2011

Authenticating Digital Government Information

Timothy L. Coggins
University of Richmond, tcoggins@richmond.edu

Recommended Citation
Timothy L. Coggins & Sarah G. Holterhoff, *Authenticating Digital Government Information, in* Government Information Management in the 21st Century (Peggy Garvin ed., 2011).

CHAPTER 9

Authenticating Digital Government Information

TIMOTHY L. COGGINS AND SARAH G. HOLTERHOFF[1]

> Instead of relying on the voodoo information taken from the Internet, Plaintiff must hunt for hard copy back-up documentation in admissible form ....[2]

Introduction

The quotation above from *St. Clair v. Johnny's Oyster & Shrimp, Inc.*, a 1999 US federal district court case, captures a perception of the trustworthiness of digital information that over ten years later is, in many instances, still uncomfortably close to reality. It raises two important questions with which governments providing online information and users of that information must grapple: Is digital government information reliable and trustworthy? Has the government entity providing digital information online taken the care necessary to ensure its authenticity?

This chapter presents a historical perspective of authenticity of government information, provides definitions of significant terms and phrases related to authentication, offers basic descriptions of some methods used to ensure authenticity of government information, and identifies some examples of what is happening at the federal and state level in the United States and in other countries to address these important questions. It also suggests some strategies and appropriate steps toward the goal of an affirmative answer to the two questions under consideration. The authors are both law librarians, and the examples used in this chapter are government-issued legal information. However, the principles, processes, and concepts identified in this chapter should be applied to all types of digital government information.[3]

1 The authors thank Matthew R. Farley (J.D., 2010, University of Richmond School of Law), Reference Intern at the University of Richmond School of Law Library, for his valuable research assistance.

2 *St. Clair v. Johnny's Oyster & Shrimp, Inc.*, 76 F. Supp. 2d 773, 775 (S.D. Tex. 1999).

3 Authentication of government-issued information is a complex issue that is difficult to address thoroughly in this chapter; therefore, a list of suggested readings and resources appears at the end of the chapter for those who would like to learn more about authentication.

Historical Perspective of Authenticity and the Transition to Digital Information

Throughout the history of the written word, an important issue with recorded information has been its integrity, both the accuracy and the completeness of the content. Painstaking copying of manuscripts began in medieval monasteries and continued in universities, with care taken to maintain uniformity and to avoid corruption of the text. Royal monarchs confirmed the authenticity of their official edicts, orders, decrees, and declarations by stamping them with a special seal. The advent of the printing press made the accurate reproduction of information content much easier to achieve. When early printers needed to provide a warranty of reliability for their work and to protect it from fraud, they added unique printers' marks to their publications. In the developing print culture, a fundamental factor ensuring the integrity of documents was the fixed nature of the print medium.

With the transition to the age of digital information,[4] particularly information made available on websites, the integrity of recorded information surfaces once again as an issue. In recent years national and state governments have turned increasingly to digital format for their official publications. Government information can be created, updated, and distributed in digital format with greater speed and efficiency than is possible with print format. Users of government information have enjoyed expanded access and greater ease of use with digital formats. However, the change to a digital environment highlights a new set of information management issues. Concern has been growing in some quarters about the substitution of digital sources for print ones without proper care being taken to ensure the integrity of the digital versions and to preserve the content. Guarantees of authenticity such as seals, printers' marks, and the fixed nature of the print medium do not transfer to the digital age. With an explosion in the quantity and accessibility of information, the need to confirm its integrity, for legal and research purposes in particular, looms as a major issue.

Many have raised concerns about digital government publications being vulnerable to alteration or corruption of the content accidentally or maliciously, as well as the effect that alterations and corruption may have on national security. The flexibility that the digital format provides is also a fundamental reason for concern. The fluid character and elastic, changeable nature of digital media require technological solutions to protect and preserve the integrity of the information and new types of seals or marks to signify authenticity to users of the information. In the prefatory note to a uniform law that the National Conference of Commissioners of Uniform State Laws (NCCUSL) is drafting about authentication, the Drafting Committee highlights this issue:

> Electronic legal information moves from its originating computer through a series of other computers or servers until it eventually reaches the individual consumer. The information is susceptible to being altered, whether accidentally or maliciously, at each transfer. Any such alterations are virtually undetectable. A major issue raised by the

