InterPARES 2 Project
International Research on Permanent Authentic Records in Electronic Systems

Title: Authenticity, Accuracy and Reliability in the Public Sector: Annotated Bibliography

Status:	Final (public)
Version:	1.0
Submission Date:	October 2005
Release Date:	September 2007
Author:	The InterPARES 2 Project
Writer(s):	Mary Beth Sullivan School of Information Science and Policy, State University of New York at Albany
Project Unit:	Domain 2
URL:	http://www.interpares.org/display_file.cfm?doc= ip2_biblio_aar_public_sector_annotated.pdf

Bibliographic Information:
Author: Internet Policy Institute
Title: Report of the National Workshop on Internet Voting: Issues and Research Agenda
Journal or Book:
Editor(s):
Publication Details: Arlington: Internet Policy Institute, 2001
Page Numbers: 1-62
Web Source: FindLaw Legal News and Commentary:
http://news.findlaw.com/cnn/docs/voting/nsfe-voterprt.pdf
Description: PDF available on WWW
Subjects: Focus 3/Domain 2/ Terminology Cross-domain / Policy Cross-domain and Government - e-government - voting
Class Descriptor:

Abstract:
"Report of the National Workshop on Internet Voting: Issues and Research Agenda" is based on a workshop sponsored by the National Science Foundation, and conducted in cooperation with the University of Maryland and hosted by the Freedom Forum. This report discusses technical and procedural considerations involved in creating an Internet voting system for public elections. It describes poll site Internet voting, kiosk voting, and remote Internet voting. Analysis of the advantages and disadvantages of each type of voting are explored. This fifty-four page document was published by the Internet Policy Institute in 2001.

Annotation:
This report describes authenticity, accuracy, and reliability in terms of government and voting. Our terms are utilized to describe vote recording systems and election records, not strictly to address records management issues. "…there has been strong interest in voting over the Internet as a way to make voting more convenient and, it is hoped, to increase participation in elections. Internet voting is seen as a logical extension of Internet applications in commerce and government. In the wake of the 2000 election, Internet systems are among those being considered to replace older, less reliable systems. Election systems, however, must meet standards with regard to security, secrecy, equity, and many other criteria, making Internet voting much more challenging than most electronic commerce or electronic government applications. This report addresses the feasibility of different forms of Internet voting from both the technical and social science perspectives, and defines a research agenda to pursue if Internet voting is to be viable in the future. It is based on a workshop that took place before the 2000 election, but it nonetheless addresses many of the issues that are now being debated about what to do to improve the integrity of elections. The topics addressed here, while all related to Internet voting, are also relevant to discussions about other electronic voting systems." (p. 1)

Keywords:

Authenticity:
Authenticity in all voting records must be proven. Faith in voting is equivalent to faith in government. (p. 11) Any form of voting should have "reliable and demonstrably authentic election records." (p. 11)

Accuracy:
Accuracy is mentioned as the correctness of the vote that is recorded. (p. 6) “The 2000 presidential election, and the subsequent five-week period in which the election results were in doubt due to the disputed vote count in Florida, changed the context of the online voting debate. There is now widespread interest in improving the accuracy and reliability of election systems, and increased convenience has become a secondary concern.” (p. 6)

“Accuracy—election systems should record the votes correctly.” (p. 11)

Accuracy depends on the system, the technology and equipment, and the people involved in the record keeping. (p. 27)
“Accuracy depends upon a variety of factors, such as the integrity of the system, the vulnerability of the hardware, software, and networking medium, and skilled personnel to operate and troubleshoot the system, none of which is transparent to monitoring officials.” (p. 27)

“Accurate voter registration lists are important to election integrity.” (p. 33)

Reliability:
Reliability is the absence of any voting system failure. (p. 3, 11) This report calls for research into the “…development of reliable poll site and kiosk Internet voting systems that are not vulnerable to any single point of failure and cannot lose votes.” (p. 3)

“Reliability—election systems should work robustly, without loss of any votes, even in the face of numerous failures, including failures of voting machines and total loss of Internet communication.” (p. 11)

Reliability is contrasted with voting security or the prevention of intentional disruption of the voting system. (p. 17)
“Whereas security refers to the resistance of a system to deliberate, intelligent, or interactive attack, reliability focuses on the questions of a system’s ability to perform as intended, in spite of apparently random hardware and software failures. For example, a computer memory failure could result in the loss of recorded votes. The viability of electronic voting rests, in part, on the ability of system designers and elections officials to incorporate redundancy into any deployed voting system and to develop contingency plans for possible failures.” (p. 17)

“The most important reliability consideration of all is that the votes be captured accurately in redundant and non-volatile storage within the voting client.” (p. 36)

“Reliability– The ability of a system or component to perform its required functions under stated conditions for a specified period of time.” (p. 46)

Other key terms:

For this report, other key terms relating to authenticity and/or voting include: eligibility, authentication, uniqueness, integrity, verifiability, auditability, secrecy, non-coercibility, flexibility, convenience, certifiability, transparency, and cost-effectiveness.

Trust and confidence are linked to authenticity of voting records and the legitimacy of the election. "With electronic voting systems, public confidence in the election relies on trust in technical experts instead of a transparent process." (p. 27)

Annotator: Mary Beth Sullivan
Date of Annotation: August 6, 2005
Other Notes: I do not know where this report was published. It might have been in Arlington, VA because of the involvement with the NSF. The Internet Policy Institute seems to be defunct. Their web site (http://www.internetpolicy.org) now forwards visitors to (grassroots.org), a 501c3 group that provides services to charities.

Bibliographic Information:
Author: National Archives
Title: Generic requirements to sustain electronic information over time: 1 Defining the characteristics for authentic records
Journal or Book:
Editor(s):
Publication Details: Kew, Richmond, Surrey, UK: National Archives, 2004
Page Numbers: 1-17
Web Source: National Archives web site:
http://www.nationalarchives.gov.uk/electronicrecords/pdf/generic_reqs1.pdf
Description: PDF available on WWW
Subjects: Focus 3/Domain 2/ Terminology Cross-domain / Policy Cross-domain and Government - e-government - authentic records
Class Descriptor:

Abstract:
"Defining the characteristics for authentic records" explores authenticity, reliability, integrity, and usability and describes characteristics of authentic electronic records. It is the first of four documents in PDF format on the National Archives web site covering "Generic requirements to sustain electronic information over time". These requirements are referred to as the "minimum necessary" for sustainable records to meet the BS ISO 15489 standard. This seventeen page document was published by the National Archives (Kew, Richmond, Surrey, United Kingdom) in 2004.

Annotation:
The definitions strongly relate to Domain 2, Focus 3, although the references to accuracy seem to be implied in the document's examination of integrity and reliability. This document provides "…government departments (with) an understanding of the principles which underpin any attestation that a record or a category of electronic records are considered to be authentic in accordance with BS ISO 15489 Information and documentation – Records management standard. If records are to be sustained there must be confidence that the maintained records possess authenticity, reliability, integrity and usability. A summation of the attributes, which would support an attestation of authenticity and integrity and which need to be maintained as part of the electronic record is provided in this document."

(http://www.nationalarchives.gov.uk/electronicrecords/pdf/generic_reqs1.pdf, p. 3) "The guidance is intended primarily for those working in central government; the principles will also be relevant in local government and throughout the public sector." (http://www.nationalarchives.gov.uk/electronicrecords/pdf/generic_reqs1.pdf, p. 3)

Keywords:

Authenticity:
Authenticity comes from what is known about a record. (p. 5) "A presumption of authenticity is an inference that is drawn from known facts about the manner in which a record has been created, handled, and maintained." (p. 5)

Eliminating change to a record ensures authenticity. (p. 5) "It will be necessary to sustain electronic records over time as a valued corporate asset, in a manner that retains their reliability and integrity for as long as they are required, preserving their value as a corporate record. This will include prevention of changes to the content or context to retain authenticity, and continued maintenance in an appropriate format to retain accessibility." (p. 5)

Accuracy:
Accuracy is only mentioned in passing when reliability is examined. (p. 9) "Trust is critical to reliability as without it there can be no meaningful faith in the accuracy of the retained records." (p. 9)

Reliability:
Reliability can be verified when the record system is examined and found to reflect the "legitimate business process." (p. 8)

"…a reliable record as one whose contents can be trusted as a full and accurate representation of the transactions, activities or facts to which they attest and can be depended upon in the course of subsequent transactions or activities." (p. 8)

Other key terms:

The identity of a record is defined as characteristics which "…distinguish it from other records…" (p. 8) A record must be correctly identified before it can have authenticity, accuracy, or reliability.

This document seems also imply a link between accuracy and integrity. An accurate record can be said to have integrity when it continues to be accurate over time, that is, it is precise and correct for as long as it exists. According to this document "…a record has integrity if it remains complete and uncorrupted in all its essential respects throughout the course of its existence." (p. 8)

Annotator: Mary Beth Sullivan
Date of Annotation: August 9, 2005
Other Notes: As the work of a government agency with an intended audience in central government, this document is applicable to Focus 3, governmental activities. The least relevant material is the discussion of the function and presentation of records in the exploration of

usability. Authenticity in the electronic record keeping is explained in pages 14-17. “The organisations own policies and procedures have to reinforce the characteristics of a trusted record management system. A trusted record management system includes the rules that control the creation, maintenance, and use of the creator’s records, which support a presumption of the authenticity of the records within the system.” (p. 15) “The generic functions described in this document may also be relevant to a permanent archive but the needs of archival preservation are considered as distinct from those operations required to maintain electronic records for continuing business needs even where the overall retention period may last for some decades.” (p. 4) All four generic requirements and explanatory material in this series of documents may be found on the web at (http://www.nationalarchives.gov.uk/electronicrecords/generic.htm).

Bibliographic Information:
Author: National Archives
Title: Generic requirements to sustain electronic information over time: 2 Sustaining authentic and reliable records: management requirements
Journal or Book:
Editor(s):
Publication Details: Kew, Richmond, Surrey, UK: National Archives, 2004
Page Numbers: 1-24
Web Source: National Archives web site:
http://www.nationalarchives.gov.uk/electronicrecords/pdf/generic_reqs2.pdf
Description: PDF available on WWW
Subjects: Focus 3/Domain 2/ Terminology Cross-domain / Policy Cross-domain and Government - e-government - records management
Class Descriptor:

Abstract:
“Sustaining authentic and reliable records: management requirements” covers a wide range of managerial responsibilities necessary to maintaining electronic records. It is the second of four documents in PDF format on the National Archives web site covering “Generic requirements to sustain electronic information over time”. This document describes management procedures and provides guidance for the records environment, technology, authentication, and records access. This twenty-four page document was published by the National Archives (Kew, Richmond, Surrey, United Kingdom) in 2004.

Annotation:
This document briefly mentions authenticity and reliability. “This document defines the key elements that should be incorporated within any management strategic planning framework and the processes that will also have to be developed and supported in order to ensure that electronic records which are to be sustained over a defined period of time are able to satisfy the characteristics of a record as defined in BS ISO 15489 that is authenticity, reliability, integrity and usability. If these characteristics are not maintained the sustained records will lose credibility and will lose evidential value. This section of the generic requirements will define performance indicators and non-functional requirements as opposed to the technical management requirements…” (http://www.nationalarchives.gov.uk/electronicrecords/pdf/generic_reqs2.pdf, p. 3)

Keywords:

Authenticity:

Records are believed to have the quality of authenticity when they are certified to have authenticity. (p. 8) "A coherent set of requirements for maintaining electronic records in a manner which will enable reproduction of the records and where this is required certification of the authenticity of the reproduced records." (p. 8)
Records are authentic when basic information about the records can be verified. (p. 14) "The presumption of a record's authenticity is strengthened by knowledge of certain basic facts about it." (p. 14)

Accuracy:

Reliability:

Managing records is important to reliability. (p. 5) "The key element is defining the management processes that need to be identified and established within any organisation that proposes to maintain reliable records over a specific period." (p. 5)

Other key terms:

Authentication - "…authentication is understood to be a declaration of a record's authenticity at a specific point in time by a person entrusted with the authority to make such declaration." (p. 20)

Annotator: Mary Beth Sullivan
Date of Annotation: August 10, 2005
Other Notes: This document is also applicable to Domain 1 Records creation and maintenance. All four generic requirements and explanatory material in this series of documents may be found on the web at (http://www.nationalarchives.gov.uk/electronicrecords/generic.htm).

Bibliographic Information:
Author: National Archives
Title: Generic requirements to sustain electronic information over time: 3 Sustaining authentic and reliable records: technical requirements
Journal or Book:
Editor(s):
Publication Details: Kew, Richmond, Surrey, UK: National Archives, 6/30/2004
Page Numbers: 1-19
Web Source: National Archives web site
http://www.nationalarchives.gov.uk/electronicrecords/pdf/generic_reqs3.pdf
Description: PDF available on WWW
Subjects: Focus 3/Domain 2/ Terminology Cross-domain / Policy Cross-domain and Government - e-government - preservation of records
Class Descriptor:

Abstract:
"Sustaining authentic and reliable records: technical requirements" discuss the technology required for use and care of electronic records. It is the third of four documents in PDF format on the National Archives web site covering "Generic requirements to sustain electronic information over time". This nineteen page document was published by the National Archives (Kew, Richmond, Surrey, United Kingdom) in 2004.

