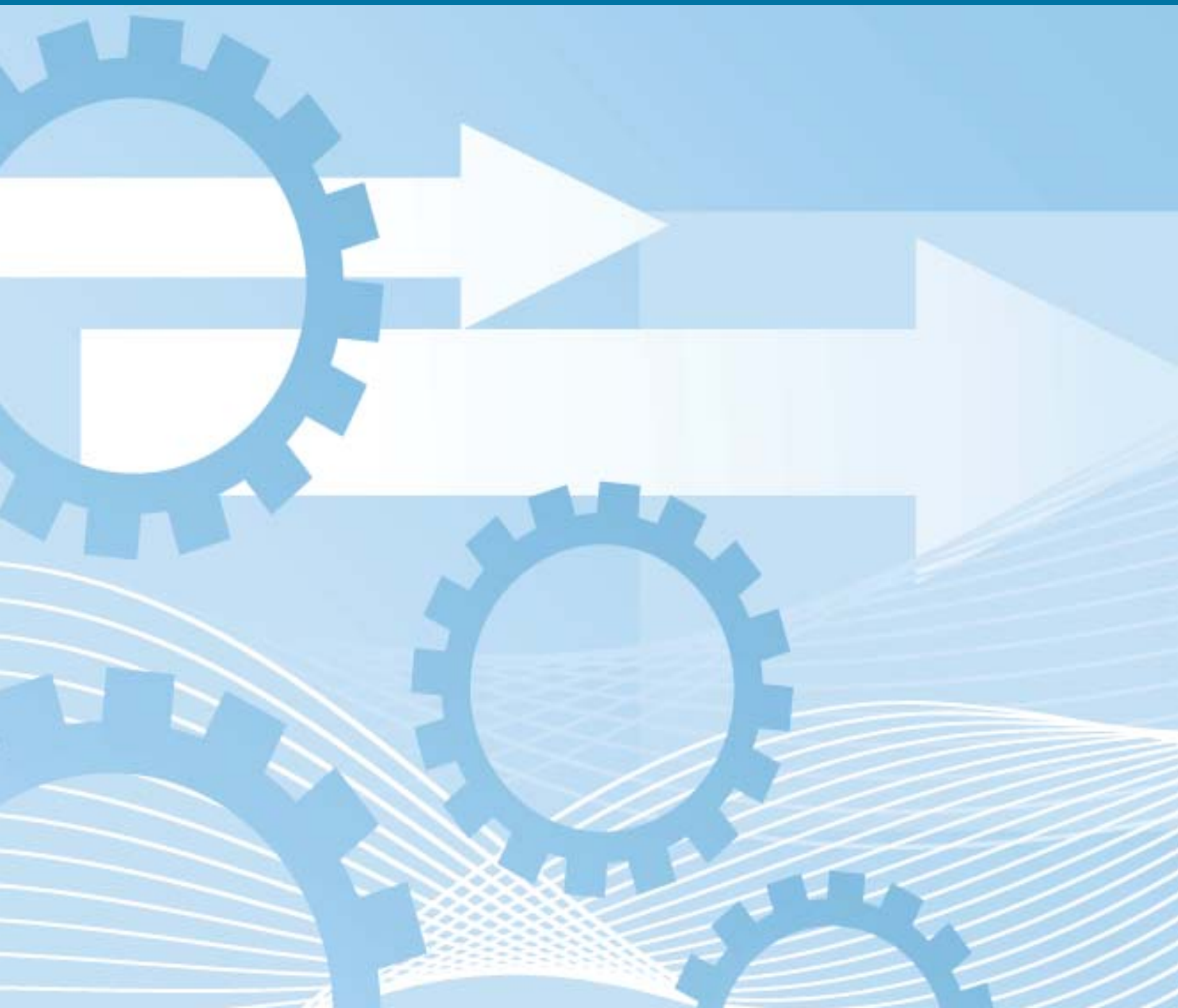
Center for
Technology in Government

Opening Government's Official Legal Materials:
Authenticity and Integrity in the Digital World