4 When referring to information in computerized or online format, the most technically accurate and precise term is "digital." However, the term "electronic" also is commonly used to indicate the same format. This chapter will generally use the former of the terms; some of the cited sources employ the latter in the same context.

change to an electronic en
by consumers is trustworth

More about the draft uniform

With the move from pap
technology and best practic
the authenticity of their dig
and to preserve the integrity
information has many benef
be safeguarded and its pres
government information mu

Why does authenticatio
the official disseminator of f
years and more recently in
use of electronic documents
digital technology makes suc
identical versions that can b

In particular, legal infor
is at risk in the digital age.
documents are official and au
been printed (and sometime
text is easily verifiable, and a
legal information typically e
with that redundancy provic
preserved. In contrast, authe
inherently susceptible to co
they are able to be authenti
needs to be authenticated
version, and measures for its

Librarians, particularly
of attention to authenticat
publications with digital ver
authentication and preserva
and other countries have beg
their national and state gove

Definitions

For a clear understanding of
key words and phrases are in

Authentication is the pro
alterations in the document

5 National Conference of Commi
Authentication and Preservation of Sta

6 Available at http://www.gpoacces

st Century

e Transition to

rtant issue with recorded
ompleteness of the content.
nasteries and continued in
void corruption of the text.
edicts, orders, decrees, and
of the printing press made
ier to achieve. When early
work and to protect it from
ns. In the developing print
ments was the fixed nature

ticularly information made
surfaces once again as an
rned increasingly to digital
n can be created, updated,
iency than is possible with
yed expanded access and
e to a digital environment
ncern has been growing in
t ones without proper care
d to preserve the content.
nd the fixed nature of the
losion in the quantity and
ity, for legal and research

blications being vulnerable
ciously, as well as the effect
ty. The flexibility that the
ncern. The fluid character
logical solutions to protect
of seals or marks to signify
ote to a uniform law that
Laws (NCCUSL) is drafting
issue:

puter through a series of
ndividual consumer. The
ly or maliciously, at each
major issue raised by the

hnically accurate and precise term is
e format. This chapter will generally
context.

change to an electronic environment, therefore, is whether the information consulted by consumers is trustworthy, or authentic.[5]

More about the draft uniform law will appear later in this chapter.

With the move from paper to digital formats, it is necessary for governments to adopt technology and best practices and to adhere to standards to ensure a level of trust in the authenticity of their digital documents, similar to that enjoyed by the print format, and to preserve the integrity of the information. While digital provision of government information has many benefits, the authenticity of content provided in this format must be safeguarded and its preservation guaranteed. The concept of authentic and reliable government information must be redefined for the digital age.

Why does authentication matter? According to the US Government Printing Office, the official disseminator of federal government information in print format for over 150 years and more recently in digital format as well, "In the 21st century, the increasing use of electronic documents poses special challenges in verifying authenticity, because digital technology makes such documents easy to alter or copy, leading to multiple, non-identical versions that can be used in unauthorized or illegitimate ways."[6]

In particular, legal information that is understood to be both official and authentic is at risk in the digital age. When using print legal materials, it is usually clear that the documents are official and authentic because of the fixed nature of the content once it has been printed (and sometimes because of a seal, stamp, or official binding or format). The text is easily verifiable, and any changes would be readily detectible. Additionally, print legal information typically exists in multiple, identical copies held in various locations, with that redundancy providing relative assurance that the authoritative content will be preserved. In contrast, authenticity is much less obvious with digital sources. They are inherently susceptible to corruption or tampering, and they are not trustworthy unless they are able to be authenticated using encryption-based methods. Digital information needs to be authenticated and verified to be the accurate, complete, and unaltered version, and measures for its long-term preservation must be taken.

Librarians, particularly law librarians, are increasingly concerned about the lack of attention to authentication shown by most governments as they replace print publications with digital versions. The American Association of Law Libraries raised the authentication and preservation issues over a decade ago, and law librarians in the US and other countries have begun efforts to bring the matter to the attention of officials of their national and state governments.

Definitions

For a clear understanding of authentication and related issues, the definitions of certain key words and phrases are important.

Authentication is the process of verifying that a document is authentic and that no alterations in the document occurred in its route from the producer of the document to

5 National Conference of Commissioners on Uniform State Laws (Uniform Law Commission), Prefatory Note, Authentication and Preservation of State Electronic Legal Materials Act (2010).