Annotation:
This document is most relevant to InterPARES in its discussion of technical considerations for preservation of e-government records, and is more appropriate to Domain 3 Methods of appraisal and preservation. "This document is intended to provide the key technical requirements needed to specify and implement a sustainable solution for electronic records." (http://www.nationalarchives.gov.uk/electronicrecords/pdf/generic_reqs3.pdf, p. 3)

Keywords:

Authenticity:
Documentation that verifies the authenticity of a record should come from the caretakers of the records. (p. 16) "In certain circumstances it will (be) necessary for departments to provide copies of sustained records together with a certificate or attestation of authenticity that one or more records are authentic. Logically this would be undertaken by the person or persons responsible for the active maintenance of the sustained records and could take the form of a document, an attachment, or an annotation, which attests to the authenticity of one or more records." (p. 16)

Accuracy:

Reliability:

Other key terms:

Annotator: Mary Beth Sullivan
Date of Annotation: August 11, 2005
Other Notes: All four generic requirements and explanatory material in this series of documents may be found on the web at (http://www.nationalarchives.gov.uk/electronicrecords/generic.htm).

Bibliographic Information:
Author: National Archives
Title: Generic requirements to sustain electronic information over time: 4 Guidance for categorising records to identify sustainable requirements
Journal or Book:
Editor(s):
Publication Details: Kew, Richmond, Surrey, UK: National Archives, 2004
Page Numbers: 1-23
Web Source: National Archives web site:
http://www.nationalarchives.gov.uk/electronicrecords/pdf/generic_reqs4.pdf

Description: PDF available on WWW
Subjects: Focus 3/Domain 2/ Terminology Cross-domain / Policy Cross-domain and Government - - e-government - appraisal of records
Class Descriptor:

Abstract:
"Guidance for categorising records to identify sustainable requirements" discusses how to classify electronic records and satisfy the requirements to maintain them. It is the fourth of four documents in PDF format on the National Archives web site covering "Generic requirements to sustain electronic information over time". This twenty-three page document was published by the National Archives (Kew, Richmond, Surrey, United Kingdom) in 2004.

Annotation:
Pages 11-19 identify the requirements for reliability, integrity, and usability. These are the most pertinent sections for Domain 2, Focus 3. "This document provides high-level guidance for departments seeking to categorise their records to scope the specific nature of the requirements needed to sustain these record categories as authentic records in order to ensure that electronic records which are to be sustained over a defined period of time are able to satisfy the characteristics of a record as defined in BS ISO 15489 that is authenticity, reliability, integrity and usability. If these characteristics are not maintained the sustained records will lose credibility and will lose evidential value." (http://www.nationalarchives.gov.uk/electronicrecords/pdf/generic_reqs4.pdf, p.3) "This document is intended to assist departments to clarify the record attributes that need to be sustained over time. These in turn will help identify broad record categories and the resource requirement needed to sustain the records to a standard appropriate for the duration of the continuing business need." (http://www.nationalarchives.gov.uk/electronicrecords/pdf/generic_reqs4.pdf, p. 7)

Keywords:

Authenticity:
Strategic planning will be essential to secure resources for maintaining authentic records, in order for electronic records management adapts to technology and changes in government. (p. 6) "the ability to predict where resources will need to be allocated according to changes either in software or in terms of machinery of government changes to ensure records are sustained to the appropriate level of authenticity." (p. 6)

This document asserts that there are different levels of authenticity. (p. 7) "The rigour with which sustainable requirements need to be applied will not be the same for all records as the length and type of business and operational use will not be the same. The differences in business and operational use will affect records in a way that will affect their need for authenticity, for example records used in court proceedings need to have a higher level of authenticity than those used for research purposes." (p. 7)

Authenticity may need to be proven maintained and proven over time to show the integrity of records. (p. 14) "…integrity is bound to the need to demonstrate authenticity over time…" (p. 14)

Accuracy:
Trust is linked to accuracy. (p. 11) "Trust is critical to reliability as without it there can be no meaningful faith in the accuracy of the retained records." (p. 11)

Reliability:
This document discusses trust, relationship or context, and longevity in relation to reliability. (p. 11) The document indicates that record context is important to reliability. However, it seems this was a poor word choice, and it may more strongly indicate that context of the records is important to authenticity. (p.11)

There may be varied levels of reliability needed. (p. 12) "Trust is critical to reliability as without it there can be no meaningful faith in the accuracy of the retained records." (p. 11)

"The questions provided … will help determine what contexts or relationships must be maintained for the records to be considered reliable." (p. 11)

"Longevity refers to the duration of the period for which the business still depends on the records to fulfil a residual business need. The requirement for reliability may differ according to the different types or categories of records created and held by a department." (p. 12)

Other key terms:

Integrity and credibility seem to be used to mean trustworthiness and authenticity in this document.

Annotator: Mary Beth Sullivan
Date of Annotation: August 12, 2005
Other Notes: The section on page 9 "Assessing the value of records" may have some use for Domain 3 Methods of appraisal and preservation. All four generic requirements and explanatory material in this series of documents may be found on the web at (http://www.nationalarchives.gov.uk/electronicrecords/generic.htm).

Bibliographic Information:
Author: Public Record Office Victoria
Title: Management of Electronic Records PROS 99/007 (Version 2)
Journal or Book:
Editor(s): Hon. John Thwaites, MP, Minister for Victorian Communties
Publication Details: Victoria: State of Victoria Department for Victorian Communities, 2003
Page Numbers: 1-22
Web Source: Victorian Electronic Records Strategy – Forever Digital web site: http://www.prov.vic.gov.au/vers/standard/standard/default.htm (HTML file) and http://www.prov.vic.gov.au/vers/standard/pdf/99-7_ver2-0.pdf (PDF)
Description: PDF and HTML files on the www
Subjects: Focus 3/Domain 2/ Terminology Cross-domain / Policy Cross-domain and Government - e-government - records management

Class Descriptor:

Abstract:
"Management of Electronic Records PROS 99/007 (Version 2)" is the first of twelve documents that compose the Victorian Electronic Records Strategy. All of the documents indicate how the Public Records Office Victoria is using the Victorian Electronic Records Strategy (VERS) to handle electronic records. VERS attempts to "archive electronic records into a long-term format that is not dependent on a particular computer system (hardware or software)." (http://www.prov.vic.gov.au/vers/standard/ver1/99-7s2.htm) This document describes the format of the records, their structure and metadata, as well as compliance with the standard. This twenty-two page document was published by the Public Record Office Victoria (PROV) (North Melbourne, State of Victoria, Australia) in 2003.

Annotation:
The standard described in this document contains definitions that pertain to authenticity, accuracy, and reliability. These definitions have been extracted for further exploration. "The Victorian Electronic Records Strategy (VERS) addresses the cost-effective, long-term, preservation of electronic records. (http://www.prov.vic.gov.au/vers/standard/version2.htm). "This document is the Standard itself and is primarily concerned with conformance." (http://www.prov.vic.gov.au/vers/standard/pdf/99-7_Advice_ver_2-0.pdf, p. 3) "Recordkeeping 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." (p. 3)

Keywords:

Authenticity:
"authentic (record). An authentic record is one that can be proven to be what it purports to be (i.e. the content is what it appears to be, it was created by the person who appears to have created it and it was created at the time it appears to have been created)." (p. 16)

"preservation (ISO 15489.1 term). Processes and operations involved in ensuring the technical and intellectual survival of authentic records through time." (p. 19)

"migration (ISO 15489.1 term). Act of moving records from one system to another, while maintaining the records' authenticity, integrity, reliability, and useability." (p. 19) "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." (p. 19)

Accuracy:
"digital signature A security mechanism that demonstrates that a particular piece of data (e.g. a record) has not been altered since creation. See certificate, certificate authority, private key, public key, and public/private keypair." (p. 17)

Reliability:
"migration (ISO 15489.1 term). Act of moving records from one system to another, while maintaining the records' authenticity, integrity, reliability, and useability." (p. 19)

Other key terms:

"integrity Integrity refers to the record being complete and with no unauthorised alterations. Note that records can be altered and retain their integrity provided the alterations are allowed by policy, are authorised, and are documented." (p.18)

Annotator: Mary Beth Sullivan
Date of Annotation: August 18, 2005
Other Notes: "The structure and requirements of VERS are formally specified in the Standard for the Management of Electronic Records (PROS 99/007) and its five technical specifications. There are also six Advices that describe aspect of VERS. The relationship between the VERS Standard, the Specifications that support this Standard, and the Introduction and Advices that explain VERS is shown" in a table on the Victorian Electronic Records Strategy – Forever Digital web site. The standard and its five specifications are legal requirements. The six advices are not compulsory. (http://www.prov.vic.gov.au/vers/standard/version2.htm)

Bibliographic Information:
Author: Public Record Office Victoria
Title: Advice 9: Introduction to the Victorian Electronic Records Strategy (VERS)
Journal or Book:
Editor(s): Hon. John Thwaites, MP, Minister for Victorian Communities
Publication Details: Victoria: State of Victoria Department for Victorian Communities, 2003
Page Numbers: 1-31
Web Source: Victorian Electronic Records Strategy – Forever Digital web site:
http://www.prov.vic.gov.au/vers/standard/advice_09/default.htm (HTML file) and
http://www.prov.vic.gov.au/vers/standard/pdf/99-7_Advice_ver_2-0.pdf (PDF)
Description: PDF and HTML files on the www
Subjects: Focus 3/Domain 2/ Terminology Cross-domain / Policy Cross-domain and Government - e-government -records management
Class Descriptor:

Abstract:
"Advice 9: Introduction to the Victorian Electronic Records Strategy (VERS)" is the second of twelve documents that compose the Victorian Electronic Records Strategy. All of the documents indicate how the Public Records Office Victoria is using the Victorian Electronic Records Strategy (VERS) to handle electronic records. VERS attempts to "archive electronic records into a long-term format that is not dependent on a particular computer system (hardware or software)." (http://www.prov.vic.gov.au/vers/standard/ver1/99-7s2.htm) This document provides an overview of VERS and explains its objectives. This thirty-one page document was published by the Public Record Office Victoria (PROV) (North Melbourne, State of Victoria, Australia) in 2003.

Annotation:
As the introductory document to the VERS standard, this document provides an overview of all aspects of the standard, including its technical aspects and application. There seemed to be extensive references to authenticity, accuracy, and reliability. "The Victorian Electronic Records Strategy (VERS) addresses the cost-effective, long-term, preservation of electronic records. (http://www.prov.vic.gov.au/vers/standard/version2.htm). "These properties (context, authenticity, reliability, and integrity) are independent of whether the record is paper or electronic. In both paper and electronic records these properties are not contained in the content of the record. Instead, they are partially represented by information associated with the record content (this information is normally known as 'metadata' when dealing with electronic records). Authenticity, reliability, and integrity are also partially dependent on the processes used to capture and manage the records. The challenge in preserving electronic records is ensuring that the systems that manage the electronic records hold sufficient metadata and implement suitable processes to ensure the long-term retention of context, authenticity, reliability, and integrity." (p. 16) "VERS defines a standard set of metadata that holds the information necessary to show the context, authenticity, reliability, and integrity of a record." (p. 17) "This is to be contrasted to the situation where the metadata is held in a database separate from the content. In this situation it is easily possible to lose the metadata, or to lose the linkage between the metadata and the content. If either of these situations occur, the record context, authenticity, reliability, and integrity are lost." (p. 17)

Keywords:

Authenticity:
"4 Preservation Approach
There are five main challenges when preserving electronic records over a long period. These are:

- program obsolescence
- loss of record context, authenticity and integrity
- media failure
- reliability
- loss of recordkeeping system." (p. 12)

"The context of a record equates to how the record relates to other records held by an organisation. Context is critical to the use of a record. Frequently, an answer to a question will not be given by one record. Instead, a user is interested in understanding a story which is documented in a collection of related records. The context of a record allows the discovery of these related records.