Opening Government's Official Legal Materials:
Authenticity and Integrity in the Digital World

Alan S. Kowlowitz
Government Fellow

Center for Technology in Government
University at Albany/SUNY
187 Wolf Road, Suite 301
Albany, NY 12205
www.ctg.albany.edu

February 2012

FOREWARD

Records have always been essential to the transparency, continuity, and reliability of government programs and processes. Today, the records that serve the business, evidentiary, and historical needs of government are increasingly electronic or digital first. Over our 18-year history, CTG has consistently helped provide the public sector with new concepts, tools, and strategies to create and manage electronic records. In these efforts, CTG has worked with all fifty state governments, several U.S. territories, a number of U.S. local governments, the U.S. Library of Congress, and the United Nations.

With this brief, CTG is using its knowledge of electronic records to assist governments in their drive toward greater openness; in this case by supporting states' efforts to increase access to official legal materials in electronic form. New open government initiatives underscore the importance of effectively managing government information so that it is both useful to the public and retains its integrity and authenticity. Questions of integrity and authenticity are of particular importance when the records of interest are primary legal records such as laws, regulations, and court decisions. For such records, usefulness is a function of the extent to which the custodian of those records, in this case state government agencies, have been able to maintain the integrity and authenticity of the record, along with the content.

Many state legislatures are or will be considering laws to allow the creation, provision of access, and preservation of their most fundamental legal records in a digital form that can be presented, accepted, and validated as authentic and legally valid. The policy, managerial, and technological ramifications of such legislation are considerable. This brief was written to give states a high-level overview of the issues and to outline some first steps toward ensuring that each state puts in place a strategy that responds to the specific interests and requirements of that state. The brief will help states develop a roadmap for dealing with the many issues that must be addressed when implementing such legislation if access to official legal materials in electronic form is to truly respond to the vision of a more open government.

Theresa A. Pardo
Director
Center for Technology in Government

Executive Summary

Increasingly, state governments are moving toward making primary legal materials available online via state government websites. Several factors are driving this move toward placing such legal materials online:

- The availability of information technologies that make it possible to electronically "publish" what can be considered official or authentic materials.
- Open government and accountability advocates ongoing call for government to make more data publicly accessible and usable.
- The assumption that government can achieve cost savings and service improvements by automating processes and moving towards a paperless government.
- The fact that in some states primary legal materials are already only published online, but their "authenticity" or value as an "official record" is at best inconsistent.

The goal in these efforts, and also the challenge, is to provide users with more efficient access while ensuring that the electronic versions of primary legal materials are as "official" as their paper originals. The desire of state governments to make this a priority is strong. However, they currently lack the necessary policies and management practices necessary for success. State legislators and their staffs, legislative reference librarians, state archivists, and chief information officers all have important roles to play in laying the foundation for these efforts through the creation of new policy, management, and technology capabilities.

Recently, the **National Conference of Commissioners on Uniform State Laws** (NCCUSL) brought clarity to questions about just how states should move forward by approving the *Uniform Electronic Legal Material Act* (UELMA)[1]. The Act requires that official electronic legal material be:

- ***Authenticated***, by providing a method to determine that it is unaltered.
- ***Preserved***, either in electronic or print form.
- ***Accessible***, for use by the public on a permanent basis.

This brief provides background to UELMA, explores the concepts behind authenticated electronic materials, and identifies what it will take to create, maintain, and make available official electronic legal material. It also highlights the solution implemented by the U.S. Government Printing Office as an instructive case for states contemplating creating official electronic legal material.

These aspects of the uniform model law underscore the perplexing and challenging administrative, policy, and technical issues for state legislatures, none of whom have yet passed a version of UELMA.

Entering the world of official electronic legal materials raises issues that are complex but not unique. In building their own plans and capabilities, state legislatures can utilize the experience and knowledge gathered in the electronic signatures, electronic records preservation, open government, and public value fields. To do so, policy makers, legislators, and CIOs will have to consider the following:

- ***Technical challenges*** of implementing records authentication and preservation technologies that in the past have been considered too expensive or difficult to implement.
- ***Managerial challenges*** of implementing processes and standards to ensure records preservation.