6 Available at http://www.gpoaccess.gov/authentication/index.html.

the recipient. Others describe authentication as validation of a user, computer, or some digital object to ensure that it is what it claims to be.

Authenticity describes the quality of being authentic or of established authority for truth and correctness. It typically refers to the quality and credibility of the digital document and covers issues such as genuineness, legitimacy, undisputed credibility, believability, and trustworthiness.

Certification is the process that is used to ensure that a digital object is authentically the content issued by the author or the issuer. A *certificate* is a mark of veracity that conveys certification information to users and is in some way joined to the object itself.

Chain of custody (confidence or responsibility) refers to the verifiable record of the sequential steps in the handling of a digital document, usually beginning with a certified original text. Chain of custody normally utilizes certification and digital signatures.

Digital signature and *electronic signature* are slightly different terms. An *electronic signature* is a generic, technology neutral term that refers to the many different ways that a person can sign an electronic record. Electronic signatures include signatures such as those typed at the end of an email message, a secret code or PIN, or a unique biometrics-based identifier such as a finger print. A *digital signature* is an electronic symbol, sound, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record. The digital signature is used to authenticate the identity of the sender or of the signer of a document and to ensure the integrity of the original content of a document.

Digital (or electronic) document is data that is recorded or stored on any medium (technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities) in or by a computer system or other similar device and that can be read or perceived by a person or a computer system or other similar device. The words "digital" and "electronic" are often used interchangeably.

Official version is a document either in paper format or disseminated digitally that is governmentally mandated or approved by statute or rule by authorities. Digital and paper versions of a document may be equal in status. Frequently today, however, the paper version may be the only version that is designated as official. In some instances, the digital version may be the only official version. In other situations, there may not be an official version because a court, for example, might elect to discontinue publishing its own reporter for its decisions and rely instead on an unofficial commercial version.

Permanent public access refers to a government policy and practice that ensures applicable government information is preserved for current, continuous, and future public access.

Prima facie evidence of the law denotes evidence in common law jurisdictions that would be sufficient to prove a particular proposition or fact unless that evidence is rebutted. Official versions of documents are *prima facie* evidence of the law in most jurisdictions. Section 5 of the draft NCCUSL uniform act indicates that "[e]lectronic legal material authenticated under Section 4 [of this Act] is presumed to be a true and correct copy of the legal material."

Reliability is a broader term that covers concepts such as authoritative character, official status, and integrity.

Definitions of other terms, including public key infrastructure, biometrics, and cryptography, appear in the next section of this chapter.

Use of Authenticati

The purpose of authentica
integrity, reliability, and tru
is what it purports to be—
actually taken the necessa
methods used to ensure au
nearly unintelligible for th
authentication that is famili
that he or she claims to be—

Here are some commor
ensure that an individual is

PASSWORDS

Passwords, the most comm
require a user to remember
to a desired resource or se
technology include the fr
unchanged for long periods
of overly simplistic passwo
are at risk of falling prey t
play an important role in
with other technologies for

TOKENS

Token devices such as magn
USB keys typically last long
They provide little protect
possession of these object
Tokens are more effective
or a password.

PUBLIC KEY INFRASTRUC

Public key infrastructure
certificates, which are often
authority acts as a third-
integrity of the content. T
by a Web browser during a
applications encounter the
the issuing certificate or c
the website owner. Digital
highly secure, encrypted i
the sender) and public key
text. While PKI has seen v

Use of Authentication Technology: A Basic Example

The purpose of authentication as it relates to government information—to ensure the integrity, reliability, and trustworthiness of a document and to confirm that a document is what it purports to be—is widely understood, even if many governments have not actually taken the necessary steps to authenticate their documents. The technological methods used to ensure authenticity, however, are not as well understood and may be nearly unintelligible for those who lack scientific or computer expertise. An example of authentication that is familiar to everyone—helping ensure that an individual is the person that he or she claims to be—provides a good illustration of authentication generally.

Here are some commonly used types of user authentication technology that help to ensure that an individual is the person that he or she claims to be.

