumed to be 'reliable hearsay'. Authenticity of unsigned and undated records can be conferred by the fact that they were generated and kept as part of the normal business activity. The records are given reasonable weight because if the records were inaccurate they would be useless for the business purpose for which they are kept.

Signatures are important on documents for many reasons. There are two types of documents which are usually signed; agreements (which might be disputed), and those which record an act of will (a decision) to which the person may be held accountable.

In law, the act of signing a document must be a conscious decision as it effects an act of will. This has implications for the automatic application of digital signatures to documents. Therefore in developing a digital signature methodology for authenticating electronic records, a distinction should be made between records that record the exercise of an act of will (i.e. a decision), and records that record an event (e.g. a meeting or conversation).

2. Issues with moving from paper to electronic records

The legal community is moving from a paper based model to an electronic based model. Currently the legal situation is in a state of flux. The extension of current practice with paper records to electronic records has been difficult. This is because of:

- Technology assumptions in statute law. Existing laws often mention or assume specific technology. The *Evidence Act* specifies a particular set of technologies that are defined to produce ‘copies’. More abstractly, there is a common law question about whether digital signatures are signatures. The Commonwealth and Victorian Legislatures are dealing with this by changing various acts to be technologically neutral. This process has not yet been completed.

As a side note, introduction of printouts of digital information (e.g. financial records) are routinely introduced into evidence. This is achieved by the person introducing the printouts swearing that they were, in fact, produced from the computer in question, and that the records were created under the normal course of business. This is an example of the development of case law in practice.

As a second side note, an interesting question is whether a paper printout of an electronic record (e.g. email) is an acceptable copy as printing out an electronic record is not covered by the Evidence Act.

- Lack of case law. Even after the statute law has been modified, the courts must develop an interpretation of this law. This process takes place as a side effect of conducting cases and the interpretation will consequently take many years to develop. One consequence of this lack of common law is that legal advice may be equivocal rather than definite. The advice is usually to the effect that the least risk is to assume the most conservative interpretation. The probability is that initial systems will consequently be over-engineered, and requirements will be subsequently relaxed as experience is gained with the technology.
- Lack of forensic experience with computer technology. The legal system is very familiar with the forensic capabilities to detect forgery in paper documents, but have much less experience with detecting forgery in electronic documents by means of system evidence (e.g. evidence from the file system). As a result there appears to be an emphasis on external evidence such as digital signatures. This emphasis may change as experience is gained with computer technology.

3. Admissibility of Electronic Records

It is clear that there may be a legal problem with the admissibility of electronic records as the current Victorian *Evidence Act* was not written with electronic evidence in mind. The proposed new Victorian *Evidence Act* will follow the new Commonwealth *Evidence Act*. The new Commonwealth Act removed the requirement that the ‘best evidence’ is the original. A copy is acceptable, and a copy is defined to be anything produced by a process which produces a copy.

Note that removal of the ‘best evidence’ principle means that judging the weight of the record becomes more important; any record could be introduced, but a judge may assign a low weight to it. Judges will be forced to assess how much weight is to be given to a copy produced by a particular process. Common law will be built up over a long period about what techniques are required to produce copies with the maximum weight, but this is no help in designing systems now.

4. Weight of Electronic Records

With paper records weight is determined by authenticity, and authenticity is determined in a variety of ways depending on the importance of the record.

The legal discussion on demonstrating the authenticity of electronic records has focussed on the use of digital signatures. The discussion of digital signatures, however, has generally been conducted at a high level and rarely considers the effect of the system that applies the digital signature on the resulting authenticity. (Note here we are not talking about the choice of digital signature technology itself, but how that technology is applied within a particular system.)

The cost of implementing a sound digital signature application is likely to be sufficiently high that the level of authenticity required of an electronic record, like a paper record, will depend on its importance. Unfortunately for people implementing systems now, the required degree of authenticity will only be evolved over time within common law.

5. Digital Signatures in Lieu of Handwritten Signatures

Acts are being passed to allow the use of digital signatures in lieu of normal signatures, but these are deliberately technology neutral. This neutrality allows the law to be flexible in light of rapidly developing technology. Issues of what is an appropriate technology and key length are being left to industry consensus and, ultimately, to common law. These acts have not yet been passed, but any system built now should be prepared to deal with digital signatures in lieu of normal signatures.

6. Summary

In summary, the legal situation on electronic records is in a state of flux. Because of the need to develop common law interpretations, this uncertainty can be expected to last for a significant period (possibly decades may pass before the legal questions of electronic records are completely resolved).

The two significant legal issues are the legal admissibility of electronic copies of records, and the status of digital signatures. It should be noted that the question of the legal status of an electronic copy of a record does not affect a record whose original is in an electronic format. The question of evidential status is not a simple 'yes/no' decision. Evidential status is a question of weight, and courts have been flexible in accepting paper records with a wide variety of evidential integrity. There is no reason to assume that they would be any less pragmatic in accepting electronic records with a range of evidential integrity. However, it should be noted that legal discussions focus on the use of digital signatures for ensuring evidential integrity.

In practice, the implementation of a system handling electronic records will require balancing the implementation cost against the importance of the records concerned. The point of balance will change as technology evolves and matures, and the legal situation clarifies and common law is evolved.