- ***Fiscal challenges*** of making long-term commitments of resources during an era when such resources are very scarce.
- ***Policy and political challenges*** of ensuring of UELMA-based laws take into consideration the context of their state and are readily implementable.

RECOMMENDATIONS

As state legislatures and policy makers begin to consider an UELMA-based law, we recommend the following five steps to guide them through a comprehensive planning process focused on identifying and analyzing the challenges of implementing official electronic legal materials in their state and developing action plans for addressing the issues raised.

- Find out how publication of and public access to electronic legal materials are presently handled within your state.
- Assess the readiness of your state's IT communities to address the challenges of authentic legal material.
- Assess the public value of making official legal materials available.
- Assess the costs and potential cost savings of implementing official electronic legal materials.
- Identify the policy, management, and technical issues of implementing official electronic legal materials and examine potential solutions or ways of addressing these issues in the context of your state.

To produce official legal materials in electronic form, states must address the critical issues of record authenticity, integrity, and preservation.

History
of Electronic Records and Signature Laws

Over eleven years ago, individual state legislatures began establishing a legal framework to give electronic transactions conducted through the use of electronic records and signatures the same force of law as those conducted by non-electronic means. The early adopting states initially enacted digital signature laws that required the use of robust technologies to ensure the authenticity and integrity of electronic signatures and technologies. This approach changed when NCCUSL issued the technology neutral *Uniform Electronic Transactions Act* (UETA)[2]. UETA allowed contracting parties to use any approach to electronic signing they saw fit. UETA did not provide guidance on what technologies or approaches would best serve different types of electronic transactions and was also silent on issues of authenticity, integrity, and preservation.

Since it was issued, most states have looked to UETA as their model for electronic records and signature laws. State efforts were accelerated and nationalized when in 2000 the U.S. Congress enacted the *Electronic Signatures in Global and National Commerce Act* (ESIGN)[3]. ESIGN was designed to facilitate the use of electronic records and electronic signatures in interstate and foreign commerce by ensuring the validity and legal effect of contracts entered electronically. ESIGN's general intent was that a contract or signature "may not be denied legal effect, validity, or enforceability solely because it is in electronic form." This made electronic signatures and records the legal equivalent of their paper counterparts, and therefore subject to the same legal scrutiny of electronic records authenticity that applies to paper.

ESIGN limited states' ability to modify, limit, or supersede ESIGN's substantive provisions unless the state adopted UETA as approved and recommended for enactment by the NCCUSL in 1999. Alternatively, states could adopt a law that did not conflict with ESIGN's major provisions by giving greater legal validity to a specific electronic record or signature technology[4]. All other state electronic records and

DEFINITIONS

Primary legal material includes state administrative codes and registers, state statutes and session laws, and state high and intermediate appellate court opinions.

Authentic text is one whose content has been verified by a government entity to be complete and unaltered when compared to the version the content originator approved or published. An authentic text is able to be authenticated, which means it can be validated.

Authentication of electronic documents is a process involving computer technology to verify a text as authentic that may involve digital signatures or digital watermarks. Authentication also involves proving chain of custody relating to trustworthy archival procedures and that appropriate processes and procedures were used to handle, protect, and preserve relevant data.

Chain of custody concerns the record of sequential steps in the handling of electronic materials to prove it has not been changed or modified since it left its point of origin. The chain typically begins with a duly certified text from the documents creating entity. Chain of custody information is basic evidence of procedures for data handling that would contribute to online resources being accepted as authenticate.

An ***official version*** of regulatory materials, session laws, statutes, or court opinions is one that has been governmentally mandated or approved by statute or rule. It might be produced by the government, but does not have to be.

Permanent public access is a policy and practice ensuring applicable government information is preserved for current, continuous and future public access.