PASSWORDS

Passwords, the most common and least expensive form of authentication technology, require a user to remember a string of characters and enter this information to gain access to a desired resource or service. Problems with passwords as a form of authentication technology include the frequent sharing of passwords, the tendency to leave them unchanged for long periods, the reuse of a password across multiple accounts, and the use of overly simplistic passwords. Owners of passwords with one or more of these problems are at risk of falling prey to novice identity thieves or simple hacking tools. Passwords play an important role in user authentication, but they should be used in conjunction with other technologies for adequate security.

TOKENS

Token devices such as magnetic strips (credit cards), smart cards, identification cards, and USB keys typically last longer than passwords and are more difficult to hack or reproduce. They provide little protection, however, if lost or stolen. Similar to passwords, simple possession of these objects often serves as the only means to distinguish the owner. Tokens are more effective if they are combined with something else such as a PIN code or a password.

PUBLIC KEY INFRASTRUCTURE

Public key infrastructure (PKI) refers to authentication technology that uses digital certificates, which are often issued by an independent certificate authority. The certificate authority acts as a third-party reference regarding the identity of the owner or the integrity of the content. The certificate can be attached to email messages or references by a Web browser during an e-commerce transaction as a means of identification. When applications encounter these certificates, the origin can be verified by inquiring back to the issuing certificate or certification authority to ensure the identity of the sender or the website owner. Digital certificates also provide a means to allow users to exchange highly secure, encrypted information using a combination of a private key (owned by the sender) and public key (freely shared with recipients) to encrypt and decrypt message text. While PKI has seen very limited use in the marketplace as an application to affirm

that an individual is, in fact, the person that he or she claims to be, it is viewed as essential for the authentication of digital government information.

BIOMETRICS

Biometric devices examine unique physical characteristics to differentiate one person from another. Biometric verification, using fingerprints, irises, voice patterns, or facial patterns, is considered to be highly secure because these physical characteristics are unique to each individual and cannot be easily duplicated. The reliability of biometrics can be strengthened further by combining several types of recognition, known as multiple biometrics, and/or requiring users to enter a PIN code in order to provide a unique self-identification.

Applying Authentication Technology to Digital Government Information

To authenticate digital government information, governments are using some of the same types of technology used in user authentication, as well as other technology such as digital certificates and certification, cryptography, digital signatures, and seals of authenticity. The primary purpose of these technologies is to ensure the integrity of the content and to give reasonable assurance to users of the information that a document is what it purports to be (reliability) and that it can be used and cited by a person for what it claims to be (trustworthiness). Following are brief descriptions of these commonly used types of technology.

PUBLIC KEY INFRASTRUCTURE

Public key infrastructure is a system of hardware, software, policies, and people that provides a range of security assurances, including authentication, data integrity, data confidentiality, and non-repudiation. PKIs provide a desired level of trust using public key-based cryptographic techniques to generate and manage electronic certificates.

Certificates link one individual or entity to a public key. The public key validates the information provided by the individual or entity or facilitates data encryption. Certificates verify digital signatures (providing authentication and data integrity) and facilitate data encryption (providing confidentiality). If designed and implemented correctly, a PKI can ensure that a given digital signature is properly linked to the individual or entity associated with it (providing non-repudiation) and can satisfy the criteria used to evaluate systems that produce electronic signatures.

DIGITAL SIGNATURES

Digital signatures are a document-dependent way of encrypting information by applying asymmetric encryption. Asymmetric encryption uses a key pair, consisting of a private and a public key. To sign a document digitally, the first step is creation of a hash value. The hash value is the result of a mathematical calculation (using algorithms also called hash functions), which transforms the document into a string of a certain length. The

hash value is signed subse
The addressee can check
to the digital signature a
further ensures the integ
document is tampered wi

Digital signatures pro
the PKI discussion: auth
signature guarantees tha
or altered. The digital si
information has been pr
signature represents that
denying that the informa

A digital signature b
identity. A digital certifi
a trusted intermediary c
Certification of a signatu
that a notary is a physica

DIGITAL CERTIFICATES

A digital certificate is an
a public key and a speci
public key, and other ide
directory or other databa
certificate or certification
in the certificate does, i
certification authority d
certificates, and oversees
of digital certificates. A
such as the starting date

CRYPTOGRAPHY

Cryptography is a form
contents of a documen
in order to hide the co
modification through th
comparable to a lock, an
by clicking the lock to its
can unlock (the decrypti

There are three con
(secret key) cryptograp
cryptography. Symmetri
the information sender
algorithms are well suite
integrity and origin of
to create the unique co

hash value is signed subsequently by the signer's private key and added to the document. The addressee can check the origin of the document by applying the signer's public key to the digital signature and checking whether the hashes match. The digital signature further ensures the integrity of the document, because the hash value changes if the document is tampered with or altered.

