

Authentic Digital Records: Laying the Foundation for Evidence

A foundation for proving that records submitted as evidence are reliable, usable, and have integrity is built with policies and procedures based on standards and best practices – and documentation that shows they have been followed.

Stephen Mason

Editor's Note: This article is based on this author's research project commissioned by the ARMA International Educational Foundation (AIEF) in 2006, *Proof of the Authenticity of a Document in Electronic Format Introduced as Evidence*. The full report may be downloaded free from the AIEF website at www.armaedfoundation.org.

Proving the authenticity of records is of great concern to information and records managers. While this concern initially involved the integrity of paper-based records, today it extends to include records in digital format. Following are the factors to be taken into account when laying the evidential foundations for submitting evidence in digital format into court in the United States.

Legal Foundation for Authenticating Digital Documents

Rule 901 of the U.S. Federal Rules of Evidence, which governs the authentication of evidence, says that the requirement of authentication is "satisfied by evidence sufficient to support a finding that the matter in question is

what its proponent claims."

The type of evidence available to a court to determine the authenticity of a digital document will comprise a mix of technical attributes and organizational matters. The 2005 case of *In re Vee Vinhnee, debtor, American Express Travel Related Services Company Inc. v. Vee Vinhnee* illustrates the nature of the evidence required.

In this case, American Express claimed Vinhnee failed to pay credit card debts and took action to recover the money. After a trial that occurred in the absence of the defendant, the trial judge determined that American Express failed to authenticate certain records in digital format. American

Express appealed the verdict, and the decision of the trial judge was affirmed.

In respect of the issues in this particular trial, Judge Christopher Klein pointed out that:

"...the focus is not on the circumstances of the creation of the record, but rather on the circumstances of the preservation of the record during the time it is in the file so as to assure that the document being proffered is the same as the document that originally was created."

In essence, the judge made the pertinent point that the issue is "that the record is what it purports to be." The judge continued to explain the issues involved in this process:

"The logical questions extend beyond the identification of the particular computer equipment and programs used. The entity's policies and procedures for the use of the equipment, database, and programs are important. How access to the pertinent database is controlled and, separately, how access to the specific program is controlled are important questions. How changes in the

At the Core

This article

- ▶ Describes six factors in authenticating digital evidence
- ▶ Discusses issues in laying the evidential foundation for records
- ▶ Provides practical advice for building a strong foundation for submitting digital evidence in U.S. courts



100111010
010011001110
11101001100101
001100111010100
0101001100111 010
0111101001100101
1001100111010100
1010100110011110
0111101001100101
0100110011110
01001100

database are logged or recorded, as well as the structure and implementation of backup systems and audit procedures for assuring the continuing integrity of the database, are pertinent to the question of whether records have been changed since their creation.

“There is little mystery to this. All of these questions are recognizable as analogous to similar questions that may be asked regarding paper files: policy and procedure for access and for making corrections, as well as the risk of tampering. But the increasing complexity of ever-developing computer technology necessitates more precise focus.”

Klein reached the conclusion that early attempts at establishing a foundation for electronic evidence were too cursory, while also accepting that judicial notice is commonly taken of the validity of the theory underlying the use of computers and the validity of the data generated generally. The judge then set out the tests described by Edward J. Imwinkelried in *Evidentiary Foundations* in respect to considering electronic records as a form of scientific evidence:

1. The business uses a computer.
2. The computer is reliable.
3. The business has developed a procedure for inserting data into the computer.
4. The procedure has built-in safeguards to ensure accuracy and identify errors.
5. The business keeps the computer in a good state of repair.
6. The witness had the computer readout certain data.
7. The witness used the proper procedures to obtain the readout.
8. The computer was in working order at the time the witness obtained the readout.
9. The witness recognizes the exhibit as the readout.

10. The witness explains how he or she recognizes the readout.
11. If the readout contains strange symbols or terms, the witness explains the meaning of the symbols or terms for the trier of fact.

The judge amplified the fourth test:

Several methods are used to preserve electronic data, including technology preservation, technology emulation, and data refreshing. Risks attach to whichever method is used, and it is important to ensure that whatever method is employed can be defended ...



“The ‘built-in safeguards to ensure accuracy and identify errors’ in the fourth step subsume details regarding computer policy and system control procedures, including control of access to the database, control of access to the program, recording and logging of changes, backup practices, and audit procedures to assure the continuing integrity of the records.”

The members of the court proceeded to evaluate the exhibits submitted by American Express using the tests set out by Imwinkelried. It was made clear that the evidence of the custodian of the records at American Express was far too vague to be accepted. The following problems were identified:

- Generally, the evidence was vague and unpersuasive.
- The custodian did not have the requisite knowledge to provide the evidence.
- The person providing evidence on behalf of American Express merely asserted that he was an employee of American Express and was personally familiar with the systems, both hardware and software. He failed to inform the court of his job title or of his relevant experience and training that would provide an element of authority to his evidence.
- American Express failed to provide information about its computer policy and system control procedures, control of access to the relevant databases, control of access to the applicable programs, how changes to the data were recorded or logged, what backup practices were in place, and whether there were any audit procedures used to provide assurance of the continuing integrity of the records.