An authentic record is one that is capable of being proved to be what it purports to be (i.e. the content is what it appears to be, it was created by the person who appears to have created it, and it was created at the time it appears to have been created)." (p. 15)

"Management by a recordkeeping system should be viewed as a medium-term solution. Any computer system has a relatively short life – say five to ten years – and there must be a plan to extract records from a system and to migrate them to a replacement system (or to manage them by some other mechanism if there is no replacement system). This migration is likely to be complex, as it is necessary to preserve sufficient information to show that the record was properly managed to ensure authenticity and integrity when under control of the original system. A particular concern about migration is that this may have to occur under extreme time or budgetary constraints." (p. 17)

"Many archives do not specify that it is necessary to digitally sign records. Instead, integrity is shown by custody in an archival system. This has been the traditional approach to showing authenticity and integrity of paper records held by an archive. The reason PROV feels that this is inappropriate for electronic records is that custody was always backed up by forensic tests with paper records. Such tests are in their infancy with electronic records. Further, a digital archive is a far less benign environment than a paper repository and records can easily be altered by software bugs and hardware failures. Such failures can systematically affect large parts of the collection. It was felt that a verification mechanism independent of the digital archive was desirable." (p. 17-18)

"Documenting the history of the record. It must be possible to document the history of the record from the time of its creation. This includes the registration of the record, reclassification or alteration to the context of the record, any preservation actions (e.g. format conversions), transfers between recordkeeping systems, and export to PROV.
This is to prevent the loss of context, authenticity, and integrity discussed in section 4.2." (p. 22)

"Documenting the creation of the record (i.e. being able to show that a record is authentic). This includes documenting who registered the record, when it was registered, and the context of the registration. This is to prevent the loss of authenticity discussed in section 4.2." (p. 22)

"…metadata prevents the loss of context, authenticity, and integrity described in section 4.2." (p. 25)
"These properties (context, authenticity, reliability, and integrity) are independent of whether the record is paper or electronic. In both paper and electronic records these properties are not contained in the content of the record. Instead, they are partially represented by information associated with the record content (this information is normally known as 'metadata' when dealing with electronic records). Authenticity, reliability, and integrity are also partially dependent on the processes used to capture and manage the records. The challenge in preserving electronic records is ensuring that the systems that manage the electronic records hold sufficient metadata and implement suitable processes to ensure the long-term retention of context, authenticity, reliability, and integrity." (p. 16)

Accuracy:
"The unfortunate problem with obtaining a program to display a particular format is that programs are inherently fragile. They depend for their correct operation on a complicated computer infrastructure." (p. 13)

"One final issue with program obsolescence is the accuracy of rendering the information. Programs interpret the digital data." (p. 13)

"Formal de jure standards are preferred as long-term preservation formats, however, because it is more likely that vendors will implement them accurately. The problem with proprietary formats, particularly those where only one or two implementations exist, is that the vendor that owns the format may 'cheat' and either not implement the format accurately, or add additional undocumented features." (p. 14)

"…PROV has judged that a key characteristic of record it was necessary to preserve was the appearance of the record as the original creator saw it. This led to the selection of PDF as a long-term preservation format over an XML format, as PDF can ensure a far more accurate representation." (p. 14)

"Published formats are preferred to unpublished industry standard formats, for two reasons:

- There may be only a short window of opportunity for conversion before an obsolete format becomes unreadable. An archive must monitor the obsolescence of the formats and fund conversion before this window closes.
- The conversion is dependent on externally sourced products and may not be sufficiently accurate for archival purposes." (p. 15)

"Conversion to a long-term preservation format is a conversion process, similar to digitising or microfilming paper records, and an agency or archive must ensure accuracy of conversion. For example, there are many methods of converting to PDF, but some of them can produce inaccurate representations of the record. The mechanisms used in microfilming or digitising (e.g. statistical sampling of the conversion process) can be used in ensuring accuracy of digital conversion." (p. 15)

"The timing of the conversion has a bearing on the accuracy of conversion. Where the record is converted sometime after it is created, the conversion accuracy may be limited. This may occur, for example, if the conversion program is upgraded and this changes the results of the conversion. In selecting a conversion process, it is worth considering whether the process is used for day-to-day business activities, as this vastly improves the conversion accuracy." (p. 15)

"Records may be lost by system failure. Such failures can include:

- Corruption due to failure to accurately copy records from one place to another. This includes errors in copying from one piece of media to another, or from disk into memory. A particular challenge with preventing this type of failure is identifying all those locations in the computer system where records are copied.
- Corruption due to failure of indexing. This may result in the records still physically existing but the recordkeeping system 'forgetting' that the record exists.

- Hardware failure. Records ultimately have a physical representation, either on media (e.g. disk or tape), or in memory. Hardware failures such as disk crashes can cause the loss of the record.
- Disaster. Records will be lost if the computer holding them is damaged by a disaster such as a fire or flood." (p. 20)

"Conversion to long-term preservation format. At some point the record content must be converted to a long-term preservation format to ensure that access to the record is independent of the application that created it. This issue is discussed extensively in section 4.1. Conversion may occur at any time, but two common points are when the record is registered, or when the record is exported. Late conversion increases the risk of record loss, as it increases the chance that the necessary application will not be available or will produce an inaccurate conversion." (p. 22)

"Refreshing. The recordkeeping system must be capable of accurately refreshing the media on which the records are held. This is to cover the mechanical and chemical deterioration of both the media and the hardware that reads the media, as discussed in section 4.3." (p. 22-23)

Reliability:
"The focus of the Standard is therefore on:

- the functions that recordkeeping systems in agencies must support in order to preserve electronic records whilst they are being held by the agency
- the physical representation of the records when they are exported from an agency to PROV
- the mechanisms used to reliably export records from an agency to PROV." (p. 11)

"A reliable record is one that contains a full and reliable representation of the facts which the record documents. Note that a record can be authentic, but not reliable. A record is not reliable, for example, if the author of the record left out material facts, misrepresented the position, or simply lied. Such a record would still be authentic as the content is as the author intended and it was created by the apparent author at the apparent time. Authenticity is concerned with the truth of the record as an object; reliability is concerned with the truth of the contents of the record." (p. 15)

"Reliability. The recordkeeping system must not lose records entrusted to its care, as discussed in section 4.4. Records may be lost by software failures (e.g. inaccurate copying), or by catastrophes (e.g. the system being destroyed). Reliability is partially addressed by the quality of the engineering within the recordkeeping program; including that defensive coding practices have been applied (these check that functions have worked correctly). However, quality software will not, by itself, be sufficient to ensure that records are never lost. All software must be assumed to contain bugs. In addition, software cannot guard against hardware failures or natural disasters. To prevent the loss of records, the agency responsible for the recordkeeping system must institute and test a proper backup and disaster-recovery regime." (p. 22)

"The VERS Standard requires the recordkeeping system as a whole to be reliable. In this case the system is not just considered to be the actual recordkeeping application, but includes:

- the hardware on which the application runs
- the system software, such as the operating system and storage management systems
- the processes and procedures that surround the system such as back-up regimes and disaster recovery." (p. 20)

Other key terms:

There is a useful discussion of electronic record keeping on page 16. This may be relevant to Domain 2, Focus 3, but also to Domain 1, Focus 3 for perspectives on record creation and maintenance. “In a traditional paper-based recordkeeping system these properties are largely demonstrated by the procedures involved in the creation, storage, and handling of the record. For example, reliability is shown by the fact that the record was created for future reference as part of a standard business procedure. Authenticity and integrity is shown by the procedures involved in managing and controlling access to records. Ultimately, these procedures are backed up by conventional forensic tests such as tests on signatures, the age of the paper, type of typewriter, and ink. This reliance on procedures can be transferred to many electronic records, particularly those managed by application specific systems. Consider a financial system, for example. The records would be considered reliable because they are automatically generated by the system as a side-effect of carrying out financial tasks. They are authentic because the actions can only be carried out via the financial system and the system keeps logs of who carried out the task, when it was carried out, and how the tasks are related. Finally, the logs record any changes to the records, and hence the records have integrity. However, many electronic records are not managed in such a formal way. This particularly applies to those records held in generic software applications (e.g. email systems) or in the general file system. Fundamentally, the problem is that these systems are not designed to ensure authentic records or to ensure their integrity once created. These records can be the most important held by an agency; for example, they may document the development of government policy. One method of ensuring authenticity and integrity of these records is to install an application that is designed to manage records and to ensure their authenticity and integrity (a recordkeeping system). Once records are registered with the recordkeeping system, the system can ensure that the record retains integrity. Essentially, the recordkeeping system acts as a vault, mediating and recording access to the records. Just like the financial system, the recordkeeping system only allows certain operations on the registered records, only allows authorised users to perform those operations, and keeps audit trails of all operations. However, there are several issues with using a recordkeeping system to ensure the reliability and integrity of records. The effectiveness of a recordkeeping system depends on users placing their records under the control of the system. At some point, for example, users must move their emails from their mailbox to the recordkeeping system. This is to be contrasted to a financial system, for example, where the system is used to carry out the tasks associated with managing money, the records being automatically generated as a side-effect. With a recordkeeping system, the tasks are carried out in other applications and users have to consciously decide to place the records under the control of the system.” (p. 16)

Annotator: Mary Beth Sullivan
Date of Annotation: August 22, 2005
Other Notes: “The structure and requirements of VERS are formally specified in the Standard for the Management of Electronic Records (PROS 99/007) and its five technical specifications. There are also six Advices that describe aspect of VERS. The relationship between the VERS Standard, the Specifications that support this Standard, and the Introduction and Advices that explain VERS is shown” in a table on the Victorian Electronic Records Strategy – Forever Digital web site. The standard and its five specifications are legal requirements. The six advices are not compulsory. (http://www.prov.vic.gov.au/vers/standard/version2.htm) “Integrity refers

to the record being complete and without unauthorised alterations. Note that records can be altered and retain their integrity, provided the alterations are allowed by the policy of the organisation, are authorised, and are documented." (p. 15)

Bibliographic Information:
Author: Public Record Office Victoria
Title: Specification 1: System Requirements for Preserving Electronic Records
Journal or Book:
Editor(s): Hon. John Thwaites, MP, Minister for Victorian Communities
Publication Details: Victoria: State of Victoria Department for Victorian Communities, 2003
Page Numbers: 1-11
Web Source: Victorian Electronic Records Strategy – Forever Digital web site:
http://www.prov.vic.gov.au/vers/standard/spec_01/default.htm (HTML file) and
http://www.prov.vic.gov.au/vers/standard/pdf/99-7-1_Std_ver_2-0.pdf (PDF)

Description: PDF and HTML files on the www
Subjects: Focus 3/Domain 2/ Terminology Cross-domain / Policy Cross-domain and Government - e-government - records management
Class Descriptor:

Abstract:
"Specification 1: System Requirements for Preserving Electronic Records" is the third of twelve documents that compose the Victorian Electronic Records Strategy. All of the documents indicate how the Public Records Office Victoria is using the Victorian Electronic Records Strategy (VERS) to handle electronic records. VERS attempts to "archive electronic records into a long-term format that is not dependent on a particular computer system (hardware or software)." (http://www.prov.vic.gov.au/vers/standard/ver1/99-7s2.htm) This document contains both requirements and recommendations for an electronic recordkeeping system. This eleven page document was published by the Public Record Office Victoria (PROV) (North Melbourne, State of Victoria, Australia) in 2003.

Annotation:
This document specifies how authenticity, accuracy and reliability are maintained in an electronic record keeping system. "The Victorian Electronic Records Strategy (VERS) addresses the cost-effective, long-term, preservation of electronic records. (http://www.prov.vic.gov.au/vers/standard/version2.htm).

Keywords:

Authenticity:
"The following list summarises the VERS functional requirements for a system that preserves electronic records:
…
The system must manage the record while it is being held in the recordkeeping system such that it is possible to:

- demonstrate that the record is authentic
- demonstrate that a record has not been modified in an unauthorised fashion (i.e. that it retains integrity)
- modify a record
- document the history of the record
- copy the records to new storage media (also known as ‘refreshing’)
- reliably retain the record despite system failures and disasters
- export the records to another system.” (p. 7-8)

“The recordkeeping system must be capable of demonstrating that a record is authentic; that is, the system must prove that the content is what it appears to be, who created it, and when it was created.” (p. 9)

Accuracy:
“The accuracy of any copy must be verified by ensuring that all records or folders which have not been marked for destruction have been copied, and that the contents of the records or folders have been copied accurately.” (p. 10)

“The accuracy of the refresh must be verified by ensuring that all records and folders (except those which have been disposed of) have been copied, and that the contents of the records and folders have been copied accurately.” (p. 10)

Reliability:
“3.7 Reliability
The system must not lose records or folders once they have been registered with the recordkeeping system.
Records or folders must not be lost due to catastrophic failure of the system, media failure, or physical disaster (e.g. fire).” (p.11)

Other key terms:

Annotator: Mary Beth Sullivan
Date of Annotation: August 23, 2005
Other Notes: “The structure and requirements of VERS are formally specified in the Standard for the Management of Electronic Records (PROS 99/007) and its five technical specifications. There are also six Advices that describe aspect of VERS. The relationship between the VERS Standard, the Specifications that support this Standard, and the Introduction and Advices that explain VERS is shown” in a table on the Victorian Electronic Records Strategy – Forever Digital web site. The standard and its five specifications are legal requirements. The six advices are not compulsory. (http://www.prov.vic.gov.au/vers/standard/version2.htm)

Bibliographic Information:
Author: Public Record Office Victoria
Title: Specification 2: VERS Metadata Scheme
Journal or Book:

Editor(s): Hon. John Thwaites, MP, Minister for Victorian Communities
Publication Details: Victoria: State of Victoria Department for Victorian Communities, 2003
Page Numbers: 1-149
Web Source: Victorian Electronic Records Strategy – Forever Digital web site:
http://www.prov.vic.gov.au/vers/standard/spec_02/default.htm (HTML file) and
http://www.prov.vic.gov.au/vers/standard/pdf/99-7-2_Std_ver2-0.pdf (PDF)
Description: PDF and HTML files on the www
Subjects: Focus 3/Domain 2/ Terminology Cross-domain / Policy Cross-domain and Government - e-government - records management
Class Descriptor:

Abstract:

“Specification 2: VERS Metadata Scheme” is the fourth of twelve documents that compose the Victorian Electronic Records Strategy. All of the documents indicate how the Public Records Office Victoria is using the Victorian Electronic Records Strategy (VERS) to handle electronic records. VERS attempts to “archive electronic records into a long-term format that is not dependent on a particular computer system (hardware or software).” (http://www.prov.vic.gov.au/vers/standard/ver1/99-7s2.htm) This document describes metadata used in VERS Encapsulated Object (VEO) format. This one hundred forty-nine page document was published by the Public Record Office Victoria (PROV) (North Melbourne, State of Victoria, Australia) in 2003.