Like UETA, ESIGN sidestepped the issues of authenticity, integrity, and preservation of electronic records and signatures, which are key to creating authentic primary legal materials and were issues of concern to some legislatures before the issuance of UETA and passage of ESIGN.

signature laws were threatened with pre-emption. Passage of UETA was the course of least resistance for states and today 47 states have adopted UETA-based laws.

The framework established by ESIGN affirmed the direction set by UETA-based state laws. It was oriented toward facilitating electronic commerce and e-government, was strongly technology neutral, and provided limited guidance on what technologies would best serve different types of transactions and electronic records. Like UETA, ESIGN sidestepped the issues of authenticity, integrity, and preservation of electronic records and signatures, which are key to creating authentic primary legal materials and were issues of concern to some legislatures before the issuance of UETA and passage of ESIGN.

These issues of authenticity, integrity, and preservation have now re-emerged after being off the radar screen of many state legislatures and policy makers. This re-emergence has been driven by open government initiatives and the cost saving implications of making primary legal resources such as state administrative codes and registers, state statutes, and session laws available online in a form or format that would be deemed *official* and could be used for the same purposes as official print versions. Across the U.S., state legislatures are now passing specific laws authorizing the use of online versions of legal materials as official versions and some states have dropped the issuance of printed versions as a cost saving measure.

NATIONAL CONFERENCE OF COMMISSIONERS ON UNIFORM STATE LAWS

The **National Conference of Commissioners on Uniform State Laws** (NCCUSL) has worked for the uniformity of state laws since 1892. It is a nonprofit organization that provides states with non-partisan, well-conceived and well-drafted legislation that brings clarity and stability to critical areas of state statutory law.

The state uniform law commissioners come together as the **Uniform Law Commission** for one purpose—to study and review the law of the states to determine which areas of law should be uniform. The commissioners promote the principle of uniformity by drafting and proposing specific statutes in areas of the law where uniformity between the states is desirable. It must be emphasized that the ULC can only propose—no uniform law is effective until a state legislature adopts it.

More information> www.nccusl.org

Current State
of Official Electronic Primary Legal Materials

TRACKING STATE PROGRESS

The progress state governments are making towards producing official electronic primary legal material has been tracked and documented by the American Association of Law Libraries (AALL) in comprehensive surveys conducted in 2007 and 2009/10[5]. These surveys have found that many states are no longer printing official legal resources and are substituting instead with online official legal sources. By 2010, fourteen states had moved in this direction. An equal number of states have deemed as official one or more of their online primary legal resources. However, very few states have addressed the issue of the authenticity of online primary legal resources and even fewer afford ready authentication by standard methods. Twelve states legally provide for permanent public access (PPA) to one or more of their online primary legal resources.

According to AALL, states have also not acknowledged important needs of citizens and law researchers seeking government information; they have not been sufficiently deliberate in their policies and practices. Citizens and researchers seeking electronic versions' of legal material require that it be accurate, complete, and current without reservations. State governments, however, extensively use disclaimers (even for materials deemed "official") when publishing electronically. Users also face discrepancies in titling and formatting between print and electronic versions as well as unclear or infrequent update cycles, which further undercuts their trust in electronic legal materials.

There are three points that should be stressed concerning these findings. First, as noted in the survey reports, the term official has little significance if the document can not be authenticated. Therefore, the fact that states have not fully implemented standard digital authentication methods is very significant. Second, although a number of states have committed to providing permanent public access from a legal or policy perspective, the survey did not provide any evidence that states have dedicated any significant resources to accomplish long-term preservation. This appears to indicate that most states that have committed to permanent public access may not have taken the steps necessary to deliver on this commitment. Third, it is unclear if states have moved closer to acknowledging and addressing the needs of citizens and law researchers since the original 2007 survey. We have yet to find any significant progress by states in this area.

Most states that have committed to permanent public access have not fully investigated or dedicated the resources necessary to deliver on this commitment.

TECHNOLOGY CHALLENGES

The hesitancy of states to embrace electronic legal document authentication is not due to a lack of potential solutions and technologies. However, most solutions involve the use of encryption technologies associated with Public Key Infrastructure (PKI). PKI can be used to create robust digital signatures to authenticate the document being signed as well as the signer's identity.