Digital signatures provide for the three security assurances mentioned above under the PKI discussion: authentication, confidentiality, and non-repudiation. The digital signature guarantees that the document is authentic and has not been tampered with or altered. The digital signature ensures confidentiality because it represents that the information has been protected from unauthorized viewing and use. Finally, the digital signature represents that the sender will not repudiate the information by subsequently denying that the information emanated from him or her.

A digital signature by itself cannot provide sufficient evidence of the signatory's identity. A digital certificate issued by a trusted third party, sometimes referred to as a trusted intermediary or trust service provider, links the signature to the signatory. Certification of a signature in this way increases certainty and trust, in the same manner that a notary is a physical witness to manuscript signatures.

DIGITAL CERTIFICATES AND CERTIFICATION

A digital certificate is an electronic credential that guarantees the association between a public key and a specific entity. It is created by adding the entity's name, the entity's public key, and other identifying information in an electronic document that is sorted in a directory or other database. The digital certificate, created by a trusted third party called a certificate or certification authority, provides the assurance that the public key contained in the certificate does, indeed, belong to the individual named in the certificate. The certification authority digitally signs the certificate, is responsible for managing digital certificates, and oversees the generation, distribution, renewal, revocation, and suspension of digital certificates. A certification authority may also set restrictions on a certificate, such as the starting date for which the certificate is valid as well as its expiration date.

CRYPTOGRAPHY

Cryptography is a form of secret writing that uses codes and ciphers to conceal the contents of a document or message. It transforms messages into unintelligible forms in order to hide the content, to establish its authenticity, and to prevent undetected modification through the use of an algorithm and a key to function. The algorithm is comparable to a lock, and the key operates the lock. Any person can lock a door simply by clicking the lock to its closed position (the encryption), but only the owner of the lock can unlock (the decryption) the lock.

There are three commonly used classes of cryptographic mechanisms: symmetric (secret key) cryptography; secure hash functioning; and asymmetric (public key) cryptography. Symmetric (secret key) cryptography is a class of algorithms where both the information sender and the information recipient share a secret key. Symmetric algorithms are well suited for confidentiality. They can also be used to authenticate the integrity and origin of data, since only the sender and the recipient have the ability to create the unique coded text. For example, the sender could code a portion of the

message, and the recipient could code the same portion of receipt in order to verify the accuracy of the algorithm the sender used, and thus verify identity. However, it is difficult to establish the initial shared key, and most users resort to a trusted third party to do so.

Asymmetric (public key) cryptography occurs when one party has a private key and the other party has a corresponding public key. The data encrypted with one key can be decrypted with the other key. For example, coded messages generated with the private key can be accessed by all those with a public key, and information coded with the public key can be decrypted by the private key holder. Asymmetric algorithms, well suited for authentication and integrity, are used to perform three operations: (1) digital signatures, (2) key transport, and (3) key assignment.

Secure hash functioning takes a stream of data and reduces it to a fixed size through a one-way (irreversible) mathematical function. The result is a "digest," which can be reproduced and verified by any party with the same stream of data and secure hash. Secure hash functioning can ensure integrity, but it can provide authentication only if the parties share a secret key. A significant issue associated with hash functioning at this time, however, is that the document has to be re-signed since algorithms expire over time.

Government Use of Authentication Technology: Current Examples—United States

Are some of the above technologies or others methods already being used by governments for the purpose of authenticating their government information? This section provides illustrations of such uses within the United States. The first example shows how the US Government Printing Office is using authentication technology and PDF versions of documents to ensure the authenticity of some important government information sources, including primary legal materials. The next examples illustrate what some states within the United States are doing to ensure the authenticity of primary sources of the law, such as administrative regulations and court opinions.

UNITED STATES FEDERAL GOVERNMENT

Users of US Government Printing Office (GPO) publications in print format have been able to rely upon the authenticity of the content of those documents. In the 1980s, GPO began supplementing or replacing print documents with tangible electronic format versions (floppy disks and CD-ROMs). With the evolution of the Internet that began in the 1990s, increasing use of digital format for the publication of government information has made authentication of the contents a major issue. GPO has recognized that digital technology makes documents easy to alter or copy, introducing the possibility of multiple non-identical versions that could be used in unauthorized or illegitimate ways.