Annotation:

The definitions and purposes of the metadata in VERS Encapsulated Object (VEO) format are explained in this specification The metadata captured is intended to address authenticity and accuracy. “The Victorian Electronic Records Strategy (VERS) addresses the cost-effective, long-term, preservation of electronic records. (http://www.prov.vic.gov.au/vers/standard/version2.htm).

Keywords:

Authenticity:

“The date and time the VERS object was created… This element is crucial in establishing the authenticity of a VERS record because knowing and being able to prove when a record was created may be vital for evidentiary or historical reasons.” (p. 27)

“Metadata that describes the record as a whole. This group of elements contains contextual information about the record that is crucial to establishing the veracity and authenticity of the record.” (p. 30)

“The dates and times at which the fundamental recordkeeping actions of creation, transaction and registration occur… This group of elements provides system validation of the acts of creation, transaction and registration. It acts in combination with other metadata elements added at creation, transaction and registration, to provide evidence of the record’s authenticity.” (p. 67)

“The date and time at which the record is captured into the recordkeeping system… This element documents the date and time that the record came under the management and control of a formal recordkeeping system. It acts as a search point for records management purposes.

The date and time a record comes under formal records management control can be crucial in proving the authenticity and integrity of that record." (p. 70)

"vers: SignatureFormatDescription… This is a textual description of the process used to sign the VEO… This element enables a human reader to understand and verify the signature that has been used to ensure the VERS record's integrity and authenticity." (p. 132)

"vers: Signature… This is the digital signature itself… This element contains the digital signature used to ensure the VERS record's integrity and authenticity." (p. 134)

"vers: FileMetadata… Metadata that describes the file as a whole. This contains contextual information about the file that is crucial to establish the veracity and authenticity of the records." (p. 137)

Accuracy:
"vers: Subject… The subject or topic of a record that concisely and accurately describes the record's content… The subject acts as a resource discovery access point at a finer level of detail than that provided by the element M32 TITLE. Some users may require searching capability at individual keyword level, rather than just by the title as a whole." (p. 55)

"vers: DocumentSubject… The subject or topic of a Document that concisely and accurately describes the Document's content." (p. 120)

Reliability:

Other key terms:

Exploration of the metadata described in this specification may help InterPARES with the work regarding methods of preservation in Domain 3, Focus 3.

Annotator: Mary Beth Sullivan
Date of Annotation: August 24, 2005
Other Notes: "The structure and requirements of VERS are formally specified in the Standard for the Management of Electronic Records (PROS 99/007) and its five technical specifications. There are also six Advices that describe aspect of VERS. The relationship between the VERS Standard, the Specifications that support this Standard, and the Introduction and Advices that explain VERS is shown" in a table on the Victorian Electronic Records Strategy – Forever Digital web site. The standard and its five specifications are legal requirements. The six advices are not compulsory. (http://www.prov.vic.gov.au/vers/standard/version2.htm)

Bibliographic Information:
Author: Victoria Public Record Office
Title: Specification 3: VERS Standard Electronic Record Format
Journal or Book:
Editor(s): Hon. John Thwaites, MP, Minister for Victorian Communities

Publication Details: Victoria: State of Victoria Department for Victorian Communities, 2003
Page Numbers: 1-19
Web Source: Victorian Electronic Records Strategy – Forever Digital web site:
http://www.prov.vic.gov.au/vers/standard/spec_03/default.htm (HTML file) and
http://www.prov.vic.gov.au/vers/standard/pdf/99-7-3_Std_ver_2-0.pdf (PDF)
Description: PDF and HTML files on the www
Subjects: Focus 3/Domain 2/Policy Cross-domain and Government - e-government - records management
Class Descriptor:

Abstract:
"Specification 3: VERS Standard Electronic Record Format" is the fifth of twelve documents that compose the Victorian Electronic Records Strategy. All of the documents indicate how the Public Records Office Victoria is using the Victorian Electronic Records Strategy (VERS) to handle electronic records. VERS attempts to "archive electronic records into a long-term format that is not dependent on a particular computer system (hardware or software)." (http://www.prov.vic.gov.au/vers/standard/ver1/99-7s2.htm) This document defines the standard electronic record format for the Victorian Electronic Records Strategy, referred to as VERS Encapsulated Object (VEO). It provides information about the XML requirements, encryption, required digital signatures, and the document type definition. This nineteen page document was published by the Public Record Office Victoria (PROV) (North Melbourne, State of Victoria, Australia) in 2003.

Annotation:
This specification is a technical document not suited to the purposes of Focus 3/Domain 2. It does not contain any references to authenticity, accuracy, and reliability and does not make use of relevant synonyms.
"The Victorian Electronic Records Strategy (VERS) addresses the cost-effective, long-term, preservation of electronic records. (http://www.prov.vic.gov.au/vers/standard/version2.htm).

Keywords:

Authenticity:

Accuracy:

Reliability:

Other key terms:

Annotator: Mary Beth Sullivan
Date of Annotation: August 24, 2005
Other Notes: "The structure and requirements of VERS are formally specified in the Standard for the Management of Electronic Records (PROS 99/007) and its five technical specifications. There are also six Advices that describe aspect of VERS. The relationship between the VERS Standard, the Specifications that support this Standard, and the Introduction and Advices that

explain VERS is shown" in a table on the Victorian Electronic Records Strategy – Forever Digital web site. The standard and its five specifications are legal requirements. The six advices are not compulsory. (http://www.prov.vic.gov.au/vers/standard/version2.htm)

Bibliographic Information:
Author: Public Record Office Victoria
Title: Specification 4: VERS Long Term Preservation Formats
Journal or Book:
Editor(s): Hon. John Thwaites, MP, Minister for Victorian Communities
Publication Details: Victoria: State of Victoria Department for Victorian Communities, 2003
Page Numbers: 1-11
Web Source: Victorian Electronic Records Strategy – Forever Digital web site:
http://www.prov.vic.gov.au/vers/standard/spec_04/default.htm (HTML file) and
http://www.prov.vic.gov.au/vers/standard/pdf/99-7-4_Std_ver_2-0.pdf (PDF)

Description: PDF and HTML files on the www
Subjects: Focus 3/Domain 2/ Policy Cross-domain and Government - e-government - records management
Class Descriptor:

Abstract:
"Specification 4: VERS Long Term Preservation Formats" is the sixth of twelve documents that compose the Victorian Electronic Records Strategy. All of the documents indicate how the Public Records Office Victoria is using the Victorian Electronic Records Strategy (VERS) to handle electronic records. VERS attempts to "archive electronic records into a long-term format that is not dependent on a particular computer system (hardware or software)." (http://www.prov.vic.gov.au/vers/standard/ver1/99-7s2.htm) This document gives the file formats, file encoding, and file settings that meet VERS requirements. This eleven page document was published by the Public Record Office Victoria (PROV) (North Melbourne, State of Victoria, Australia) in 2003.

Annotation:
This specification is a technical document not suited to the purposes of Focus 3/Domain 2. It does not contain any references to authenticity, accuracy, and reliability and does not make use of relevant synonyms.
"The Victorian Electronic Records Strategy (VERS) addresses the cost-effective, long-term, preservation of electronic records. (http://www.prov.vic.gov.au/vers/standard/version2.htm).

Keywords:

Authenticity:

Accuracy:

Reliability:

Other key terms:

Annotator: Mary Beth Sullivan
Date of Annotation: August 24, 2005
Other Notes: "The structure and requirements of VERS are formally specified in the Standard for the Management of Electronic Records (PROS 99/007) and its five technical specifications. There are also six Advices that describe aspect of VERS. The relationship between the VERS Standard, the Specifications that support this Standard, and the Introduction and Advices that explain VERS is shown" in a table on the Victorian Electronic Records Strategy – Forever Digital web site. The standard and its five specifications are legal requirements. The six advices are not compulsory. (http://www.prov.vic.gov.au/vers/standard/version2.htm)

Bibliographic Information:
Author: Public Record Office Victoria
Title: Specification 5: Export of Electronic Records to PROV
Journal or Book:
Editor(s): Hon. John Thwaites, MP, Minister for Victorian Communities
Publication Details: Victoria: State of Victoria Department for Victorian Communities, 2003
Page Numbers: 1-11
Web Source: Victorian Electronic Records Strategy – Forever Digital web site:
http://www.prov.vic.gov.au/vers/standard/spec_05/default.htm (HTML file) and
http://www.prov.vic.gov.au/vers/standard/pdf/99-7-5_Std_ver_2-0.pdf (PDF)
Description: PDF and HTML files on the www
Subjects: Focus 3/Domain 2/ Policy Cross-domain and Government - e-government - records management
Class Descriptor:

Abstract:
"Specification 5: Export of Electronic Records to PROV" is the seventh of twelve documents that compose the Victorian Electronic Records Strategy. All of the documents indicate how the Public Records Office Victoria is using the Victorian Electronic Records Strategy (VERS) to handle electronic records. VERS attempts to "archive electronic records into a long-term format that is not dependent on a particular computer system (hardware or software)." (http://www.prov.vic.gov.au/vers/standard/ver1/99-7s2.htm) This document discusses physical transfer of records including media types, archiving software, and acknowledgements for receipt of records. This eleven page document was published by the Public Record Office Victoria (PROV) (North Melbourne, State of Victoria, Australia) in 2003.

Annotation:
This specification is a technical document not suited to the purposes of Focus 3/Domain 2. It does not contain any references to authenticity, accuracy, and reliability and does not make use of relevant synonyms.
"The Victorian Electronic Records Strategy (VERS) addresses the cost-effective, long-term, preservation of electronic records. (http://www.prov.vic.gov.au/vers/standard/version2.htm).

Keywords:

Authenticity:

Accuracy:

Reliability:

Other key terms:

Annotator: Mary Beth Sullivan
Date of Annotation: August 24, 2005
Other Notes: “The structure and requirements of VERS are formally specified in the Standard for the Management of Electronic Records (PROS 99/007) and its five technical specifications. There are also six Advices that describe aspect of VERS. The relationship between the VERS Standard, the Specifications that support this Standard, and the Introduction and Advices that explain VERS is shown” in a table on the Victorian Electronic Records Strategy – Forever Digital web site. The standard and its five specifications are legal requirements. The six advices are not compulsory. (http://www.prov.vic.gov.au/vers/standard/version2.htm)

Bibliographic Information:
Author: Public Record Office Victoria
Title: Advice 10: System Requirements for Preserving Electronic Records
Journal or Book:
Editor(s): Hon. John Thwaites, MP, Minister for Victorian Communities
Publication Details: Victoria: State of Victoria Department for Victorian Communities, 2003
Page Numbers: 1-21
Web Source: Victorian Electronic Records Strategy – Forever Digital web site:
http://www.prov.vic.gov.au/vers/standard/advice_10/default.htm (HTML file) and
http://www.prov.vic.gov.au/vers/standard/pdf/99-7-1_Advice_ver_2-0.pdf (PDF)
Description: PDF and HTML files on the www
Subjects: Focus 3/Domain 2/ Terminology Cross-domain / Policy Cross-domain and Government - e-government - records management
Class Descriptor:

Abstract:
“Advice 10: System Requirements for Preserving Electronic Records” is the eighth of twelve documents that compose the Victorian Electronic Records Strategy. All of the documents indicate how the Public Records Office Victoria is using the Victorian Electronic Records Strategy (VERS) to handle electronic records. VERS attempts to “archive electronic records into a long-term format that is not dependent on a particular computer system (hardware or software).” (http://www.prov.vic.gov.au/vers/standard/ver1/99-7s2.htm) This document gives advice on Specification 1 and imposes no additional mandatory requirements. It discusses authenticity, integrity, document conversion, metadata, modifying information associated with records and folders, documenting the history of records and folders reliability, media, and record

export. This twenty-one page document was published by the Public Record Office Victoria (PROV) (North Melbourne, State of Victoria, Australia) in 2003.

Annotation:
This document provides advice on how to conform with system requirements to meet the VERS standard. The system requirements include demands for authenticity, accuracy, and reliability. "The Victorian Electronic Records Strategy (VERS) addresses the cost-effective, long-term, preservation of electronic records. (http://www.prov.vic.gov.au/vers/standard/version2.htm).