In the past, public key encryption required a relatively complex infrastructure and raised difficult issues of distributing and managing cryptographic keys as well as a myriad of policy and legal issues. A number of states explored establishing PKIs in the early 2000s but had only limited success given the cost and management issues[6]. However, the U.S. federal government has since established a robust PKI in partnership with large PKI providers. Recently, public key-like solutions have been developed that do not necessarily require the type of infrastructure required for a full blown PKI. These solutions have been

integrated into popular document products like Adobe Acrobat[7]. However, adoption of such solutions for signature and document authentication appears to be very slow at the state level.

DEFINING TRUSTED REPOSITORIES

The ability to authenticate electronic documents is just the tip of the iceberg of producing official electronic primary legal material. An equally important step is what we can refer to as the *backend management* of these materials to ensure their chain of custody and integrity from transmittal from their originating entity to their management in a long-term repository. Chain of custody requires the maintenance of clear policies and documentation of the materials' transfer or movement. It also demands that the integrity of these materials is maintained while they are stored in what can be deemed a *trusted repository*. Serendipitously, the requirements to maintain the chain of custody and integrity of digital legal materials are essentially the same as those required to preserve those documents.

Since the early 2000s, what constitutes a trusted repository for archival preservation purposes has been more clearly defined and a set of generally accepted standards developed[8]. An *Open Archival Information System* (OAIS) is a framework for a repository consisting of an organization of people and systems, that has accepted the responsibility to preserve information and make it available for a designated community. It has a particular focus on digital information. An OAIS archive maintains information that has been deemed to need *long term preservation*, even if the archives itself is not permanent. *Long term* is long enough to be concerned with the impacts of changing technologies, including support for new media and data formats, or with a changing user community. *Long term* may extend indefinitely.

The **Research Libraries Group** (RLG) further articulated the OAIS framework by developing *Trusted Digital Repositories: Attributes and Responsibilities*[9], a set of standards that could serve as a basis for certifying a repository as an OAIS. RLG, working with the **National Archives and Records Administration**, further concretized OAIS by developing a *Trustworthy Repositories Audit and & Certification: Criteria and Checklist* (TRAC Checklist)[10]. The RLG-NARA standard is comprehensive covering organizational infrastructure, digital object management, and technologies, technical infrastructure, and security.

Legislatures do not act quickly, especially on changes that would impact a state's legal system. Such changes require careful study lest states are left dealing with unintended consequences.

THE CASE OF THE U.S. GOVERNMENT PRINTING OFFICE

The technologies and standards needed to create and make available official primary legal materials that can be authenticated have been implemented by the U.S. **Government Printing Office** (GPO) for comparable materials. Even though the federal GPO has a dedicated mission to provide authentic government materials to the public and the resources to carry out this mission, its approach is instructive to state legislatures contemplating creating *official* electronic legal material[11].

GPO defines authentic content as "content that is verified by GPO to be complete and unaltered when compared to the version approved or published by the Content Originator." It has created a process for information's authenticity that assures users that they can trust the source and content of material provided. GPO's **Federal Digital System** (FDsys) preserves digital content independent of specific hardware

The Federal Digital System (FDsys) provides permanent digital access to authoritative documents that have been electronically signed by the public printer.

or software. It conforms to all TRAC Checklist's technical requirements and implements restrictions on access to content. Users cannot alter content but can only see on GPO's website a copy taken from a preservation master. FDsys security only allows preservation specialists access to content in the archive, ensuring content has not been altered. FDsys periodically checks content for corruption or changes, for the presence of an unauthorized content, or the absence of an expected content file[12]. GPO ensures and documents chain of custody by collecting and providing users with information about each significant event in the content's lifecycle including what occurred, who triggered the event, what specific files were affected, and the event's date and time.

