

Preserving State Government Digital Information



Minnesota Historical Society

Authentication of State Online Primary Legal Material: A White Paper

Abstract

*This white paper identifies and summarizes ongoing discussion about and documentation of the authentication of digital material—especially a state’s online primary legal materials—among the government records management, legislative, and judiciary communities. The current **DRAFT** version frames the issue, provides context, points to pertinent resources, and informs project partners—all in a collective effort to promote understanding and invite conversation.*

DISCLAIMER:

This white paper is a topical overview and nowise intended to offer legal advice. Consult an attorney for assistance with specific concerns or for advice.

Any comments, corrections, or recommendations may be sent to the project team, care of:

Christopher Welter
Government Records Assistant
Minnesota Historical Society
chris.welter@mnhs.org / 651.259.3262

Introduction

In late 2007, the Minnesota Historical Society (MHS) was awarded a grant from the National Digital Information Infrastructure and Preservation Program (NDIIPP) to fund MHS’s project, *A Model Technological and Social Architecture for the Preservation of State Government Digital Information*. Over the first six months of 2008, MHS met with its strategic state partners—California, Illinois, Kansas, Minnesota, Mississippi, and Vermont—to ascertain common interests among them, particularly policy issues that will affect all legislative digital content.

One of the identified issues is the **authentication of electronic material**—the process by which information is assured to be what it appears or claims to be. Simply put, the matter of authentic electronic records—and to what degree they are authentic—is a complex issue.

Records themselves may (and often do) serve different purposes and different audiences over time. Understandings of *authenticity* may vary among these audiences—record creators, record

keepers, and record users. Whereas understandings—and degrees—of authenticity have a robust tradition where paper is the primary medium, such is not the case with the advent of electronic records in the past twenty-odd years.

From Papers to Pixels

The Federal Depository Library Program (FDLP) has encouraged its participating depository libraries to pursue electronic collections. In 2006, according to the U.S. Government Printing Office (GPO), 71% of FDLP publications were electronic only, 21% were electronic or paper, and 8% were paper only.¹ Participating libraries can choose to substitute electronic for paper versions of depository publications, “provided the electronic version is complete, official, and permanently accessible.”² According to the 2007 *Biennial Survey of Depository Libraries*, nearly 59% of participating libraries chose electronic publications in lieu of paper—a 23% increase since 1999.³ In fact, GPO is developing an advanced digital system to manage Federal information, called the Federal Digital System (Fdsys).⁴

Like its Federal counterpart, state governments have utilized electronic dissemination of information. For instance, all fifty states and the District of Columbia have posted electronic versions of their respective state statutes online. The ubiquity of such online primary legal materials—declared the “official” record by some states in lieu of print copies—has promoted greater access yet has raised concomitant concerns. For instance, Minnesota’s Revisor of Statutes Michele Timmons posed the question during one partner meeting: *How can the Revisor’s Office say to the public that what they’re seeing online is in fact trustworthy?* Other project partners also echoed this sentiment.

Scope and Organization of White Paper

This white paper identifies, summarizes, and promotes resources—general and specific, theoretical and practical, international and parochial—covering both the concept of authenticity and the process of authentication.

Section 1— State Statutes, Legislative Acts, and Interpretive Rules

Summarizes the advent of electronic business transactions, the promotion and dissemination of electronic government information, and the corresponding legislation (UETA, E-Sign, E-Government) and rules (Federal Rules of Evidence, Federal Rules of Civil Procedure) that govern and affect them.

- | | |
|--|--------|
| ➤ Legal Status of Minnesota’s State Statutes | Page 4 |
| ➤ Uniform Electronic Transactions Act (UETA) | Page 4 |
| ➤ Electronic Signatures in Global and National Commerce Act (E-Sign) | Page 6 |
| ➤ E-Government Act | Page 6 |
| ➤ Federal Rules of Evidence | Page 7 |
| ➤ Federal Rules of Civil Procedure | Page 8 |

¹ http://www.access.gpo.gov/su_docs/fdlp/pubs/proceedings/06spring/mostlyelectronic-rev.pdf, 3-4

² http://www.access.gpo.gov/su_docs/fdlp/coll-dev/subguide.html

³ <http://www.fdlp.gov/repository/bsurvey/index.html>

⁴ <http://www.gpo.gov/projects/fdsys.htm>

Section 2—Current Discussion in Legal Communities

Focuses on organizations that are actively discussing authenticity, particularly as it applies to admissible electronic evidence in the American court system.

- Article: “The ‘Authenticity Crisis’ In Real Evidence” Page 9
- Article: “Authentic Digital Records: Laying the Foundation for Evidence” Page 9
- American Bar Association—Information Security Committee Page 10
- Uniform Law Commission (ULC) Page 11
- American Association of Law Libraries (AALL) Page 13
- The Sedona Conference Page 15
- Association of Reporters of Judicial Decisions (ARJD) Page 16

Section 3—Selected Initiatives

Covers two initiatives: 1) the U.S. Government Printing Office’s recent adoption of Public Key Infrastructure (PKI) technology to authenticate PDF documents; 2) the implementation of the framework model Control Objectives for Information and related Technology (Cobit).