Keywords:

Authenticity:
"The recordkeeping system must be capable of demonstrating that a record is authentic; that is, the system must prove that the content is what it appears to be, who created it, and when it was created.

The recordkeeping system must record the identity of the user creating the record and the time it was created. This information must not be forgeable or capable of being altered by either users or system administrators.

Authenticity is derived from the business processes associated with the creation of the record, in particular where the record is captured as part of the normal process of doing business. The recordkeeping system demonstrates authenticity by means of metadata captured when the record is registered. From a technology perspective, demonstrating authenticity is dependent upon the accuracy of the metadata being captured and whether this metadata can be shown to be unaltered." (p. 8)

"Ensuring that the metadata proving authenticity is unchanged after capture is an aspect of record integrity and is discussed in the next section." (p. 9)

"It must not be possible for any users, records managers, or system administrators to modify the audit log without a record being made of the modification. If an audit log can be modified without a record being kept of this modification, no trust could be placed in the audit trail. Modifications include complete or partial deletion of the audit log." (p. 14)

Accuracy:
"Conversion upon registration is preferred, as problems with the conversion are more likely to be detectable and correctable. Typical problems with late conversion can include:

- password-protected files which can no longer be opened
- inaccurate conversion due to 'upgrading' of software (which may include plugins).

Inaccurate conversions include changes in appearance of the content (e.g. repagination, changes in fonts, etc.)" (p. 11)

"Conformance is shown by the implementation of a suitable disaster recovery regime where policies and procedures are set down to ensure that records are backed up off-site. PROV may audit the agency to ensure that the disaster recovery regime is being carried out diligently and correctly." (p. 16)

"The accuracy of any copy must be verified by ensuring that all records or folders which have not been marked for destruction have been copied, and that the contents of the records or folders have been copied accurately.
The purpose of copying records and folders is to provide a substitute for the originals should they be destroyed. Consequently, the production of a backup copy must be treated in all particulars as if the Record was being refreshed to new media. In particular, the accuracy of the copy must be checked.

Conformance can be achieved by a formal statement from the vendor responsible for the disaster recovery software that the accuracy of copies is verified." (p. 16)

"The accuracy of the refresh must be verified by ensuring that all records and folders (except those which have been disposed of) have been copied, and that the contents of the records and folders have been copied accurately.
Accuracy is normally ensured by verifying the copy (i.e. checking that all records and folders have been copied and performing a bitwise comparison of the original record and the copy).

Conformance to this point is the responsibility of the vendor supplying the software performing the refresh, and is achieved by the vendor supplying a statement certifying that all refreshes are verified as accurate copies." (p. 17)

Reliability:
"Note that reliability in this context is only concerned with ensuring reliable storage and handling of electronic records. It is not concerned with the reliable provision of service. While the provision of service is important, it is not an aspect of preservation.

Conformance is achieved by a formal statement from the vendor about the processes used to prevent record losses." (p. 15)

Other key terms:

Annotator: Mary Beth Sullivan
Date of Annotation: August 25, 2005
Other Notes: "The structure and requirements of VERS are formally specified in the Standard for the Management of Electronic Records (PROS 99/007) and its five technical specifications. There are also six Advices that describe aspect of VERS. The relationship between the VERS Standard, the Specifications that support this Standard, and the Introduction and Advices that explain VERS is shown" in a table on the Victorian Electronic Records Strategy – Forever Digital web site. The standard and its five specifications are legal requirements. The six advices are not compulsory. (http://www.prov.vic.gov.au/vers/standard/version2.htm)

Bibliographic Information:
Author: Public Record Office Victoria
Title: Advice 11: VERS Metadata Scheme
Journal or Book:

Editor(s): Hon. John Thwaites, MP, Minister for Victorian Communities
Publication Details: Victoria: State of Victoria Department for Victorian Communities, 2003
Page Numbers: 1-54
Web Source: Victorian Electronic Records Strategy – Forever Digital web site: http://www.prov.vic.gov.au/vers/standard/advice_11/default.htm (HTML file) and http://www.prov.vic.gov.au/vers/standard/pdf/99-7-2_Advice_ver_2-0.pdf (PDF)
Description: PDF and HTML files on the www
Subjects: Focus 3/Domain 2/ Terminology Cross-domain / Policy Cross-domain and Government - e-government - records management
Class Descriptor:

Abstract:
“Advice 11: VERS Metadata Scheme” is the ninth of twelve documents that compose the Victorian Electronic Records Strategy. All of the documents indicate how the Public Records Office Victoria is using the Victorian Electronic Records Strategy (VERS) to handle electronic records. VERS attempts to “archive electronic records into a long-term format that is not dependent on a particular computer system (hardware or software).” (http://www.prov.vic.gov.au/vers/standard/ver1/99-7s2.htm) This document describes how to use the metadata and imposes no additional mandatory requirements. This fifty-four page document was published by the Public Record Office Victoria (PROV) (North Melbourne, State of Victoria, Australia) in 2003.

Annotation:
The advice in this document briefly refers to authenticity and accuracy as they apply to the metadata in the VERS standard.
“The Victorian Electronic Records Strategy (VERS) addresses the cost-effective, long-term, preservation of electronic records. (http://www.prov.vic.gov.au/vers/standard/version2.htm).

Keywords:

Authenticity:
“Digital Signature (M23). This subelement contains a digital signature applied by the agent to provide proof as to the authenticity and integrity of the record. This element is deprecated in VERS, as the same function is performed by the Signature Block (M134) element. This subelement could be used if the record has been digitally signed outside the VERS system, but agencies should note that a significant amount of information must be available to validate a digital signature.” (p. 12)

Accuracy:
“The Preservation History (M76) element lists the preservation actions that have taken place on a record. The intent is that this element will document events that may affect the quality or accuracy of the record. A typical preservation event is format conversion (e.g. from Word to PDF).” (p. 27)

Reliability:

Other key terms:

Annotator: Mary Beth Sullivan
Date of Annotation: August 25, 2005
Other Notes: "The structure and requirements of VERS are formally specified in the Standard for the Management of Electronic Records (PROS 99/007) and its five technical specifications. There are also six Advices that describe aspect of VERS. The relationship between the VERS Standard, the Specifications that support this Standard, and the Introduction and Advices that explain VERS is shown" in a table on the Victorian Electronic Records Strategy – Forever Digital web site. The standard and its five specifications are legal requirements. The six advices are not compulsory. (http://www.prov.vic.gov.au/vers/standard/version2.htm)

Bibliographic Information:
Author: Public Record Office Victoria
Title: Advice 12: VERS Standard Electronic Record Format
Journal or Book:
Editor(s): Hon. John Thwaites, MP, Minister for Victorian Communities
Publication Details: Victoria: State of Victoria Department for Victorian Communities, 2003
Page Numbers: 1-81
Web Source: Victorian Electronic Records Strategy – Forever Digital web site: http://www.prov.vic.gov.au/vers/standard/advice_12/default.htm (HTML file) and http://www.prov.vic.gov.au/vers/standard/pdf/99-7-3_Advice_ver_2-0.pdf (PDF)
Description: PDF and HTML files on the www
Subjects: Focus 3/Domain 2/ Terminology Cross-domain / Policy Cross-domain and Government - e-government - records management
Class Descriptor:

Abstract:
"Advice 12: VERS Standard Electronic Record Format" is the tenth of twelve documents that compose the Victorian Electronic Records Strategy. All of the documents indicate how the Public Records Office Victoria is using the Victorian Electronic Records Strategy (VERS) to handle electronic records. VERS attempts to "archive electronic records into a long-term format that is not dependent on a particular computer system (hardware or software)." (http://www.prov.vic.gov.au/vers/standard/ver1/99-7s2.htm) This document is a guide to VERS Encapsulated Object (VEO) and imposes no additional mandatory requirements. This eighty-one page document was published by the Public Record Office Victoria (PROV) (North Melbourne, State of Victoria, Australia) in 2003.

Annotation:
"The Victorian Electronic Records Strategy (VERS) addresses the cost-effective, long-term, preservation of electronic records. (http://www.prov.vic.gov.au/vers/standard/version2.htm).

Keywords:

Authenticity:
"2 Goals behind the VEO design

We believe that there are four basic principles that need to be adopted in preserving electronic records. These are:

- Self-sufficiency. As far as possible, the electronic record should be independent of systems, outside data, and documentation.
- Structured textual encoding. The information that encapsulates the content should be encoded as a structured piece of text rather than as binary data.
- Integrity. It must be possible to demonstrate that the record is either unmodified or that any modifications are documented and are authorised.
- Preservation of authenticity and context. It must be possible to show who created the record, when it was created, what the record documents, and how the record relates to other records." (p. 7)

"2.4 Preservation of authenticity and context
Authenticity and context are documented in the record or folder that contains the record. This documentation is normally represented as metadata. VERS provides extensive metadata to hold this information and this aspect of recordkeeping is discussed in PROS 99/007 Specification 2: VERS Metadata Scheme, and its associated advice (Advice 11)." (p. 10)

"Attachments to the email can then be included as sub-Documents beneath the email body Document, clearly differentiating between the body and the attachments (which the user may not have opened). Finally, additional Documents can be used to represent the remaining header information not presented to the user (this information shows how the email was transmitted and may be critical in demonstrating the integrity and authenticity of the email)." (p. 16)

"5.2 Public key storage in VERS
Validation of a digital signature requires the public key of the signer. If the public key has been lost or discarded the integrity of the preserved object cannot be verified using digital signatures. Further, verification depends on being certain that the stored public key actually belonged to the purported signer (otherwise the preserved object could be modified, resigned, and the public key replaced). Public keys must consequently be securely stored for the lifespan of the signed objects; this could be for a century or more. Note that private keys should not be archived; indeed, proof of authenticity is improved if it can be shown that private keys are destroyed once their use has ceased." (p. 33)

"When using this approach to verify the integrity of a digital signature on an electronic record, the first step is to verify the digital signature using the certificates contained in the record. This shows that the content of the record has not changed since the record was signed and that the certificates actually belong to the record. The second step is to choose another record signed by that user around that time and compare the certificates in the two records. The certificates should be identical. If they are, then either a forger has forged both records or both records are authentic. (In practice the test is slightly more involved than this, as a user's private key is periodically replaced and the certificates will validly change.) Clearly, the certificates in the suspect record should be compared with those in more than one record signed by that user; the more records compared, the more likely the records are valid. This is a probabilistic approach, but with a sufficiently large number of digital objects there would be strong evidence that the records have not been tampered with. The security can be increased further by arranging for a record to be signed multiple times." (p. 35)

Accuracy:
"The contents of the signature block are:

- Signature Format Description (M135). This element is a textual description of the process of generating the digital signature. It is intended to be read by developers in the future who are implementing software to verify the digital signature. Recommended values for this element are given in PROS 99/007: Specification 2, VERS Metadata Scheme.
- Signature Algorithm (M149). This element identifies the algorithms used to generate the digital signature. It is explained in more detail in section 5.3.1.
- Signature (M138). This element contains the actual digital signature. It is encoded in Base 64.
- Certificate Block (M139). This element contains the certificates necessary to verify the digital signature. This element is explained in more detail in section 5.3.2.
- Signer (M137) and Signature Date (M136). These elements are purely descriptive.