GPO's strategy to ensure the continued usability of content is to transfer data to a more current file format. This does not always mean that the content is identical to the original, but it does mean that the content's significant properties have been preserved. GPO ensures that content has not been changed or destroyed without authorization (content integrity) using the following tools:

U.S. GOVERNMENT PRINTING OFFICE DEFINITION OF AUTHENTIC CONTENT

The Government Printing Office (GPO) defines **authentic content** as:

"Content that is verified by GPO to be complete and unaltered when compared to the version approved or published by the Content Originator."

For a complete list of authentication terms and their corresponding definitions used by GPO, go to:

www.gpo.gov/pdfs/authentication/Authentication%20Definitions.pdf

- ***Cryptographic Hash Values*** are provided for every publicly-accessible file. Users can use the hash values and publicly-available tools to check that content has not been altered.

- ***Digital Signatures*** are applied to PDF documents, the most common format used for public access, to provide assurance that they were not altered since they were downloaded from GPO's websites. A user receiving a GPO published PDF from another source can use the digital signature to determine if content has been altered and to verify that GPO was the material's source.

Implementation Challenges

With a uniform law, appropriate technologies, and a working model (GPO), why haven't states quickly moved forward to fully embrace official digital legal materials? The answer to this question is complex, combining both obvious and obscure explanations.

The implementation of official digital legal materials requires legislative action. Legislatures do not act quickly especially on changes that would impact a state's legal system. Such changes require careful study lest states are left dealing with unintended consequences. Additionally, no state legislature has yet passed UELMA. Legislatures are understandably risk adverse and feel much more comfortable if they can see how the implementation of official digital legal materials has worked in other states, especially states they see as comparable.

A complicating factor in many states is that many types of official legal materials are published, and in some cases codified, by private firms under contract with the state. Many of these relationships are long term going back over a hundred years. How the publication of official digital legal material would affect these publishers is unclear. However, UELMA requires that a state entity be designated as the publisher of each official electronic legal document.

Another factor is cost. Assumed cost savings has been a driver for making electronic legal materials available. However, cost is a two-edged sword. Indeed it is not an expensive proposition to create PDFs of laws, regulations, and other legal material and make them available on a website; but providing authentic official legal materials, maintaining them, and insuring their permanent preservation will involve the cost of new systems, processes, and technologies. The cost implications have not yet been fully explored and state legislatures may be very hesitant to move forward until they are.

Additionally, some of the technologies involved such as PKI-based digital signatures were rejected by many states as too costly and complex to implement. This impression remains despite the emergence of less complex types of digital signature implementations.

All of this leaves state legislatures with many more unanswered questions. Will official electronic legal material add or reduce the costs of making these materials available? How long will it take to recover the costs of implementing official legal materials?

The implications of permanently preserving official digital legal materials raises even more red flags from a cost perspective. The first step in achieving this requirement as well as establishing chain of custody would be to develop and maintain a system or repository that meets TRAC or OAIS standards. This would require states to commit dedicated resources to preserving electronic legal material in perpetuity. Few states have provided their archival and library institutions with the resources to adequately preserve existing permanent digital information. Moreover, the costs of providing permanent public access, including the ability to authenticate documents, have not been adequately explored and analyzed.

All of this leaves state legislatures with many unanswered questions. Will official electronic legal material add or reduce the costs of making these materials available? How long will it take to recover the costs of implementing official legal materials? Cost recovery models could include charging for copies of or access to authenticated electronic legal material. UELMA is silent on this issue, but states do have the option to charge for certain types of access (e.g., providing certified authentic copies to law firms). However,

each state will need to discover for themselves which cost recovery models make sense and are politically feasible.

Also related to cost is the issue of the public value of authentic electronic legal material. States have assumed there is value in making this material available but have not conducted systematic assessments of who may benefit from the availability of such material. Such an assessment would likely reveal that certain segments of the using public would greatly benefit, while the value to the general public might be marginal.

For example, it may be found that the needs of most users would be met by simple PDF copies of legal material, while the legal community would get a greater economic benefit from having access to certified authentic electronic legal materials. There may also be losers in this equation. Legal publishing firms such as Westlaw and Lexis/Nexis may find that their services are less valuable if authenticated electronic legal materials are publicly available. A public value analysis would be extremely helpful in developing cost recovery models as well as making legislative arguments for moving ahead with UELMA-type legislation.