- U.S. Government Printing Office (GPO) Page 18
- Cobit Guidelines Page 19

Legal Status of Minnesota's State Statutes

When Minnesota's Revisor of Statutes asks *How can the Revisor's Office say to the public that what they're seeing online is in fact trustworthy?*, it is precisely because all print copies of the state statutes are certified by that office.

Minnesota Statutes Section 3C.13 (Legal Status of Statutes) reads in part, "Any volume of Minnesota Statutes, supplement to Minnesota Statutes, and Laws of Minnesota certified by the revisor according to section 3C.11, subdivision 1, is prima facie evidence of the statutes contained in it in all courts and proceedings."

Minnesota Statutes Section 3C.11 (General Publication Duties), subdivision 1 (Certificate of Correctness) reads,

In preparing an edition of Minnesota Statutes, a supplement to Minnesota Statutes, or an edition of Laws of Minnesota, the Revisor's Office shall compare each section in the edition with the original section of the statutes or with the original section in the enrolled act from which the section was derived, together with all amendments of the original section. In one copy of the edition, the revisor shall attach a certificate certifying that this comparison has been made and that all sections appear to be correctly printed. The copy containing the revisor's certificate must be filed in the office of the secretary of state as a public record. All other copies of the edition must contain a printed copy of the certificate.

The Revisor's certificate reads, "I certify that each section printed in Minnesota Statutes [year of publication] has been compared with the original section of the statutes or with the original section in the enrolled act from which the section was derived, together with all amendments to the original section. All sections appear to be correctly printed. [name] Revisor of Statutes."

The following disclaimer about official versions of state statutes is included on the Revisor's Web site: "Information on this website is not intended to replace the official versions. However, every attempt has been made to ensure that the information on this website is accurate and timely. The website is presented 'as is' and without warranties, either express or implied, including warranties regarding the content of this information."⁵

Foundations for an Electronic Environment

Beginning in the late 1990s, legal communities and legislative bodies began to address the advent of electronic commerce and communications. Here follow synopses of the cogent legislative acts and related administrative rules.

Uniform Electronic Transactions Act of 1999 (UETA)

<<http://www.law.upenn.edu/bll/archives/ulc/fnact99/1990s/ueta99.htm>>

⁵ <https://www.revisor.leg.state.mn.us/statutes/?view=info>

The National Conference of Commissioners on Uniform State Laws (NCCUSL), which is also known as the Uniform Law Commission, promulgated UETA, a comprehensive effort to prepare state law for electronic commerce. It establishes the legal equivalence of electronic records and signatures with paper writings and manually signed signatures, removing barriers to electronic commerce.

To review all of NCCUSL's efforts on UETA, refer to "Electronic Transactions Act" on NCCUSL's acts list.⁶ The National Conference of State Legislatures (NCSL) also maintains a listing of which states have adopted UETA, when they did so, and each's specific statutory citation.⁷

The Minnesota State Archives' *Trustworthy Information Systems Handbook* summarizes UETA thus:

The purpose of the Uniform Electronic Transactions Act (UETA) is to develop an act relating to the use of electronic communications and records in contractual transactions. The UETA governs electronic records and signatures relating to a transaction, defined as limited to business, commercial and governmental affairs. It is intended to be consistent with the Uniform Commercial Code, but not duplicative of it. As a result, the UETA is procedural and affects the underlying substantive law of a given transaction only if absolutely necessary in light of the differences in media used. Whether a record is attributed to a person, and whether an electronic signature has any effect, is left to other substantive law.⁸

The 62-page report (known as the Final Act⁹) consists of twenty-one sections. Its clear and limited objective is to ensure "that an electronic record of a transaction is the equivalent of a paper record, and that an electronic signature will be given the same legal effect, whatever that might be, as a manual signature."

Section 7 lays out the act's four basic rules:

The most fundamental rule in Section 7 provides that a "record or signature may not be denied legal effect or enforceability solely because it is in electronic form." The second most fundamental rule says that "a contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation." The third most fundamental rule states that any law that requires a writing will be satisfied by an electronic record. And the fourth basic rule provides that any signature requirement in the law will be met if there is an electronic signature.¹⁰

Section 12 (Retention of electronic records; originals) states that "If a law requires that a record be retained, the requirement is satisfied by retaining an electronic record of the information in the record which: (1) accurately reflects the information set forth in the record after it was first generated in its final form as an electronic record or otherwise; and (2) remains accessible for later reference."

Conceptually, the report acknowledges that an original document, so-called, in an electronic environment is problematic. However, Section 12 "assures that information stored electronically

⁶ <http://www.nccusl.org/Update/DesktopDefault.aspx?tabindex=0&tabid=65>

⁷ <http://www.ncsl.org/programs/lis/CIP/ueta-statutes.htm>

⁸ <http://www.mnhs.org/preserve/records/tis/AppendixEVII.html>

⁹ <http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm>

¹⁰ http://www.nccusl.org/Update/uniformact_summaries/uniformacts-s-ueta.asp

will remain effective for all audit, evidentiary, archival and similar purposes”—provided there is a “reliable assurance that the electronic record accurately reproduces the information” of the original. The report states that Section 12 is consistent with the Federal Rules of Evidence 1001(3) and Uniform Rules of Evidence 1001(3) (1974).