They contain the name of the organisation or person who applied the digital signature, and the date the signature was applied. Note that this information is not protected by the digital signature and so cannot be trusted to be accurate.
The structure of a Lock Signature Block is identical to that of a Signature Block." (p. 36)
"The process of onioning has three problems:
It is not possible to modify any of the Documents within a record. In particular it is not possible to:

- Add additional Documents. This may need to occur if the user omits a relevant Document from the record.
- Delete Documents. This may need to occur if a Document has been incorrectly incorporated in the record.
- Modify the metadata associated with a Document or Encoding. This may need to occur if a Document or Encoding has been incorrectly described.
- Add an Encoding to a Document. This may occur if a long-term preservation format is replaced by a new preservation format and all instances of the old format are migrated.
- Delete an Encoding from a Document. This may occur when a particular format can no longer be processed." (p. 22)

Reliability:

Other key terms:

Trust and integrity are key concepts that pertain to authenticity. Both are referred to in this advice. "VEO Metadata. The VEO Metadata consists of the VEO Format Description (M2) and Version (M3) elements. VEO Metadata is intended to introduce the VEO to a user who is reading the raw text of the VEO with no knowledge of VEOs or any VERS documentation. The scenario envisaged is that a programmer has been given a VEO, but no supporting documentation, and instructed to extract the record from it. The VEO Metadata occurs right at the beginning of the VEO and states the version, format and encoding of the object and identifies the documents where more information about can be found. The VEO Format Description (M2) is a text description of the format and encoding of the VEO, and the Version (M3) is the version of the PROS 99/007 Standard used. It should be noted that no trust can be placed in the information in either of these two elements as they are not protected by digital signature." (p. 11)

"This is a particularly useful approach as it exploits the strengths of the archive and avoids having to trust the integrity of an archive of certificates." (p. 35)

Annotator: Mary Beth Sullivan
Date of Annotation: August 25, 2005
Other Notes: "The structure and requirements of VERS are formally specified in the Standard for the Management of Electronic Records (PROS 99/007) and its five technical specifications. There are also six Advices that describe aspect of VERS. The relationship between the VERS Standard, the Specifications that support this Standard, and the Introduction and Advices that explain VERS is shown" in a table on the Victorian Electronic Records Strategy – Forever Digital web site. The standard and its five specifications are legal requirements. The six advices are not compulsory. (http://www.prov.vic.gov.au/vers/standard/version2.htm)

Bibliographic Information:
Author: Public Record Office Victoria
Title: Advice 13: VERS Long Term Preservation Formats
Journal or Book:
Editor(s): Hon. John Thwaites, MP, Minister for Victorian Communities
Publication Details: Victoria: State of Victoria Department for Victorian Communities, 2003
Page Numbers: 1-17
Web Source: Victorian Electronic Records Strategy – Forever Digital web site: http://www.prov.vic.gov.au/vers/standard/advice_13/default.htm (HTML file) and http://www.prov.vic.gov.au/vers/standard/pdf/99-7-4_Advice_ver_2-0.pdf (PDF)
Description: PDF and HTML files on the www
Subjects: Focus 3/Domain 2/ Terminology Cross-domain / Policy Cross-domain and Government - e-government - records management
Class Descriptor:

Abstract:
"Advice 13: VERS Long Term Preservation Formats" is the eleventh of twelve documents that compose the Victorian Electronic Records Strategy. All of the documents indicate how the Public Records Office Victoria is using the Victorian Electronic Records Strategy (VERS) to handle electronic records. VERS attempts to "archive electronic records into a long-term format that is not dependent on a particular computer system (hardware or software)." (http://www.prov.vic.gov.au/vers/standard/ver1/99-7s2.htm) This document explains the reasons particular file formats were chosen for VERS and imposes no additional mandatory requirements. This seventeen page document was published by the Public Record Office Victoria (PROV) (North Melbourne, State of Victoria, Australia) in 2003.

Annotation:
This advice is most useful for Domain 2, Focus 3 in its description of accuracy and file format, file copying and file conversion for long-term preservation purposes. "The Victorian Electronic

Records Strategy (VERS) addresses the cost-effective, long-term, preservation of electronic records. (http://www.prov.vic.gov.au/vers/standard/version2.htm).

Keywords:

Authenticity:

Accuracy:
"In the long-term it may be necessary to supersede a long-term preservation format. Typically this would occur if support for the original long-term preservation format was deemed to be too expensive and there was a suitable current format. Replacing a long-term preservation format requires a suitable conversion program. Such a conversion program is not simple, as it requires:

- monitoring to determine when the existing long-term preservation format is ceasing to be viable
- an evaluation, to determine an appropriate replacement format
- sourcing or writing of routines to perform the conversion
- identification of all instances of the superseded format in the collection
- conversion of all instances
- extensive testing to ensure that the conversion is accurate
- documentation of the conversion process." (p. 8-9)

"Accurate conversion means that the resulting file accurately reflects what the original creator of the record saw when they viewed the record. At a minimum the conversion should result in a file that contains the same information and appearance as if the record was printed from the originating application." (p. 9)

"Accurately rendering record content is a key advantage of PDF, for example, over XML representations of documents. PDF precisely and accurately describes each page in a document. XML, on the other hand, describes the logical structure of the document. While stylesheets make it possible to indicate the desired appearance of an XML document, it is not possible to guarantee accuracy of rendition, for two reasons:

- there is no requirement for browsers to accurately apply the style specified in a stylesheet.
- the appearance of the pages depends on the layout algorithms used by the browser.

Different algorithms, for example, could result in text being moved between pages." (p. 11)

"Independent implementations. Formats that have several independently written implementations are preferred over formats where there is only one implementation.
Independent implementations help ensure that vendors accurately implement the specification. It should be noted that significant 're-badging' occurs in the computer industry and this can make it difficult to determine how many independent implementations there actually are. In a given situation it may appear that there are several independent implementations, but, in given situation it may appear in fact, but, in fact, all the implementations may use the
same code licensed from the original developer." (p. 12)

"For many types of records there is no suitable format with a published specification. In this case, VERS recommends that an 'industry standard' format be selected. These formats need not be published.
The long-term preservation strategy is that records in an 'industry standard' format must be converted before the format becomes obsolete. This approach is more risky than adopting a format that has a published specification for two reasons:

- It is necessary to monitor the viability of the 'industry standard' format and to convert the records before the format becomes unviable. If the monitoring fails, and records are left in an industry standard format after this format ceases to be used, the records may be lost as it may not be possible to obtain software that will render the record.
- It is necessary to accept whatever conversion accuracy is produced by the available conversion utilities, as an archive cannot implement its own conversion utilities." (p. 12)

"Encryption, passwords, and copy protection are used to secure the contents of a file from unauthorised access.

- Encryption encrypts the contents of a file to prevent unauthorised access. Access is dependent on knowing the decryption key.
- Password protection is usually combined with encryption. The application will not open the file unless the correct password has been supplied.
- Copy protection uses a variety of mechanisms to prevent unauthorised copying. It is typically used to protect the rights of copyright holders." (p. 9-10)

Reliability:

Other key terms:

Annotator: Mary Beth Sullivan
Date of Annotation: August 25, 2005
Other Notes: "The structure and requirements of VERS are formally specified in the Standard for the Management of Electronic Records (PROS 99/007) and its five technical specifications. There are also six Advices that describe aspect of VERS. The relationship between the VERS Standard, the Specifications that support this Standard, and the Introduction and Advices that explain VERS is shown" in a table on the Victorian Electronic Records Strategy – Forever Digital web site. The standard and its five specifications are legal requirements. The six advices are not compulsory. (http://www.prov.vic.gov.au/vers/standard/version2.htm)

Bibliographic Information:
Author: Public Record Office Victoria
Title: Advice 14: Export of Electronic Records to PROV
Journal or Book:
Editor(s): Hon. John Thwaites, MP, Minister for Victorian Communities
Publication Details: Victoria: State of Victoria Department for Victorian Communities, 2003
Page Numbers: 1-22
Web Source: Victorian Electronic Records Strategy – Forever Digital web site:
http://www.prov.vic.gov.au/vers/standard/advice_14/default.htm (HTML file) and

http://www.prov.vic.gov.au/vers/standard/pdf/99-7-5_Advice_ver_2-0.pdf (PDF)
Description: PDF and HTML files on the www
Subjects: Focus 3/Domain 2/ Terminology Cross-domain / Policy Cross-domain and Government - e-government - records management
Class Descriptor:

Abstract:
"Advice 14: Export of Electronic Records to PROV" is the twelfth of twelve documents that compose the Victorian Electronic Records Strategy. All of the documents indicate how the Public Records Office Victoria is using the Victorian Electronic Records Strategy (VERS) to handle electronic records. VERS attempts to "archive electronic records into a long-term format that is not dependent on a particular computer system (hardware or software)." (http://www.prov.vic.gov.au/vers/standard/ver1/99-7s2.htm) This document explains how export of electronic records works under Specification 5 and imposes no additional mandatory requirements. This twenty-two page document was published by the Public Record Office Victoria (PROV) (North Melbourne, State of Victoria, Australia) in 2003.

Annotation:
This advice is relevant to Focus 3, Domain 2 because it explains how the Public Record Office Victoria handles the export of electronic records in an accurate manner.
"The Victorian Electronic Records Strategy (VERS) addresses the cost-effective, long-term, preservation of electronic records. (http://www.prov.vic.gov.au/vers/standard/version2.htm).

Keywords:

Authenticity:

Accuracy:
"The normal operation of this process is shown in the following diagram. The agency sends the VEO to PROV. After PROV has accepted responsibility for the contents of the VEO it sends an Acceptance back to the agency. The agency can then discard its copy of the VEO.
It is important to note that the acceptance message is an acceptance of responsibility. It is not just an acknowledgement of receipt." (p.8)

"If something goes wrong with the export, the operation of the protocol is shown in the following diagram. In this example, the acceptance message has been lost in the transfer back to the agency. Because the agency has not received the acceptance message within a specific period of time (known as a 'timeout'), it resends the VEO. PROV reprocesses the VEO and sends a new acceptance message. The timeout period is not defined in the Specification as it will depend on the processing time within PROV and on the mechanism used to transfer information between the agency and PROV. The re-transmission of the VEO may be triggered automatically or manually. This protocol has both benefits and costs. The major benefit is that the process is self-healing. In the event of an error in transferring the VEO, the system will recover. Failures that will be corrected include:

- The agency believing that they had sent the VEO when they had not.
- Loss of the VEO during the export to PROV.

- Loss of the VEO at PROV.
- PROV not transmitting the Acceptance.
- Loss of the Acceptance during its transmission to the agency.
- Loss of the Acceptance by the agency.
- However, the implications of this protocol are that:
- The agency must keep track of the VEOs that it has sent to PROV and resend them if no acceptance message is received within the specified period.
- The agency must mark VEOs that have been accepted so that they are not resent.
- PROV must be capable of accepting multiple copies of the same VEO without error and resending an acceptance message if it has received them before.
- The agency must implement the protocol." (p. 9)

"The external label is used to ensure the correct media is loaded onto a drive." (p. 10)

"Having correctly labelled tapes allows error checking, and also provides for multi-file volumes (allowing easy writing of multiple sets of data, possibly at different times) and provides for multi-volume files (allowing files larger than a volume to be handled on multiple tapes). Without the labelling control, this sort of capability would need to be handled with commands or scripts, which is not desirable, and is error-prone." (p. 10)

"It is important to realise that burning an 'error free' disc is not the end of the story. An apparently error-free disc almost certainly will contain errors, but these will be masked by the error correction added when the CD is burnt. The number of errors will depend on:

- the original quality of the disc. The quality of the disc varies dramatically between vendors, between vendor production facilities, and between production batches.
- interactions between the disc and the writer. Many factors can result in the CD writer producing a CD with a high error rate. For example, the laser in the CD loses power over time, which can result in less accurate CD burning. A more complex issue is the different types of dyes used in recordable CDs, which require different use of the laser.

This means, for example, that a CD writer optimised for one type of dye may do a poorer job with a disc that uses a different dye." (p. 12)

Reliability:

Other key terms:

Annotator: Mary Beth Sullivan
Date of Annotation: August 25, 2005
Other Notes: "The structure and requirements of VERS are formally specified in the Standard for the Management of Electronic Records (PROS 99/007) and its five technical specifications. There are also six Advices that describe aspect of VERS. The relationship between the VERS Standard, the Specifications that support this Standard, and the Introduction and Advices that explain VERS is shown" in a table on the Victorian Electronic Records Strategy – Forever Digital web site. The standard and its five specifications are legal requirements. The six advices are not compulsory. (http://www.prov.vic.gov.au/vers/standard/version2.htm)

Bibliographic Information:
Author: Uniform Law Conference of Canada Legislative Counsel
Title: Uniform Electronic Commerce Act
Journal or Book:
Editor(s):
Publication Details: Ottawa, ON: Uniform Law Conference of Canada, 1999
Page Numbers:
Web Source: Uniform Law Conference of Canada web site:
http://www.law.ualberta.ca/alri/ulc/current/euecafa.htm (archived with comments) and
http://www.ulcc.ca/en/us/index.cfm?sec=1&sub=1u1 (current, no comments)
Description: Word Perfect document and HTML file on WWW
Subjects: Focus 3/Domain 2/ Terminology Cross-domain / Policy Cross-domain and
Government - e-government - e-commerce
Class Descriptor:

Abstract:
The Uniform Law Conference of Canada Legislative Counsel drafted the Uniform Electronic Commerce Act as an application of the UNCITRAL Model Law on Electronic Commerce of 1996 in Canada. Divided into three parts, the act is concerned with the ability of government and private enterprise to make regulations for conducting business whether in electronic or paper format. The act synchronizes regulations for paper and electronic format. The act outlines rules for certain areas of communication. It also specifically deals with “carriage of goods”.