In order to disseminate, protect, and preserve information from all three branches of government, GPO has launched its Federal Digital System or FDsys.[7] This system

7 See http://www.gpo.gov/fdsys. As of December 20, 2010, FDsys became GPO's official system of record for online government information. FDsys describes itself now as the location to access "America's Authentic Government Information."

provides no-fee digital acces
information submitted by
preserve the information as
system, GPO Access.

FDsys has three roles:
content, and as an advanced
its lifecycle to ensure con
standards to ensure long-te
combines extensive metada

GPO uses a digital cer
certain documents in PDF
providing assurance that th
them. At this time, the cha
GPO receives the content a
one example in which an
Budget of the US Governm
using a PKI signature. In o
to apply a digital signature
between the certificate and
within that path must be c
on PDF documents is Ado
used to certify these docu
users with assurance that t

In addition to certifyi
add a visible Seal of Authe
GPO signs and certifies a
of Authenticity and in the
print a document that has
automatically print on the
of Authenticity is a graphic
Information." This seal no
By using digital signature t
the document has not beer

A digital file that has b
information and the staten
since it was disseminated
of Authenticity, verifies d
documents, at no charge to
serve the same purpose a
documents. Documents th
primary sources of law as
and certified, containing G
technology), the current ed
Code of Federal Regulation
at this time are Congressio

provides no-fee digital access to official and authenticated versions of federal government information submitted by Congress and Federal agencies. FDsys is also intended to preserve the information as technology changes. It is replacing and improving an earlier system, GPO Access.

FDsys has three roles: as a system to manage content, as a repository to preserve content, and as an advanced search engine. It securely controls digital content throughout its lifecycle to ensure content integrity and authenticity. It follows archival system standards to ensure long-term preservation and access of digital content. Its search engine combines extensive metadata creation with modern search technology.

GPO uses a digital certificate to apply digital signatures to the official content of certain documents in PDF format after the validity of the content has been confirmed, providing assurance that the documents have not been altered since GPO disseminated them. At this time, the chain of custody that GPO provides begins in most cases when GPO receives the content and does not extend back to the content originator. However, one example in which an uninterrupted chain of certificates currently does exist is the Budget of the US Government (FY 2010 and FY 2011), for which GPO received content using a PKI signature. In order for users to validate the certificate that was used by GPO to apply a digital signature to the document, a chain of custody or a certification path between the certificate and an established point of trust is established. Every certificate within that path must be checked. The software required for validating digital signatures on PDF documents is Adobe Acrobat or Reader, version 7.0 or higher. The technology used to certify these documents allows GPO to secure the data integrity and provides users with assurance that the content is unchanged since GPO disseminated it.

In addition to certifying a document, GPO uses digital signature technology to add a visible Seal of Authenticity to authenticated and certified PDF documents. When GPO signs and certifies a document, a blue ribbon icon appears to the left of the Seal of Authenticity and in the Signatures tab within Adobe Acrobat or Reader. When users print a document that has been signed and certified by GPO, the Seal of Authenticity will automatically print on the document, but the blue ribbon will not print. The GPO Seal of Authenticity is a graphic of an eagle next to the words "Authenticated US Government Information." This seal notifies users that a document has been authenticated by GPO. By using digital signature technology to add the Seal to a PDF document, GPO attests that the document has not been altered since it was authenticated and disseminated by GPO.

A digital file that has been digitally signed and certified by GPO includes identifying information and the statement that "GPO attests that this document has not been altered since it was disseminated by GPO." A digital signature, viewed through the GPO Seal of Authenticity, verifies document integrity and authenticity of GPO online Federal documents, at no charge to users. The visible digital signatures on online PDF documents serve the same purpose as handwritten signatures or traditional wax seals on printed documents. Documents that have been authenticated by GPO by mid-2010 include such primary sources of law as public and private laws from 1995 forward (digitally signed and certified, containing GPO's Seal of Authenticity, using Public Key Infrastructure (PKI) technology), the current edition of the US Code, the Statutes at Large (2003–2006), and the Code of Federal Regulations (select years). Among other digital documents authenticated at this time are Congressional bills from 1993 forward (new bills are authenticated as they

are posted), the Federal Register, Presidential documents, and the Budget of the United States for FY 2010 and FY 2011 (digitally signed and certified PDF files).[8]