Written as an optional portion of the Act, Sections 17-19 apply directly to state governmental agencies. Section 17 covers creation and retention of electronic records, and conversion of written records; it “allows a state to designate one agency or officer as the authority on creation and retention of governmental records.” Section 18 covers acceptance and distribution of electronic records; it “allows a state to designate which agency or officer regulates the communication of electronic records and use of electronic signatures between agencies and other persons.” Section 19 covers interoperability; it “allows a state to designate an agency or officer to set standards that promote consistency and interoperability between state agencies with respect to the use of electronic records and signatures.”¹¹

E-Sign Act of 2000

http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ229.106.pdf

Formally known as the Electronic Signatures in Global and National Commerce Act, E-Sign is an act “To facilitate the use of electronic records and signatures in interstate or foreign commerce.”

For a synopsis on how UETA and E-Sign compare and contrast, see ULC’s hosting of Patricia Brumfield Fry’s essay, “Why Enact UETA? The Role of UETA After E-Sign.”¹²

Under “General Rule of Validity” (§101), the act establishes two fundamental points ensuring the validity and legal effect of contracts entered into electronically:

- 1) that “a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form;
- 2) that “a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation.”

Under “Definitions” (§106), an electronic signature “means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.”

E-Government Act of 2002

http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ347.107.pdf

This is an act “To enhance the management and promotion of electronic Government services and processes by establishing a Federal Chief Information Officer within the Office of

¹¹ UETA Summary; http://www.nccusl.org/Update/uniformact_summaries/uniformacts-s-ueta.asp

¹² <http://www.nccusl.org/Update/Docs/Why%20Enact%20UETA.asp>

Management and Budget, and by establishing a broad framework of measures that require using Internet-based information technology to enhance citizen access to Government information and services, and for other purposes.”

Under Definitions [§3542(b)(1)(A)], “integrity . . . means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.”

Federal Rules of Evidence

<<http://judiciary.house.gov/media/pdfs/printers/110th/evid2007.pdf>>

These rules govern the introduction of evidence in proceedings, both civil and criminal, in Federal courts. While they do not apply to suits in state courts, the rules of many states have been closely modeled on these provisions.

Article IX covers authentication and identification.

Rule 901(a) General Provision: “The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.”

Rule 901(b) illustrates specific, non-exclusive examples, some of which may be germane to online legislative information:

(7) *Public records or reports.* Evidence that a writing authorized by law to be recorded or filed and in fact recorded or filed in a public office, or a purported public record, report, statement, or data compilation, in any form, is from the public office where items of this nature are kept.

(9) *Process or system.* Evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result.

(10) *Methods provided by statute or rule.* Any method of authentication or identification provided by Act of Congress or by other rules prescribed by the Supreme Court pursuant to statutory authority.

Rule 902 covers self-authentication where “Extrinsic evidence of authenticity as a condition precedent to admissibility is not required with respect to the following” examples, some of which may be germane to online legislative information:

(4) Certified copies of public records. A copy of an official record or report or entry therein, or of a document authorized by law to be recorded or filed and actually recorded or filed in a public office, including data compilations in any form, certified as correct by the custodian or other person authorized to make the certification, by certificate complying with paragraph (1), (2), or (3) of this rule or complying with any Act of Congress or rule prescribed by the Supreme Court pursuant to statutory authority.

(5) Official publications. Books, pamphlets, or other publications purporting to be issued by public authority.

Article X defines *writings, recordings, and photographs*, and it differentiates between *originals* and *duplicates*.

According to Rule 1001, an *original* “is the writing or recording itself or any counterpart intended to have the same effect by a person executing or issuing it,” whereas a *duplicate* “is a counterpart produced by the same impression as the original, or from the same matrix.”

Rule 1002 establishes that an original is required as evidence; however, Rule 1003 establishes that a duplicate is admissible unless

- 1) “a genuine question is raised as to the authenticity of the original”
- 2) “in the circumstances it would be unfair to admit the duplicate in lieu of the original.”

Rule 1005 addresses public records:

The contents of an official record, or of a document authorized to be recorded or filed and actually recorded or filed, including data compilations in any form, if otherwise admissible, may be proved by copy, certified as correct in accordance with rule 902 or testified to be correct by a witness who has compared it with the original. If a copy which complies with the foregoing cannot be obtained by the exercise of reasonable diligence, then other evidence of the contents may be given.

Federal Rules of Civil Procedure

<<http://judiciary.house.gov/media/pdfs/printers/109th/31308.pdf>>

The FRCP govern the conduct of all civil actions brought in Federal district courts. While they do not apply to suits in state courts, the rules of many states have been closely modeled on these provisions.

Amendments to the FRCP that explicitly address electronically stored information (ESI) took effect in December 2006.