Annotation:
The act does not specifically deal with authenticity. Accuracy is mentioned as the absence of error, or in context of the actions taken to remedy an error after it has occurred. Instead, of the terms for consideration by Domain 2 Focus 3, reliability receives the most attention in the act, primarily in the sections dealing with e-signature. “The Uniform Electronic Commerce Act is designed to implement the principles of the UN Model Law in Canada. It applies, however, beyond the scope of "commerce", to almost any legal relationship that may require documentation. A list of exceptions appears in section 2. The commentary to each section explains the principles and, where necessary, the operation of the section. Further assistance may be sought in the UN Guide to Enactment of the Model Law, which is at the same World Wide Web address as the Model Law, noted above. The Uniform Act has three parts. The first part sets out the basic functional equivalence rules, and spells out that they apply when the people involved in a transaction have agreed, expressly or by implication, to use electronic documents. This avoids the need to amend all the many statutes that may state or imply a medium of communication. This part applies some special rules to governments. It has been widely considered, not just in Canada but in several other countries, that the general permission to use electronic communications may expose governments to an overwhelming variety of formats and media that they may not have the capacity to handle and that may not work for their particular purposes. Private sector entities can limit their exposure by contract; governments often deal with people with whom it has no contract. Part 1 therefore allows governments to set its own rules for incoming electronic documents. Outgoing documents would have to conform to the general standards of the Act, unless authorized to do otherwise by some other legislation. Part 2 of the Uniform Act sets out rules for particular kinds of communications, including the formation and operation of contracts, the effect of using automated

transactions, the correction of errors when dealing with a computer at the other end of the line, and deemed or presumed time and place of sending and receiving computer messages. Part 3 makes special provision for the carriage of goods, to permit electronic documents in a field that depends, on paper, on the use of unique documents, the creation of which is challenging electronically." (http://www.law.ualberta.ca/alri/ulc/current/euecafa.htm)

Keywords:

Authenticity:

Accuracy:
Accuracy can include the ability to review electronic information and correct information when errors occur as seen in Comment Part 2 Section 22. "This section supplements the general law of mistake where an electronic document is created or sent in error by a natural person to an electronic agent." (Comment Part 2 Section 22)

Reliability:
Reliability can apply to the relationship between electronic documents as much as it applies to the information within a record as seen in the definitions in Comment: Section 1. "The definition of "electronic signature" does not create a different legal meaning of signature in the electronic world… The electronic signature may be "associated with" the document, by mathematical logic or otherwise. The reliability of the association will affect the validity of the signature." (Comment: Section 1. The definitions in this section apply in this Act.)

This act calls for a reliability standard for e-signature as seen in Comment: Section 10. "…the association of the electronic signature with the relevant electronic document shall be reliable for the purpose for which the electronic document was made, in the light of all the circumstances, including any relevant agreement and the time the electronic signature was made." (Signatures Section 10 b)

"…where the authorities responsible for a signature requirement take the view that the requirement does imply some degree of reliability of identification or of association with the document to be signed, they may under subsection (2) make a regulation to impose a reliability standard… Signatures submitted to government must conform to information technology requirements and also to any rules about the method of making them or their reliability." (Comment: Section 10.)

Other key terms:

Section 11 "Provision of originals" seems to imply that original records are authentic.

Annotator: Mary Beth Sullivan
Date of Annotation: August 4, 2005
Other Notes: The Uniform Law Conference of Canada Legislative Counsel web site has moved. An archived version is maintained at the old URL at the University of Alberta and a new web site has been published under its own new domain name.

Bibliographic Information:
Author: United Kingdom Office of the e-Envoy
Title: e-Government Policy Framework: Electronic Records Management
Journal or Book:
Editor(s):
Publication Details: Kew, Richmond, Surrey, UK: Office of the e-Envoy, 2001
Page Numbers: 1-32
Web Source: Office of the e-Envoy document archives on the GovTalk web site:
http://www.govtalk.gov.uk/documents/ERM%5Fversion2%2Epdf
Description: PDF and Word document on WWW
Subjects: Focus 3/Domain 2/ Terminology Cross-domain / Policy Cross-domain and Government - e-government - records management
Class Descriptor:

Abstract:
"e-Government Policy Framework: Electronic Records Management" calls for systematic electronic records management for existing electronic records with evidential value. It outlines a plan for the execution of the 2004 deadline for "Modernising Government" for all new electronic records. This thirty-two page document was published by the Office of the e-Envoy (Kew, Richmond, Surrey, United Kingdom) in 2001.

Annotation:
This document is an outline of an electronic records management plan for government in the United Kingdom. It applies to Domain 2 Focus 3, in the discussion of the ways in which authentic records are valuable and the means with which the government can maintain them as authentic records. The document also conveys the message that well run and well-documented record keeping systems are essential to accuracy and reliability. "The framework for electronic records management:

- provides background guidance to assist with the inclusion of electronic document and records management considerations in departmental e-business strategies
- provides a framework and a set of milestones for departments and agencies to move towards full electronic records management by gaining formal control of existing electronic records that have value as evidence; and to plan for the implementation of electronic records management systems that will meet the Modernising Government target – that by 2004 all newly created public records will be electronically stored and retrieved
- encourages the adoption of cross-government standards for metadata and interoperability to support greater commonality and inter-departmental working in electronic document and records management, and in the sharing and exchange of electronic records between government systems." (p. 6)

Keywords:

Authenticity:
Authentic electronic government records permit government to make decisions based on the evidence contained in the records. Authenticity makes electronic records legally admissible. (p.

8) “Effective electronic records management (ERM) supports… evidence-based policy making by providing reliable and authentic information for the evaluation of past actions and decisions… (and) various specialised legislation by demonstrating the authenticity of records and supporting legal admissibility.” (p. 8)

Authenticity will depend on having appropriate measures in place to maintain authentic records. This may include the need to coordinate paper and electronic record keeping. (p. 9) “Government organisations will need to develop infrastructure for ERM in three ways… by implementing electronic systems for the management of electronic documents and records within government organisations, so that these can be accessed, maintained and retrieved in a manner which retains authenticity and integrity; and by harmonizing electronic with residual paper-based record-keeping systems.” (p. 9)

It is necessary to keep the evidence of authenticity with the records being authenticated. (p. 13) “Electronic documents generated within a government organisation, which have been electronically signed and authenticated, will also need to be retained with evidence of their authenticity.” (p. 13)

Authenticity is maintained when records are tracked within the record keeping system. (p. 13) “Where a secure electronic records management system is in place, the record-keeping system itself will provide evidence of continued authenticity for records which it contains (since that is its function) and a simple level of metadata on the facts of authentication may be sufficient. In these circumstances, procedures should be defined to control the space between the point of transaction at which the document is authenticated, and entry of the record into a secure record-keeping system.” (p. 13)

Common metadata will contribute to demonstrating continued authenticity. (p. 19) “Joint working and integrated systems will require government organisations to share and exchange electronic records and documents. Export and import between records management systems will be much simplified by a common metadata structure and a common vocabulary – by using standard ways of categorising descriptive elements and standard term for their description. This will also be important for the longer-term migration of electronic documents to new hardware/software platforms. In addition, common metadata standards on issues such as authentication – what information to keep with records of authenticated transactions, for example, in order to demonstrate continued authenticity over time – will improve reliability and accountability.” (p. 19)

Accuracy:
Accuracy is important in the access and retrieval of records. (p. 30) “Record access facilities must be able to… enable the correct display and printing of all records at all times” (p. 30)

Reliability:
Proper record keeping cares for reliable records and secures their reliability. (p. 10) “Good electronic record-keeping requires…electronic record-keeping systems that are designed to manage reliable and authentic records, ensuring that the integrity and reliability of electronic records is secured…” (p. 10)

Other key terms:

Annotator: Mary Beth Sullivan
Date of Annotation: July 29, 2004
Other Notes: "How can I access historical or old Office of the e-Envoy publications? Publications issued by the Office of the e-Envoy (1999-2004) have now been archived and are available on request by email" (from the e_government web site FAQ page: http://www.cabinetoffice.gov.uk/e-government/frequently_asked_questions)

Bibliographic Information:
Author: United States Department of Health and Human Services, Food and Drug Administration
Title: Part II Department of Health and Human Services, Food and Drug Administration 21 CFR Part 11 Electronic Records; Electronic Signatures; Final Rule Electronic Submissions; Establishment of Public Docket; Notice
Journal or Book: Federal Register: March 20, 1997 (Volume 62, Number 54)
Editor(s):
Publication Details: Washington D.C.: United States Food and Drug Administration, 1997
Page Numbers: 13430-13466 (Federal Register pagination), 1-38 (PDF)
Web Source: U. S. Food and Drug Administration Office of Regulatory Affairs web site: http://www.fda.gov/ora/compliance_ref/part11/frs/background/11cfr-fr.htm (HTML file) and http://www.fda.gov/ora/compliance_ref/part11/FRs/background/pt11finr.pdf (PDF)
Description: PDF file and HTML document on the www
Subjects: Focus 3/Domain 2/ Terminology Cross-domain / Policy Cross-domain and Government - e-government - electronic records - electronic signatures
Class Descriptor:

Abstract:
This issue of the Federal Register deals with "Part II Department of Health and Human Services, Food and Drug Administration 21 CFR Part 11 Electronic Records; Electronic Signatures; Final Rule Electronic Submissions; Establishment of Public Docket; Notice." It provides background on the final rule for Title 21 Part 11. This thirty-six page document explores the FDA's regulation of electronic records, their submission to the agency, and the use of electronic signatures. The document summarizes the proposed rule and the comments offered on it. The agency also publishes and explains the final rule.

Annotation:
"The Food and Drug Administration (FDA) is issuing regulations that provide criteria for acceptance by FDA, under certain circumstances, of electronic records, electronic signatures, and handwritten signatures executed to electronic records as equivalent to paper records and handwritten signatures executed on paper. These regulations, which apply to all FDA program areas, are intended to permit the widest possible use of electronic technology, compatible with FDA's responsibility to promote and protect public health. The use of electronic records as well as their submission to FDA is voluntary. Elsewhere in this issue of the Federal Register, FDA is publishing a document providing information concerning submissions that the agency is prepared to accept electronically." (p. 13430)

Keywords:

Authenticity:
Controls for open and closed systems, encryption, and digital signatures ensure authenticity. (p. 13430-13431, 13451, 13465-13466) “Section 11.30 sets forth controls for open systems, including the controls required for closed systems in § 11.10 and additional measures such as document encryption and use of appropriate digital signature standards to ensure record authenticity, integrity, and confidentiality.” (p. 13430-13431)

Comments on this rule cited a need for regulation or guidance to ensure that records are maintained in a manner to retain authenticity. (p. 13431-13432) “B. Regulations Versus Guidelines 2. Several comments addressed whether the agency’s policy on electronic signatures and electronic records should be issued as a regulation or recommended in a guideline. Most comments supported a regulation, citing the need for a practical and workable approach for criteria to ensure that records can be stored in electronic form and are reliable, trustworthy, secure, accurate, confidential, and authentic. One comment specifically supported a single regulation covering all FDA regulated products to ensure consistent requirements across all product lines. Two comments asserted that the agency should only issue guidelines or ‘‘make the regulations voluntary.’’ One of these comments said that by issuing regulations, the agency is shifting from creating tools to enhance communication (technological quality) to creating tools for enforcement (compliance quality). The agency remains convinced, as expressed in the preamble to the proposed rule (59 FR 45160 at 45165), that a policy statement, inspection guide, or other guidance would be an inappropriate means for enunciating a comprehensive policy on electronic signatures and records. FDA has concluded that regulations are necessary to establish uniform, enforceable, baseline standards for accepting electronic signatures and records. The agency believes, however, that supplemental guidance documents would be useful to address controls in greater detail than would be appropriate for regulations.” (p. 13431-13432)

There is debate about how technological flexibility can enhance or diminish authenticity. (p. 13431-13432) “3. Several comments addressed the flexibility and specificity of the proposed rule. The comments contended that agency acceptance of electronic records systems should not be based on any particular technology, but rather on the adequacy of the system controls under which they are created and managed. Some comments claimed that the proposed rule was overly prescriptive and that it should not specify the mechanisms to be used, but rather only require owners/users to design appropriate safeguards and validate them to reasonably ensure electronic signature integrity and authenticity. One comment commended the agency for giving industry the freedom to choose from a variety of electronic signature technologies, while another urged that the final rule be more specific in detailing software requirements for electronic records and electronic notebooks in research and testing laboratories.” (p. 13432)

FDA uses the term ‘‘transmitted’’ because it does not believe authenticity depends on receipt of a record. (p. 13437) “24. One comment suggested that, in describing what electronic records are within the scope of part 11, proposed § 11.1(b) should be revised by substituting ‘‘processed’’ for ‘‘modified’’ and ‘‘communicated’’ for ‘‘transmitted’’ because ‘‘communicated’’ reflects the fact that the information was dispatched and also received. The comment also suggested substituting ‘‘retained’’ for ‘‘maintained,’’ or adding the word ‘‘retained,’’ because ‘‘maintain’’ does not necessarily convey the retention requirement. The agency disagrees. The word ‘‘modified’’ better describes the agency’s intent regarding changes to a record; the word ‘‘processed’’ does not necessarily infer a change to a record. FDA believes ‘‘transmitted’’ is preferable to ‘‘communicated’’ because ‘‘communicated’’ might infer that controls to ensure integrity and authenticity hinge on whether the intended recipient actually received the record. Also, as discussed in comment 22 of this document, the agency intends for the term ‘‘maintain’’ to include records retention.” (p. 13437)

Comparison of electronic and handwritten signatures has been suggested as a method of measuring authenticity. (p. 13442) “51. One comment suggested that where handwritten signatures are captured by devices, there should be a register of manually written signatures to enable comparison for authenticity and the register also include the typed names of individuals.” (p. 13442)

Signed records in a closed system must maintain their authenticity and be able to prove that they are genuine.(p. 13443, 13452) “VII. Electronic Records—Controls for Closed Systems (§ 11.10) The introductory paragraph of proposed § 11.10 states that: Closed systems used to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine.” (p. 13443)