STATES WITHIN THE UNITED STATES

Within the past ten years, state governments in the US have been transitioning rapidly from paper to digital publication of their primary legal sources—statutes, court decisions, and regulations—without fully considering the implications of those changes. The move to digital publication of former print sources saves money and provides easier access to these sources for many public users. However, in nearly all cases, states have not adopted procedures to authenticate the new digital information or to provide a reliable infrastructure to preserve it. While a number of states have digital signature laws that apply to online business transactions and administrative matters, this use of digital technology has not carried over to such government functions as the publication of primary legal sources. Use of authentication technology for e-business and e-government is viewed as cost-effective, while employing the same technology to protect other types of state government information may be viewed as unnecessarily and prohibitively expensive. States are embracing online, digital publication dissemination to save printing costs, and the prospect of adding authentication expenses as a budget item is not a welcome one.

As of mid-2010, most US states are not using technology such as encryption, public key infrastructure, or digital signatures to authenticate the digital legal publications provided on their government websites. Some states do include disclaimers to point out that the digital versions of primary legal sources provided on their websites lack official status and/or are not authenticated. For example, posted along with the Minnesota statutes that appear on the state government website is the following message:

> 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.[9]

Despite the general lack of state action on the matter of authentication, a few states have begun to recognize and address the issue for one or more of the digital legal resources posted on their websites.

DELAWARE

Delaware is authenticating and certifying its online administrative documents and some legislative documents (session laws). Delaware authenticates its online Delaware Administrative Code by using digital signatures on PDF documents. While there is no

8 As part of its strong and continuing focus on the topic, the US Government Printing Office convened a "Document Authentication Workshop" on June 18, 2010 to seek input from federal agencies and the user community about authentication. The workshop covered issues such as authentication for automated, high volume applications, standards and methods for bulk data authentication, chain of custody, re-authentication over time, and granular authentication. At the workshop GPO representatives mentioned that GPO is already making available bulk XML data for the Federal Register and the Code of Federation Regulations, but this data is unsigned at this time and therefore not authentic or official.

9 See https://www.revisor.mn.gov/statutes/?view=info.

officially published compilat
certain titles available on th
those titles. The official ver
(commonly called Laws of D
Session laws from 1999 to th
as authentic. Online Delawa

OHIO

Ohio has begun to address
source—Supreme Court of
are authenticated through
authentication procedures
searchable in the database
Adobe Reader has a tab, eit
pen and paper, which is inc
indicate that the document
Official versions of opinion

UTAH

In 2007 the Utah Divisi
authentication to its websi
added to publication files.
confirm the integrity of a
provided by the Division
available, many at no cost,
not match exactly, then the
hash for the Utah State Bu
files, and Utah Administrat

ARKANSAS

The state of Arkansas dec
Reports and Arkansas App
on the state judiciary web
explored ways to authenti
authenticate two versions
WordPerfect format) and t
be able to warrant the cha
files are protected from alt
from Singlepoint (a United

10 See http://regulations.delawa
11 See http://delcode.delaware.
12 See www.sconet.state.oh.us/
13 All are available from http://

officially published compilation of the entire Delaware administrative code, the state makes certain titles available on the state's website[10] and has begun certifying the authenticity of those titles. The official version of the state session laws is Laws of the State of Delaware (commonly called Laws of Delaware or Delaware Laws), published by the State of Delaware. Session laws from 1999 to the present are available on the state's website[11] and are certified as authentic. Online Delaware court documents have not been certified or authenticated.

OHIO

Ohio has begun to address the authentication of online legal resources, but only for one source—Supreme Court of Ohio opinions. The opinions posted on the Court's website are authenticated through the use of digital signatures. Ohio uses encryption-based authentication procedures for all decisions, which are available as PDF files and are searchable in the database on the Ohio Supreme Court website.[12] Each opinion opened in Adobe Reader has a tab, either labeled "signatures" or identified by an icon representing a pen and paper, which is incorporated into the document's frame. Under that tab, notations indicate that the document is "signed by the Supreme Court." The opinions are unofficial. Official versions of opinions are located in the print versions of Ohio Official Reports.