Rule 34 covers, for discovery purposes, the production of documents, electronically stored information, and tangible things. Specifically, Rule 34(a)(1)(A) addresses “any designated documents or electronically stored information—including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations—stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form.”

Overview

Because of the nature of evidence and its role in the judiciary process, the legal community has long been concerned with the purported authenticity of it. Some observers have called the proliferation of digital data and electronic records a sea change, one that has outpaced the legal community's response to it. The following two articles specifically address these issues, providing background and context.

In March 2006 *Law Practice Today* published George L. Paul's article, "The 'Authenticity Crisis' In Real Evidence."¹³ Paul provides a succinct overview of so-called real evidence, both analog and digital, and how an understanding of authenticity (especially as it relates to the Federal Rules of Evidence) must be more closely examined.

Paul reflects that the Federal Rules of Evidence were enacted in 1975, when informational records relied on analog technology and "the relative immutability of [its] storage media." Because analog technology "makes alteration expensive, a process requiring both skill and intent" and "alteration . . . usually detectable," juries "became accustomed" to accepting such informational records as genuine pieces of evidence. Digital informational records, however, are comparatively more malleable.

Stephen Mason¹⁴, a barrister in the United Kingdom, takes up this same issue in his article, "Authentic Digital Records: Laying the Foundation for Evidence" (published in the September/October 2007 issue of *The Information Management Journal*). The article itself is based on Mason's research project, *Proof of the Authenticity of a Document in Electronic Format Introduced as Evidence*, commissioned by the ARMA International Educational Foundation.¹⁵

Mason's touchstone for his article is the 2005 court case *In re Vee Vinhnee, debtor, American Express Travel Related Services Company Inc. v. Vee Vinhnee*. Claiming that Vinhnee failed to pay credit card debts, American Express attempted to recoup its losses, but the trial judge determined that American Express failed to authenticate certain records in digital format, ultimately sabotaging its case.

In addressing American Express's handling of its electronic records, the judge summarized thus:

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. (34)

Mason asserts that the characteristics of authentication are comprised in three categories:

¹³ <http://www.abanet.org/lpm/lpt/articles/tch03065.shtml>

¹⁴ Chambers of Stephen Mason Web site; <http://www.stephenmason.eu/>

¹⁵ <http://www.armaedfoundation.org/2006researchprojects.html>

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

Mason concludes that (for records managers at least) the most difficult task is preservation of digital records. Accepting that “Perfection is impossible,” he recommends following accepted standards and best practices: “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” (40).

Principal Organizations & Associations

American Bar Association (ABA) <<http://www.abanet.org/>>

Among its functions, the ABA provides "information about the law, programs to assist lawyers and judges in their work, and initiatives to improve the legal system for the public."

The ABA's Information Security Committee (under the auspices of the Section of Science and Technology Law) has issued a *Digital Signature Guidelines Tutorial*¹⁶ in an effort to establish a framework for the authentication of computer-based information. It examines the historical legal concept of a "signature" and how digital signatures (using public key infrastructure, or PKI, technology) fulfill and perhaps expand that historical concept.

According to the *Tutorial*, the act of signing a writing generally accomplishes these purposes:

- **Evidence:** A signature authenticates a writing by identifying the signer with the signed document. When the signer makes a mark in a distinctive manner, the writing becomes attributable to the signer.
- **Ceremony:** The act of signing a document calls to the signer's attention the legal significance of the signer's act, and thereby helps prevent "inconsiderate engagements.
- **Approval:** In certain contexts defined by law or custom, a signature expresses the signer's approval or authorization of the writing, or the signer's intention that it have legal effect.
- **Efficiency and logistics:** A signature on a written document often imparts a sense of clarity and finality to the transaction and may lessen the subsequent need to inquire beyond the face of a document. Negotiable instruments, for example, rely upon formal requirements, including a signature, for their ability to change hands with ease, rapidity, and minimal interruption.

The *Tutorial* concludes by discussing both challenges and opportunities when implementing digital signatures. On the one hand, they may offer a solution to impostors, message integrity, formal legal requirements, and open systems. On the other, there may be significant cost overhead to both the implementing institution and to its service constituencies.

¹⁶ <http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html>

PKI technology in and of itself has fostered significant discussion about the process of authentication. In 2000, for example, Carl Ellison and Bruce Schneier published “Ten Risks of PKI: What You’re not Being Told about Public Key Infrastructure.”¹⁷ The authors hold that PKI as a commodity makes for a low up-front cost, potentially high rate-of-return product, and that the preponderance of then current literature was written and promoted by PKI vendors—ultimately leaving significant questions about PKI’s efficacy unanswered, which the authors attempt to address.

In a rebuttal to Ellison and Schneier, Carlisle Adams (University of Ottawa) and Mike Just (Secretariat, Treasury Board of Canada) wrote the white paper “PKI: Ten Years Later.”¹⁸ The paper’s abstract reads thus:

In this paper, we examine the history and evolution of so-called Public Key Infrastructure (PKI). We compare the original definition of PKI with a broader and more flexible definition that better reflects the variety of implementation philosophies available today. This current definition shows how the understanding of this technology has matured (although its essential characteristics have remained unchanged) and is derived, at least in part, from an evaluation and comparison of several quite different forms of PKI as well as a consideration of PKI criticisms over the years. The original definition of PKI may be dead or dying, but PKI technology continues to thrive as an extremely useful (and, in some cases, necessary) authentication solution.