Authority checks help to maintain authenticity. (p. 13448) “82. Proposed § 11.10(g) states that procedures and controls for closed systems must include the use of authority checks to ensure that only authorized individuals use the system, electronically sign a record, access the operation or device, alter a record, or perform the operation at hand… The agency advises that authority checks, and other controls under § 11.10, are intended to ensure the authenticity, integrity, and confidentiality of electronic records, and to ensure that signers cannot readily repudiate a signed record as not genuine.” (p. 13448)

Device checks can help verify that records are authentic. (p. 13449) “Device checks would be necessary under PDMA when the source of commands or data is relevant to establishing authenticity, such as when licensed practitioners order drug samples directly from the manufacturer or authorized distributor without the intermediary of a sales representative. Device checks may also be useful to firms in documenting and identifying which sales representatives are transmitting drug sample requests from licensed practitioners.” (p. 13449)

Digital signatures may help to ensure authenticity under this rule but they are not required. (p. 13451) “VIII. Electronic Records—Controls for Open Systems (§ 11.30) Proposed § 11.30 states that: ‘‘Open systems used to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity and confidentiality of electronic records from the point of their creation to the point of their receipt.’’ In addition, § 11.30 states: * * * Such procedures and controls shall include those identified in § 11.10, as appropriate, and such additional measures as document encryption and use of established digital signature standards acceptable to the agency, to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.” (p. 13451)

“The agency advises that § 11.30 requires additional controls, beyond those identified in § 11.10, as needed under the circumstances, to ensure record authenticity, integrity, and confidentiality for open systems. Use of digital signatures is one measure that may be used, but is not specifically required. The agency wants to ensure that the digital signature standard used is, in fact, appropriate. Development of digital signature standards is a complex undertaking, one FDA does not expect to be performed by individual firms on an ad hoc basis, and one FDA does not now seek to perform.” (p. 13451)

Additional methods to ensure authenticity are dependent upon the situation. (p. 13452) “As discussed in comment 94 of this document, use of digital signatures and encryption would be an option when extra measures are necessary under the circumstances. In the case of PDMA records, such measures may be warranted in certain circumstances, and unnecessary in others. For example, if electronic records were to be transmitted by a firm’s representative by way of a public online service to a central location, additional measures would be necessary. On the other hand, where the representative’s records are hand delivered to that location, or transferred by direct connection between the representative and the central location, such additional measures to ensure record authenticity, confidentiality, and integrity may not be necessary. The agency does not believe that it is practical to revise § 11.30 to elaborate on every possible situation in which additional measures would or would not be needed.” (p. 13452)

“The agency advises that the concept of nonrepudiation is part of record authenticity and integrity, as already covered by § 11.10(c).” (p. 13452)

FDA agrees that certification of electronic signature systems may not enhance authenticity. (p. 13456) “119. Proposed § 11.100(c) states that persons using electronic signatures must certify to the agency that their electronic signature system guarantees the authenticity, validity, and binding nature of any electronic signature. Persons utilizing electronic signatures would, upon agency request, provide additional certification or testimony that a specific electronic signature is authentic, valid, and binding. Such certification would be submitted to the FDA district office in which territory the electronic signature system is in use. Many comments objected to the proposed requirement that persons provide FDA with certification regarding their electronic signature systems. The comments asserted that the requirement was: (1) unprecedented, (2) unrealistic, (3) unnecessary, (4) contradictory to the principles and intent of system validation, (5) too burdensome for FDA to manage logistically, (6) apparently intended only to simplify FDA litigation, (7) impossible to meet regarding ‘‘guarantees’’ of authenticity, and (8) an apparent substitute for FDA inspections. FDA agrees in part with these comments.” (p. 13456)

“Subpart B—Electronic Records § 11.10 Controls for closed systems. Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records. (b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records. (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period. (d) Limiting system access to authorized individuals. (e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying. (f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate. (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. (h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction. (i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks. (j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification. (k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation." (p. 13465)

"§ 11.30 Controls for open systems. Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in § 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality." (p. 13465-13466)

Accuracy:
Accurate performance in a validated system, accurate copies of records and accurate record retrieval are all parts of accuracy. (p. 13465) This seems to indicate that accuracy in a record keeping system helps to ensure that records are authentic.

Reliability:

Other key terms:

Annotator: Mary Beth Sullivan
Date of Annotation: August 26, 2005
Other Notes: Guidances for 21 CFR Part 11 have been updated since this document was reviewed by InterPARES in 2004. I recommend reading the new draft drafts for more complete information. See (http://www.fda.gov/ora/compliance_ref/part11/default.htm) for the updates. Note that PDMA refers to the Prescription Drug Marketing Act Report to Congress of June 2001.

Bibliographic Information:
Author: United States General Accounting Office
Title: Information Management: Challenges in Managing and Preserving Electronic Records
Journal or Book:
Editor(s):
Publication Details: Washington D.C.: United States General Accounting Office, 2002
Page Numbers: 1-77 (numbered pages in report), 1-83 (total pages in PDF)
Web Source: Government Accountability Office web site:
http://www.gao.gov/new.items/d02586.pdf
Description: PDF file on the www
Subjects: Focus 3/Domain 2/ Terminology Cross-domain / Policy Cross-domain and Government - e-government - records management
Class Descriptor:

Abstract:
"Information Management: Challenges in Managing and Preserving Electronic Records" is a report to addressed to congressional requesters on June 12, 2002. This seventy-seven page report examines electronic records generated by the federal government. The General Accounting Office was asked to prepare this report to assess the ability of the National Archives and Records Administration to handle these records. Different methods of handling the records are compared. Current research projects into electronic recordkeeping are also reviewed. The GAO asked the National Archivist to review of draft of its findings and includes some of the archivist's comments. GAO makes independent recommendations for further action to be taken.

Annotation:
"Why GAO Did This Study - In the wake of the transition from paper-based to electronic processes, federal agencies are producing vast and rapidly growing volumes of electronic records. The difficulties of managing, preserving, and providing access to these records represent challenges for the National Archives and Records Administration (NARA) as the nation's recordkeeper and archivist. GAO was requested to (1) determine the status and adequacy of NARA's response to these challenges and (2) review NARA's efforts to acquire an advanced electronic records archiving system, which will be based on new technologies that are still the subject of research." (Highlights of GAO-02-586, a report to Congressional Requesters, un-numbered page) "GAO recommends that the Archivist of the United States develop documented strategies to raise awareness of the importance of records management programs and for conducting systematic inspections of these programs. In addition, to reduce risks, GAO recommends that the Archivist reassess the schedule for acquiring the new archival system so that the agency can complete key planning tasks and address IT management weaknesses." (Highlights of GAO-02-586, a report to Congressional Requesters, un-numbered page) "NARA is not alone in facing the challenges posed by electronic records, particularly long-term preservation. There is a general consensus in the archival community that a viable strategy for the long-term preservation and archiving of electronic records has yet to be developed. Accordingly, archives scholars, national archival and library institutions, and private industry representatives are collaborating on major initiatives to develop the theoretical and methodological knowledge needed for the permanent preservation of records created in electronic systems." (p. 12-13)

Keywords:

Authenticity:
This passage indicates that eliminating changes to data reduces concerns about authenticity. Persistent object preservation or POP will not change the data in electronic records, therefore it helps to maintain authenticity. (p. 54) "According to NARA, persistent object preservation would accommodate preservation of persistent but evolving collections by providing the ability to dynamically reconstruct data collections on new technology. The result would be a system that could upgrade individual technical components and migrate media while safeguarding the archived records. POP would thus not only enable the use of future, advanced technologies, it would also reduce threats to integrity and authenticity, because POP would not require changes in the preserved data. However, POP may not be sufficiently mature to be translated into system design." (p. 54)

Electronic record keeping is handled differently by the private and public sectors. Authenticity requirements are more stringent for government and academic records. (p. 56) "While government and academic institutions are searching for a permanent solution to electronic records archiving problems, the private sector, also concerned about and affected by the potential loss of electronic records, relies on existing information architectures and off-the-shelf technologies to make accessible massive volumes of electronic records dating back over two decades. These archiving achievements do not meet the rigorous requirements for permanence and authenticity that are demanded by a government archive, nor are their owners required to process, store, and access the full range of complex file formats encountered by governments. However, they do illustrate the capability to provide storage and access to large quantities of data. Two of the most notable private sector efforts are the Internet Archives and the Google archive of Usenet messages." (p. 56)

The Veterans Administration is looking for guidance and standards for electronic signatures used in federal agencies to ensure authenticity. (p. 72) "VA patient enrollment records present another instance of the confusion regarding scheduling requirements for electronic records and for records in multiple versions. Although VA is working toward a completely electronic process, enrollment records are initiated on paper because of current legal requirements for ink signatures. In general, however, VA does not schedule electronic records when it has scheduled the paper version. It is NARA
policy, however, that electronic records must also be scheduled. According to VA, another key challenge that it faces is ensuring the validity and authenticity of electronic records, and it would like to see adequate guidance and standards about electronic signatures from NARA so that all government agencies are using the same approach." (p. 72)

Accuracy:

Reliability:
This passage seems to indicate that records must be reliable from creation in order to meet the responsibilities of the federal government. (p. 17) "Agencies must create reliable records that meet the business needs and legal responsibilities of federal programs and (to the extent known) the needs of internal and external stakeholders who may make secondary use of the records." (p. 17)

"…the Secretariat Tracking and Retrieval System (STARS) tracks approximately 440,000 digital images of foreign policy memoranda and correspondence of the Secretary of State from 1986 to the present. Both STARS and SAS must not only preserve the records, but also maintain reliable and rapid access to the image data. As technologies change, preserving and providing access to the records present complex electronic records management challenges. The State Department's records management office has sole responsibility for maintaining SAS, and it has had to proceed with the long-term management and preservation of the system records—periodically updating and migrating all the images to reflect new technologies—without guidance from NARA. NARA guidance does not address updating or migration of file formats." (p. 68-69)

Other key terms:

Evidence seems to relate to authenticity and accuracy. "NARA's mission is to ensure "ready access to essential evidence" for the public, the President, the Congress, and the Courts. NARA's responsibilities stem from the Federal Records Act, which requires each federal agency to make and preserve records that (1) document the organization, functions, policies, decisions, procedures, and essential transactions of the agency and (2) provide the information necessary to protect the legal and financial rights of the government and of persons directly affected by the agency's activities.
… NARA is responsible for oversight of records management and archiving. Records management—that is, the policies, procedures, guidance, tools and techniques, resources, and training needed to design and maintain reliable and trustworthy records systems—governs the life cycle of records from creation, through maintenance and use, to final disposition." (p. 8)

Copyright may be in conflict with integrity and authenticity. "Even if the software and hardware are obsolete, their copyrighted specifications are not likely to be released for the benefit of archival integrity." (p. 46)

Migration may not ensure authenticity and integrity. "As a strategy for the long-term preservation of electronic records, relying on format migration is risky. Migration as a preservation strategy would have to be a continuous process, with conversions occurring whenever a new format needed to be introduced. With each format conversion, the possibility of loss would be increased, and the more complex the record, the more the possibility of loss. Thus, migration is at best an imperfect solution as it can potentially lead to the loss of record integrity. Migration was selected by the United Kingdom's Public Record Office as its current archival approach. In addition to migration, the Public Records Office is also considering using emulators and viewers to access archived files in their native formats." (p. 49)

Encapsulation may not threaten integrity and authenticity because the file format is not changed. "Unlike migration, encapsulation does not necessarily involve a change in the original file format. If the format is unchanged, encapsulation would avoid the problem of loss of integrity that migration entails." (p. 49)

Annotator: Mary Beth Sullivan
Date of Annotation: August 26, 2005
Other Notes: "GAO's commitment to good government is reflected in its core values of

accountability, integrity, and reliability." (PDF p. 82) A volume of records can overwhelm an archival repository. GAO seems to indicate that the authenticity, accuracy, and reliability of NASA's records would be jeopardized NARA received them and was not prepared to deal with them. It seems they are indicating policy must precede custody of records: "Presently, NASA's National Space Science Data Center archives over 20 terabytes of digital space science data from past and present NASA missions, of which 3 terabytes are currently electronically accessible. In addition, the Hubble Space Telescope has created a data archive of over 7 terabytes of images of our solar system, and continues to archive an additional 3 to 5 gigabytes every day. Archiving and ensuring data integrity of all these electronic records require periodic data renewal cycles, involving migration from old to new media, resource intensive data reorganization and reformatting, or even recreation of related software. Because these records are of permanent value and NARA has no means to archive them in any useful way, NASA retains custody of them. They accordingly fall into an undefined category: they are permanent records that NARA cannot archive. The current arrangement by which they are maintained is not covered by NARA guidance. Nor is NASA's archiving approach covered by this guidance, which does not cover migration and archival formats (other than flat ASCII files on tape), management of digital images, or maintenance of electronic records in databases for extended periods of time." (p. 66)