Also related to cost is the issue of the public value of authentic electronic legal material. States have assumed there is value in making this material available but have not conducted systematic assessments of who may benefit from the availability of such material.

RECOMMENDATIONS

As state legislatures and policy makers begin to consider an UELMA-based law, we recommend the following five steps to guide them through a comprehensive planning process focused on identifying and analyzing the challenges of implementing official electronic legal materials in their state and developing action plans for addressing the issues raised.

Find out how the publication and public access to electronic legal materials are presently handled within your state.

The present approach to publishing and providing access to primary legal material in most states is very complex. In addition, approaches likely vary between branches of government and perhaps even agencies. Legislatures need to have a clear idea of what is presently happening in their state. Are there contracts with third party publishers and legal requirements affecting how materials are published? What materials are presently available in electronic form? What materials are being made available to the public electronically? What formats and technologies are being used? Is the public presently being charged for certain types of access?

Assess the readiness of your state's IT communities to address the challenge of authentic electronic legal material.

Legislatures need to engage their state's CIO and IT communities around the question of readiness. Is this community comfortable or familiar with the technologies and standards required to implement authentic electronic legal materials? Are there barriers to implementation or technical issues that the legislature is not aware of? What role can the state's CIO play in implementing an UELMA-type law?

Assess the public value of making official legal materials available.

The American Association of Law Libraries study noted that states have not acknowledged the important needs of citizens and law researchers seeking government information. Legislatures need to determine the needs in their respective states and assess the value of authentic electronic legal materials to the range of relevant stakeholders. More specifically, they need to systematically examine how authentic electronic legal material matters and to whom.

Assess the costs and potential cost savings of implementing official electronic legal materials.

It is essential that state legislatures have full and accurate information on the potential costs of providing authentic official legal materials, maintaining them, ensuring their permanent preservation, and providing permanent access to them before implementing an UELMA-based law. State legislatures must have answers to questions such as: What are the short and long-term costs of implementing official electronic legal material? Will implementation add or reduce the cost of making these materials available? How long will it take to recover the cost of implementing official legal materials?

Identify the policy, management, and technical issues of implementing official electronic legal materials and discuss potential solutions or ways of addressing these issues in the context of your state.

Implementing official electronic legal materials will require more than the passage of a uniform law or even the provisioning of adequate resources. There are a host of practical administrative and technical considerations that must be addressed within the context of each state. What entity will administer the law and oversee implementation? What technologies and products will be selected? What repositories will be used to maintain permanent electronic legal material? What entity(ies) will provide public access? Will the same entity be responsible for preservation and access? Will existing entities such as the state archives or state library have a role? Will there be a centralized or decentralized approach to providing access? Are there constitutional issues in a centralized approach that includes the three branches of government (executive, legislative, and judiciary)?

ENDNOTES

[1]See UELMA's text see: http://www.uniformlaws.org/Shared/Docs/AM2011_Prestyle%20Finals/UELMA_PreStyleFinal_Jul11.pdf.

[2]See http://www.ncsl.org/default.aspx?tabid=13484 for links to the text of the various state statutes based on UETA.

[3]Pub. L. No. 106-229, 14 Stat. 464 ESIGN contained an explicit threat that states that did not adopt UETA or substantially similar electronic signature and records law could have their statute pre-empted by the federal government.

[4]The types of modifications states were interested in were related to not allowing e-signatures and records for certain transactions (e.g., real property transactions) or increasing the consumer protections in their e-signature laws. ESIGN also required states adopting alternative procedures or requirements to specifically reference ESIGN.

[5]*State-by-State Report on Authentication of Online Legal Resources Report*, American Association of Law Libraries, March 2007 and *2009-2010 Updates to the State-by-State Update Report on Authentication of Online Legal Resources Report*, American Association of Law Libraries, February 2010. For copies of these reports see http://www.aallnet.org/main-menu/Advocacy/aallwash/summit.