As for PKI technology being used to authenticate government information, the U.S. Government Printing Office is using it on specific PDF documents hosted on its Web site, GPO Access. (This white paper examines that matter subsequently.)

On the state level, the Minnesota State Archives addresses digital signatures (on which PKI is based) in its *Electronic Records Management Guidelines*.¹⁹

Uniform Law Commission (ULC) <<http://www.nccusl.org/Update/>>

The ULC (also known as the National Conference of Commissioners on Uniform State Laws) promulgates legislation to facilitate clarity, consistency, and efficiency among state legislative points of law. The ULC is in fact a conglomeration of commissioners appointed by each of the fifty states, the District of Columbia, the Commonwealth of Puerto Rico, and the U.S. Virgin Islands, and each appointed commissioner is a member of the bar: state legislators, practicing lawyers, state and federal judges, law professors, and legislative staff attorneys. No uniform law is effective until a state legislature adopts it.

In 1999, the ULC promulgated the aforementioned Uniform Electronic Transactions Act (UETA), a comprehensive effort to prepare state law for electronic commerce’s advent. Its single purpose is to ensure “that an electronic record of a transaction is the equivalent of a paper record, and that an electronic signature will be given the same legal effect, whatever that might be, as a manual signature.”²⁰

¹⁷ *Computer Security Journal*, vol. 16, no. 1., 2000; PDF available at <http://www.schneier.com/paper-pki.html>

¹⁸ http://middleware.internet2.edu/pki04/proceedings/pki_ten_years.pdf

¹⁹ <http://www.mnhs.org/preserve/records/electronicrecords/ersigs.html>

²⁰ <http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm>

For an up-to-date list of states that have adopted UETA—including year enacted and statutory citations—consult the National Conference of State Legislatures' UETA Web page.²¹

In autumn 2008, the ULC plans to convene the Study Committee on Authentication of Online State Legal Materials.²² Commissioner Michele Timmons, the Minnesota Revisor of Statutes, requested the study committee's creation.

In April 2007, Ms. Timmons spoke at an AALL-sponsored conference, "Authentic Legal Information in the Digital Age." In June, Ms. Timmons proposed to the ULC the creation of a study committee, but ULC's Scope and Program Committee had certain questions. In August Robert Stein, chair of ULC's Executive Committee, wrote a letter of inquiry to the AALL for input on a potential ULC study committee's scope and focus.

In December AALL's Mary Alice Baish, Acting Washington Affairs Representative, responded in a two-page letter to ULC's questions.

What objective could be achieved by a uniform law dealing with authentication of online legal resources? Citing its own 2007 report, AALL believes that online legal digital materials—"vulnerable to lapses in management and control, corruption, and tampering"—must be as trustworthy as print official legal resources, and that "state government entities must assume responsibility for ensuring the full life cycle of their online legal information."

As more state agencies eliminate print for electronic resources to cut costs, AALL is concerned that the electronic counterparts are neither capable of authentication nor permanently publicly accessible (only the most current legal information may be available online). It therefore believes that "an effort to simply update current state statutes pertaining to publication of primary legal resources would be exceedingly difficult" and that only a uniform law will spur state government entities to "address the challenges of digital authentication and preservation by implementing technological solutions" prior to abandoning print official legal resources.

What should the scope of such a project be? AALL believes that a uniform law ought to "cover all state-level online legal information" (e.g., state administrative codes and registers, state statutes and session laws, and state high and intermediate appellate court opinions).

What is the impact of copyright on public accessibility? "Having a copyright notice attached to an online legal document should have no bearing at all to its being both official and authentic."

Might the problem of authenticity be better solved with the creation of some best practices standards? AALL believes that best practices, while helpful, would prove insufficient and are a "piecemeal approach rather than a universal solution and would not address the important legal principles that are currently at stake."

Although AALL recommends no one technological solution, it does point that in 2004 France adopted the use of encryption, digital signatures, and PKI technology to ensure authentication of its online official journal (*Les Journaux Officiels*), and that the U.S. Government Printing Office is doing much the same thing.

²¹ <http://www.ncsl.org/programs/lis/CIP/ueta-statutes.htm>

²² <http://www.nccusl.org/Update/CommitteeSearchResults.aspx?committee=321>

American Association of Law Libraries (AALL) <<http://www.aallnet.org/aallwash/index.html>>

In March 2007, AALL published the *State-by-State Report on Authentication of Online Legal Resources*.²³ Considered a companion piece to AALL's 2003 *State-by-State Report on Permanent Public Access to Electronic Government Information*,²⁴ the report proposes to answer the question: How trustworthy are state-level primary legal resources on the Web?