Although it will not be necessary to provide such an in-depth analysis of digital records in every case brought before a court, Klein’s comments help illustrate the nature of the evidence that should be gathered if it is necessary to adduce such evidence.

Six Factors in Authenticating Digital Evidence

The following factors are keys to proving the authenticity of digital records:

1. *Method of preservation* – Several methods are used to preserve electronic data, including technology preservation, technology emulation, and data refreshing. Risks attach to whichever method is used, and it is important to ensure that whatever method is employed can be defended should the digital document be the subject of a legal challenge as to its authenticity.
2. *Identity* – The identity of the document will need to be established, such as the name of the purported author, the date it was created, the place of origin, and the subject matter. It can be argued that this information forms part of the reliability of the document, meaning if it can be identified correctly, and there is a degree of certainty about the document that could be relied upon.
3. *Integrity* – As discussed in the UK National Archives' *Generic Requirements for Sustaining Electronic Information over Time: 1 Defining the Characteristics for Authentic Records*, integrity is considered to refer to the "wholeness and soundness" of the document. This, in turn, is related to whether the document can be considered to be complete and uncorrupted "... in all its essential respects during the course of its existence." *ISO 15489: 2001 Information and Documentation – Records Management – Part 1 – General* provides that integrity refers to the record being complete and unaltered. While these definitions of integrity might relate to the ability to verify that the content of a document has not been changed since it was written, finished, and adopted by the author, it might be necessary to consider other matters, including, but not limited to:
 - Whether a time stamp was used, and, if it was, whether it can be

considered to be accurate, and, if in doubt, what standards were observed with the particular type of time stamp used

- Whether it is a partially written document

Where policies and procedures are followed, a degree of trust is created that reinforces the probability that a document can be trusted. However, the assumption of integrity cannot be sustained where the procedures are tested in a court and found wanting.



- Whether the test for integrity of the document should apply only to the original version or whether any tracking regarding the document's subsequent circulation is necessary. Following from this, the integrity of the circulation metadata may be required.
- Whether the metadata can be accepted as reliable and meaningful

The concept of integrity will be closely related to the organization's control over the preservation of a document, which is discussed in more detail below. Underlying the integrity of a document will be the use of digital signatures to provide evidence of verification that the document has not been altered.

4. *Usability* – The term usability is meant to cover the practical issues relating to retrieving, presenting, and interpreting the data correctly.
5. *Attributes of storage* – A range of issues arise from this perspective, mainly, but not exclusively, around technical obsolescence, which affects:
 - The media upon which data is stored
 - The application software used to create, process, and display data is replaced frequently, and some types of system software and middleware that are required by an application in order to work also change. This issue will affect older digital documents that were generated using software and machines that no longer exist. To be read, the text will require the use of different tools. The next question will be whether the application of a different tool affects a digital document in some way.
 - As discussed by Stefanie Fischer-Dieskau and Daniel Wilke in their *Digital Evidence Journal* article, the architecture of hardware changes because machines are

replaced, which means some types of software will no longer be available, supported, or maintained. In this respect, digital signature systems may be a problem. The digital signature software may still be available, but the digital signature might have been applied using a version of the software compatible with Windows 98, but not Windows XP, or the signature software tool may have been overtaken by something better. So the question then has to be asked whether the digital signature ought to be migrated, for instance, by using a further digital signature to provide for the integrity of the version that is migrated.

6. *Procedural controls* – Where policies and procedures are followed, a degree of trust is created that reinforces the probability that a document can be trusted. However, the assumption of integrity cannot be sustained where the procedures are tested in a court and found wanting. This is why the following are relevant:

- The controls in place to prevent modifying or editing the record
- Evidence of the controls to support the document is authenticated by the production of credible metadata, audit trails, and relevant reports
- The procedures in place to assess and maintain the authenticity of the document over the period of time it has been preserved
- Evidence is available to demonstrate policies were properly created, and that procedures were subsequently adopted and followed to ensure the policies were correctly implemented

Laying the Evidential Foundation

The tests proffered by Imwinkelried offer a useful starting point for the

introduction of evidence in digital format, particularly in circumstances where a party is required to lay the evidential foundations of the evidence. As the *Vinhnee* case illustrates, a number of steps may be required if the authenticity of a digital document is in ques-

Even if the actual process is not accepted in the future, it is probable, providing the process has been scrupulously well documented, that it will more readily withstand scrutiny in a court.



tion. A range of associated issues may have to be covered, including:

The form of the record:

- Whether it is provided to the court in native format – if so, whether the document has been altered
- Whether it is a scanned paper document – if so, it may be necessary to demonstrate that the process of scanning was such that the scanned document is a true replica of the original document, and there was no possibility of the document having been altered between its original receipt as a paper document and its being added to the database in electronic format
- Whether it has been re-published in digital format, such as PDF, and whether the document in question has been migrated between formats – evidentiary foundations will be required to demonstrate the efficacy of the process and what, if any, data was lost in the process

The machine that was used to retrieve the document:

- Whether the machine was the original used or a more modern machine. If it was a modern machine, was any data associated with the document lost in the process when retrieving the document?
- The type of operating and application software used when the document was first created – whether subsequent changes to both the operating and application software have altered the underlying integrity of the document in any way
- Whether the storage medium, and any migration between storage media, have altered the document
- Whether the method of retrieval has affected the document
- Whether it is possible to detect alterations to the document

In essence, the characteristics of authentication comprise three things:

1. *Reliability* – there is evidence that records are created and captured as part of the legitimate business process, and they are subject to a corporate management process
2. *Integrity* – the document is protected from unauthorized alteration
3. *Usability* – the document is capable of being retrieved, presented, and interpreted correctly

These characteristics, taken together, lay the foundations for the authenticity of a document in digital format. However, it must be emphasized that the rigor of the process will depend on the nature of the document. Admitting a statement of account as part of a business process may well be an easier exercise than, for instance, a scanned copy of a will.

Practical Advice for Building a Solid Foundation

Although documents in digital format present a particular set of unique problems for their long-term conservation, a number of very helpful initiatives have already provided a substantial amount of information and advice on this topic. From the point of view of the records manager, the most difficult question remains: how to preserve digital records? Unfortunately, the answer to this question is somewhat of a moving target because of the nature of the technology that determines the answer.

Let Standards and Best Practices Be the Guide

Perfection is impossible, and preserving digital records is no different. But start by using accepted standards and best practices – and document everything that is done to preserve data. It will be for lawyers to argue and the adjudicator to determine later – should the admissibility or authenticity of the electronic evidence become an issue – that the data was secured by adhering to the best practice that was generally accepted at the time it was preserved.

Document Policies and Procedures

Even if the actual process is not accepted in the future, it is probable, providing the process has been scrupulously well documented, that it will more readily withstand scrutiny in a court.

By following the guidance offered by national and international organizations on this topic, the records manager or archivist can offer evidence that they undertook their duties to the best standards available at the time the data was preserved.

Develop and Document Decision-making Criteria

It is necessary to ensure that criteria is agreed and documented when making decisions relating to digital documents, and appraisal methodologies for approaching digital records should be developed and maintained. Failure to have criteria in place and to implement decisions in relation to the criteria, will undermine the authenticity of the evidence. Where the evidence is in dispute, these factors will be the subject of exten-

sive cross-examination. Where it can be demonstrated that there was no or little criteria, and the documentation relating to the criteria either does not exist or is poorly documented, such lacunae will completely undermine the value of the evidence, and may well prevent it from being adduced into the proceedings, as in the *Vinhnee* case.

Turn Rhetoric into Reality

Regardless of whether information and records managers turn to national and international standards to implement relevant policies for the retention and long-term archival storage of data in electronic format, the central issue is to ensure there is no difference between the claims that a policy existed and the documents relating to the policy were properly drawn up, and any failure to abide by the policy or standards in practice. If there is a difference between the rhetoric and the reality, the opposing lawyers will mercilessly expose the gap, if the organization's own lawyers do not do it before the action begins. ■

Stephen Mason is a barrister in England and Wales, the director of the Digital Evidence Research Programme at the British Institute of International and Comparative Law and the author and general editor of *Electronic Evidence: Disclosure, Discovery & Admissibility*, the author of *Electronic Signatures in Law and E-Mail, Networks and the Internet: A Concise Guide to Compliance with the Law*, and the general editor of the *Digital Evidence Journal*. He may be contacted at stephenmason@stephenmason.co.uk.

References

- Fischer-Dieskau, Stefanie and Daniel Wilke. "Electronically Signed Documents: Legal Requirements and Measures for their Long-term Conservation." *Digital Evidence Journal*, Vol. 3, No. 1, 2006.
- Imwinkelried, Edward J. *Evidentiary Foundations*, 6 ed. Newark, N.J.: Lexis-Nexis/Matthew Bender, 2005.
- Lorraine v. Markel American Insurance Company*. Available at http://indianalawblog.com/documents/Lorraine_v_Markel.pdf provides a useful list of cases on the authentication of electronic evidence (accessed 8 August 2007).
- Mason, Stephen. *Proof of the Authenticity of a Document in Electronic Format Introduced as Evidence*. Pittsburgh: ARMA International Educational Foundation, 2006.
- United Kingdom National Archives. *Generic Requirements for Sustaining Electronic Information over Time: 1 Defining the Characteristics for Authentic Records*. Kew, Surrey: National Archives, 2002.