[6]Illinois and Washington were two states that attempted to implement PKI but even as early 2003 the lack of interest in the technology on the part of state government was noted. See "Igniting PKI," *Government Technology*, July 29, 2003.

[7]For a description of Adobe's approach to digital signatures see http://www.adobe.com/security/digsig.html.

[8]These standards are based on the *Reference Model for an Open Archival Information System* (OAIS). OAIS was originally developed for space data by Consultative Committee for Space Data Systems[1] but has since been adopted as an International Standards Organization (ISO) standard ISO 14721:2003. Further credibility was given to OAIS when UNESCO published its *Guidelines for the Preservation of Digital Heritage* using OAIS as the basis for the attributes of a digital repository and stated:

- The OAIS Reference Model is the most successful attempt to define both a conceptual model for managing digital materials of enduring value, and a vocabulary with which to discuss it.
- Anyone contemplating a responsibility for managing digital materials should seek to understand the concepts articulated in the Reference Model itself.

[9]This document can be found at http://www.oclc.org/research/activities/past/rlg/trustedrep/repositories.pdf.

[10]The TRAC Checklist can be found at http://www.crl.edu/sites/default/files/attachments/pages/trac_0.pdf. TRAC is the basis of the soon to be finalized International Standards Organization (ISO) standard Trusted Digital Repositories (TDR) (ISO 16363).

[11]More information on the GPO's approach to document authentication and preservation can be found at http://www.gpoaccess.gov/authentication/.

[12]This polling uses a SHA-256 cryptographic hash value from the content and compares it with the value recorded at the time content is received by the GPO.

About

THE CENTER FOR TECHNOLOGY IN GOVERNMENT

The mission of the Center for Technology in Government (CTG) at the University at Albany/SUNY is to foster public sector innovation, enhance capability, generate public value, and support good governance. We carry out this mission through applied research, knowledge sharing, and collaborative problem solving at the intersection of policy, management, and technology.

The results generated by each CTG project add to a growing knowledge base designed to support the work of both government professionals and academic researchers. Our guides, reports, and tools are freely available on our publications page: www.ctg.albany.edu/publications.

THE AUTHOR

Alan S. Kowlowitz
Government Fellow

Retired from state service, Alan has brought his 32 years of experience with the New York State Archives and the Office for Technology (OFT) to CTG as a Government Fellow. Alan is applying his expertise and deep knowledge of NYS government and its critical challenges to identifying key themes across past projects, taking the lead on repackaging past reports, and researching related topics to help address emerging issues in digital government.

During his tenure at both the State Archives and OFT, Alan was involved with CTG projects in various capacities. While at the State Archives he co-authored and was principle State Archives participant in the Models for Action project. While at OFT he served on the Advisory Group for Gateways project and cooperated with CTG on many other e-Government initiatives.

Alan was on the staff of the State Archives between 1979-1999 where he helped establish and then manage that institution's electronic records program. While at the State Archives, he also assisted OFT in drafting New York State's Electronic Signatures and Records Act (ESRA). Between 2000-2004, Alan served on the OFT team that developed the ESRA regulations and guidelines and established the State's e-Government/e-Commerce Program. During his tenure with both the State Archives and OFT, Alan has had extensive experience working with local governments on electronic records and e-government issues.

From 2004-2010, Alan served in OFT's Security and Risk Management Office where he developed organizational security policies and standards covering areas from Identity and Access Management to wireless networks as well as overseeing the agency's Business Continuity Program. Alan served on the NYS CIO Council's Identity and Access Management Work Group, where he developed New York State's Identity Trust Model and Enterprise Identity Management (EIM) Governance Authority policy. Before leaving OFT, Alan completed a major project to revise the agency's security policies and standards to bring them into line with International Standard Organizations security standards. He is a Certified Information Security Manager (CISM).

UNIVERSITY AT ALBANY

State University of New York

Center for Technology in Government
187 Wolf Road, Suite 301
Albany, NY 12205

PH: 518-442-3892
FAX: 518-442-3886
EMAIL: info@ctg.albany.edu
www.ctg.albany.edu