In the 2003 report, authenticity is not the primary focus but is alluded to in three separate places (emphasis added):

These needs [to manage the entire lifecycle of electronic government information] include ensuring that electronic government information is easily located; that an electronic publication is deemed “**authentic**” and “official”; and that electronic government information of long-term value will be preserved for permanent public access.

The American Association of Law Libraries (AALL) believes that the government is responsible for creating useful finding tools needed to locate electronic government information; ensuring its **authenticity**, particularly when there is no longer an official, tangible version; and guaranteeing that valuable electronic government information will be retained and preserved, ensuring permanent public access.

These [important challenges of electronic government information] include the difficulty of locating the specific government information one needs; the uncertainty one has that the electronic information is not considered to be the reliable, **authentic** version; and the ultimate frustration—a broken URL for a Web publication that one may have used as recently as a month ago. AALL believes strongly that, in the online environment, the government is responsible for creating useful finding tools to locate electronic government information; for ensuring its **authenticity** when the decision is made to no longer produce the information in an official tangible version; and for ensuring that valuable electronic government information will be not only retained and preserved, but will also remain available for permanent public access.²⁵

The 2007 report outlines six key findings and includes individual reports for all fifty states and the District of Columbia.

According to the report's introduction,

The Authentication Survey, completed [online] by AALL Members in 2006, targeted six sources of law: state administrative codes and registers, state statutes and session laws, and state high and intermediate appellate court opinions.

The summary answer to the question of their trustworthiness is this: A significant number of the state online legal resources are *official* but none are *authenticated*

²³ http://www.aallnet.org/aallwash/authen_rprt/AuthenFinalReport.pdf

²⁴ http://www.aallnet.org/aallwash/State_report.pdf

²⁵ PPA “Executive Summary” 1, 2; “Background” 8

or afford ready authentication by standard methods. State online primary legal resources are therefore not sufficiently trustworthy.

Modeled on the U.S. Government Printing Office's 2005 *Authentication* white paper,²⁶ here follows the AALL survey's working definition of authentication:

An *authentic* text is one whose content has been verified by a government entity to be complete and unaltered when compared to the version approved or published by the content originator. Typically, an *authentic* text will bear a certificate or mark that conveys information as to its certification, the process associated with ensuring that the text is complete and unaltered when compared with that of the content originator. An *authentic* text is able to be *authenticated*, which means that the particular text in question can be validated, ensuring that it is what it claims to be.

The report goes on to say that the "definition clearly recognizes that online legal resources are inherently capable of being corrupted or tampered with at the level of the individual copy. In that respect, online legal resources are fundamentally different from print legal resources."

The report concludes this is unacceptable because "To be trustworthy, digital materials . . . must be equivalent to print *official* legal resources. To be equivalent, they must be *authentic*." And "An *authenticated* resource is one shown to be a complete and unaltered version of an approved text."

As to legal admissibility, the report states, "no definite laws or rules state that particular online legal resources are entitled to judicial notice and other recognition as authoritative statements of the law. Statutes are sometimes unclear as to whether they apply to both print and online versions of legal resources or to print alone."

Summary of AALL Report's Key Findings [Project partners are highlighted in **bold**]

- 1) States have begun to discontinue print official legal resources and substitute online official legal sources [e.g., sole *official* version of the Utah statutes is on the Web].
- 2) Ten states [including **Minnesota** and **Tennessee**] plus D.C. have deemed as official one or more of their online primary legal resources.
- 3) One or more of the online primary legal sources of eight states [including **California** and **Vermont**] have "official traits," where evidence as to the actual status of the resources is conflicting.
- 4) States have not acknowledged important needs of citizens and law researchers seeking government information; they have not been sufficiently deliberate in their policies and practices. ["The prevalent use of disclaimers – which may be contrasted with very limited use of disclaimers for official and unofficial print titles – points to fundamental differences between online and print media."]

²⁶ <http://www.gpoaccess.gov/authentication/authenticationwhitepaperfinal.pdf>

- 5) No state's online primary legal resources are authenticated or afford ready authentication by standard methods [**Minnesota, Tennessee, and Vermont** are among the states cited as addressing the matter, or at least considering it].
- 6) Eight states [including **California** and **Minnesota**] have provided for permanent public access (PPA) to one or more of their online primary legal resources.

The Sedona Conference® <<http://www.thesedonaconference.org/>>

The Sedona Conference (TSC) is a nonprofit 501(c) (3) research and education institute that

. . . exists to allow leading jurists, lawyers, experts, academics and others, at the cutting edge of issues in the area of antitrust law, complex litigation, and intellectual property rights, to come together—in conferences and mini-think tanks (Working Groups)—and engage in true dialogue, not debate, all in an effort to move the law forward in a reasoned and just way.²⁷

TSC augments and complements its conferences with the Working Group Series, loosely based on an open think-tank model. Working groups investigate specific subjects, are limited to 35 core participants (though membership is not limited), and produce publications on an ongoing basis.

Presently, there are seven working groups, the first of which—Electronic Document Retention and Production (EDRP)—issued *The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production*.

As judicial understanding evolves and case law grows, all TSC working groups update their publications periodically, and all publications (drafts, commentaries, revisions, new reports, etc.) are posted online.²⁸ *The Sedona Principles*, for example, was made available in March 2003 for public comment, was formally issued in January 2004, and was updated in July 2005. *The Sedona Principles, Second Edition (2007)* was issued “to reflect the impact of the 2006 e-discovery amendments to the Federal Rules of Civil Procedure . . . and to provide useful commentary on their implementation.”²⁹

The Sedona Principles elucidates fourteen principles, the first of which reads, “Electronically stored information is potentially discoverable under Fed. R. Civ. P. 34 or its state equivalents. Organizations must properly preserve electronically stored information that can reasonably be anticipated to be relevant to litigation.”

*The Federal Rules of Civil Procedure*³⁰ Rule 34 covers, for discovery purposes, the production of documents, electronically stored information, and tangible things. Specifically, Rule 34(a)(1)(A) addresses “any designated documents or electronically stored information—including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations—stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form.”

²⁷ http://www.thesedonaconference.org/content/tsc_mission/show_page_html

²⁸ http://www.thesedonaconference.org/content/miscFiles/publications_html?grp

²⁹ *The Sedona Principles after the Federal Amendments, August 2007*;
<http://www.thesedonaconference.org/dltForm?did=2007SummaryofSedonaPrinciples2ndEditionAug17assentforWG1.pdf>

³⁰ <http://judiciary.house.gov/media/pdfs/printers/109th/31308.pdf>

The Federal Rules of Civil Procedure are *The Sedona Principles*' touchstone. However, *The Sedona Principles* "are intended to complement the Federal Rules of Civil Procedure, which provide only broad standards, by establishing guidelines specifically tailored to address the unique challenges posed by electronic document production."³¹ Moreover, "Far from supplanting *The Sedona Principles*, the new Federal Rules [issued in 2006] have highlighted the many areas of electronic discovery in which there is continued and growing need for guidance."³²

In March 2008, Sedona's EDRP published its "Commentary on ESI [Electronically Stored Information] Evidence & Admissibility."³³

The commentary moves one step beyond the practice of e-discovery to discuss the admission of ESI into evidence and is divided into three sections:

- 1) Brief survey of the applicability and application of existing evidentiary rules and case law addressing the same.
- 2) New issues and pitfalls that are looming on the horizon.
- 3) Practical guidance on the use of ESI in depositions and in court.

Appendix A includes a checklist of potential authentication methods (by format) with citations to the appropriate Federal Rules of Evidence.

Association of Reporters of Judicial Decisions (ARJD) < <http://arjd.washlaw.edu/>>

The Association of Reporters of Judicial Decisions "is an international organization of public servants whose primary responsibility is to prepare the opinions and judgments of appellate and other courts for official publication." It issued a position paper, "Statement of Principles: 'Official' On-Line Documents,"³⁴ in February 2007 and revised it in May 2008.

The six abridged principles follow:

- A government document should not be considered "official" unless it is authorized by law or is designated "official" by the governmental entity that issued it.
- There should be only one "official" version of a document in existence at any one time.
- On-line government documents should not be designated "official" unless they are (1) authenticated by encryption, digital signature, or some other computerized process to safeguard them from illegal tampering and (2) permanent in that they are impervious to corruption by natural disaster, technological obsolescence, and similar factors and their

³¹ *The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document*

Discovery iv (Sedona Conference Working Group Series 2004)

³² *The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document*

Production, Second Edition iv (The Sedona Conference® Working Group Series, 2007)

³³ http://www.thesedonaconference.org/dltForm?did=ESI_Commentary_0308.pdf

³⁴ http://arjd.washlaw.edu/ARJD_Statement_of_Principles_May2008.pdf

digitized form can be readily translated into each successive electronic medium used to publish them.

- If a governmental entity chooses to designate multiple co-existing versions (print and/or electronic) as “official,” mechanisms must be provided to ensure that each of those official versions meets the foregoing authentication and permanence criteria.
- An on-line government document, even one designated “official,” cannot be considered authoritative if it does not satisfy the foregoing authentication criterion.
- So long as only the print version of an official document meets the foregoing authentication and permanence criteria, the print version (and any printed errata thereto) should control and be considered authoritative whenever there is a discrepancy between it and an on-line version of the same document that has also been designated “official.”

Section 3: Selected Initiatives

U.S. Government Printing Office (GPO) <<http://www.gpoaccess.gov/>>

Established in 1813, GPO “is the Federal Government’s primary centralized resource for gathering, cataloging, producing, providing and preserving published information in all its forms.”³⁵

GPO oversees the Federal Depository Library Program (FDLP), which “involves the acquisition, format conversion, and distribution of depository materials and the coordination of Federal depository libraries across the country.” Historically, these materials were tangible products that were distributed throughout libraries participating in the FDLP, providing ready access to American citizens.

Since the 1990s, items increasingly may reside in both a tangible and virtual form. Accordingly, GPO launched *GPO Access on the Web*, a “free service . . . funded by the Federal Depository Library Program [that] has grown out of Public Law 103-40, known as the *Government Printing Office Electronic Information Enhancement Act of 1993*.”³⁶

The Federal Depository Library Program (FDLP) has encouraged its participating depository libraries to pursue electronic collections. In 2006, according to the U.S. Government Printing Office (GPO), 71% of FDLP publications were electronic only, 21% were electronic or paper, and 8% were paper only.³⁷ Participating libraries can choose to substitute electronic for paper versions of depository publications, “provided the electronic version is complete, official, and permanently accessible.”³⁸ According to the 2007 *Biennial Survey of Depository Libraries*, nearly 59% of participating libraries chose electronic publications in lieu of paper—a 23% increase since 1999.³⁹

It should be remembered that the FDLP must provide access to content, and that the National Archives and Record Administration is responsible for preservation of content:

The [FDLP Electronic] Collection consists of permanent access reference copies maintained by GPO or its partners for the convenience of reference. Inclusion of an agency electronic information product in the Collection is in no way intended to be a substitute for the issuing agency's disposition of that product to NARA in accordance with a records schedule.⁴⁰

More recently, GPO has focused on the authenticity (in addition to access) of digital Federal information and is maintaining a Web resource page on its authentication measures.⁴¹ According to GPO, “The information provided on [*GPO Access*] is the official, published version and the information retrieved from *GPO Access* can be used without restriction, unless specifically noted.”⁴² Moreover, GPO has begun assigning digital signatures to selected PDF

³⁵ <http://www.gpo.gov/factsheet/index.html>

³⁶ <http://www.gpo.gov/factsheet/index.html#4>

³⁷ http://www.access.gpo.gov/su_docs/fdlp/pubs/proceedings/06spring/mostlyelectronic-rev.pdf, 3-4

³⁸ http://www.access.gpo.gov/su_docs/fdlp/coll-dev/subguide.html

³⁹ <http://www.fdlp.gov/repository/bsurvey/index.html>

⁴⁰ http://www.access.gpo.gov/su_docs/fdlp/pubs/ecplan.html

⁴¹ <http://www.gpoaccess.gov/authentication/>

⁴² <http://www.gpoaccess.gov/about/index.html>

documents—including the Fiscal Year 2009 Budget. (In fact, GPO is developing an advanced digital system to manage Federal information, called the Federal Digital System, or FDSys.⁴³)

GPO released its Authentication white paper on June 23, 2005, for public comment and published its final version on October 13, 2005.⁴⁴ Concerns from the public included granularity (to date, individual documents are the only unit measure for authentication) and authentication of Web pages (GPO's authentication process applies to PDF documents only). The American Association of Law Libraries relies significantly upon this white paper in its own Authenticity report.

GPO Access digital signatures can only be validated using Adobe Acrobat or Reader, versions 7.0 or higher.

GPO Access provides links to four separate PDF documents that discuss Public Key Infrastructure (PKI) technology, which it's using for its digital signatures.

Cobit Guidelines

<http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders1/COBIT6/FAQ6/COBIT_FAQ.htm>

Organized in 1967, ISACA—formerly known as the Information Systems Audit and Control Association—is an international organization for information governance, control, security, and audit professionals.

The **Control Objectives for Information and related Technology (COBIT)** is a set of best practices (framework) for information technology (IT) management created by ISACA and the IT Governance Institute (ITGI) in 1992. COBIT provides managers, auditors, and IT users with a set of generally accepted measures, indicators, processes and best practices to assist them in maximizing the benefits derived through the use of information technology and developing appropriate IT governance and control in a company.⁴⁵

In the Executive Overview to COBIT's most recent version (4.1), it is stated that "Organizations should satisfy the quality, fiduciary and security requirements for their information." To that end, COBIT

provides good practices across a domain and process framework and presents activities in a manageable and logical structure. COBIT's good practices represent the consensus of experts. They are strongly focused more on control, less on execution. These practices will help optimise IT-enabled investments, ensure service delivery and provide a measure against which to judge when things do go wrong.⁴⁶

ISACA lists case studies from across industries—Consulting/IT, Government, Education, Manufacturing/Transportation, and Financial Services/Insurance—on its Web site.⁴⁷ In 2002 for

⁴³ <http://www.gpo.gov/projects/fdsys.htm>

⁴⁴ <http://www.gpoaccess.gov/authentication/authenticationwhitepaperfinal.pdf>

⁴⁵ <http://en.wikipedia.org/wiki/COBIT>

⁴⁶ <http://www.isaca.org/AMTemplate.cfm?Section=Downloads&Template=/ContentManagement/ContentDisplay.cfm&ContentID=34172>

⁴⁷ <http://www.isaca.org/Template.cfm?Section=COBIT6&CONTENTID=22129&TEMPLATE=/ContentManagement/ContentDisplay.cfm>

instance, the Office of Inspector General (OIG) of the U.S. House of Representatives implemented Cobit to improve and control its IT infrastructure.

The State of Kansas, one of this project's partners, is using Cobit "to guide [its] implementation of IT infrastructure and application development initiatives."⁴⁸

⁴⁸ http://www.mnhs.org/preserve/records/legislativerecords/docs_pdfs/KSmeeting20080328.pdf