UTAH

In 2007 the Utah Division of Administrative Rules announced the addition of file authentication to its website. Message-Digest algorithm 5 (MD5) authentication has been added to publication files. An MD5 hash is, in essence, a signature for a file. A user can confirm the integrity of a specific file the user downloads by comparing the MD5 hash provided by the Division with one that the user generates. Various software packages are available, many at no cost, that permit individuals to generate an MD5 hash. If the hashes do not match exactly, then the integrity of the file is in question. The Division provides an MD5 hash for the Utah State Bulletin, Utah State Digest, Utah Administrative Code and update files, and Utah Administrative Rules Index of Changes in PDF, RTF, TXT and ZIP formats.[13]

ARKANSAS

The state of Arkansas decided in 2009 to discontinue print publication of the Arkansas Reports and Arkansas Appellate Reports and to designate the appellate decisions posted on the state judiciary website as the official versions. Since then Arkansas officials have explored ways to authenticate those digital opinions. They looked for a process that would authenticate two versions of the court opinions—the "official original" (produced in WordPerfect format) and the "official copy" (PDF used for dissemination). They wanted to be able to warrant the chain of custody between the two versions and to ensure that the files are protected from alteration or tampering. They sought and received input and advice from Singlepoint (a United Kingdom-based company specializing in information integrity).

10 See http://regulations.delaware.gov/AdminCode/.

11 See http://delcode.delaware.gov/sessionlaws/.

12 See www.sconet.state.oh.us/.

13 All are available from http://www.rules.utah.gov/.

Arkansas ultimately selected a technology to verify authenticity and detect tampering by applying a unique digital fingerprint and time stamp to content files. When the "official original" document (WordPerfect file) is entered into the Arkansas document management system, it will be sealed automatically. The document will then undergo a number of changes before being released as the "official copy" (PDF file). The file will be automatically sealed at key stages in the process: renaming of the file, creation of metadata, and addition of final amendments. On the state judiciary website, a user will be able either to download the "official copy" PDF file for validation at a later date (using an applet or small java application) or to validate the file as it is being downloaded. Validation will indicate by whom the file was sealed and when the sealing occurred, ensuring that the contents of the sealed file are authentic and have not changed. If the sealed file has been tampered with in any way, the validation will fail. Arkansas began a beta test of this new technology in June 2010. PDF files with an authenticating seal were available for a short period. However, in late 2010, the PDF files no longer have seals of authentication attached to them, and there is no indication at the website when the court plans to begin using the authentication technology again.

Government Use of Authentication Technology: Current Examples—Other Countries and Organizations

Other countries are dealing with authentication of government-issued information as well. Some countries are authenticating digital information already, while others are working collaboratively within a union of member states to create the structure for general acceptance of authentication technology, such as electronic signatures. The following examples highlight the current use of authentication technology by two countries in particular and the efforts of several international organizations.

AUSTRALIA—AUSTRALIAN CAPITAL TERRITORY LEGISLATION

The online version of the Australian Capital Territory (ACT) legislation now reflects fundamental changes to reassure users about the authenticity of the legislation. The ACT Legislation Register website[14] includes the acts and ordinances as made and republished, as well as other legislative instruments such as subordinate laws, disallowable instruments, approved forms, notifiable instruments and commencement notices.

Users access authorized printed legislation on the website by downloading authorized files from the ACT Legislation Register website and printing them. The website indicates that "a document printed from an authorized file is legally presumed to be an accurate copy of the piece of legislation." The ACT Parliamentary Counsel's Office (PCO) implemented authentication technology to provide the security necessary to make certain that the downloaded files are true copies of ACT legislation. One important measure has been to provide a secure website for the legislation register using a Verisign SSL certificate. Users can verify that the website is legitimate by checking the certificate, and clicking on the Verisign icon in the bottom right corner of the legislation register homepage.

14 See http://www.legislation.act.gov.au/.

The Parliamentary Co
digital signatures to encry
private key, held securely b
was created by the PCO an
was last digitally signed. T
on the website. Users nee
apply to all digitally signe
user needs Adobe Acrobat

The PCO indicates tha
legislative materials, such
Assembly. These documer

FRANCE—LE JOURNAL

Le Journal officiel de la Re
nominal measures, listed a
agreements, parliamentar
announcements, concessi
issued information. All te
with a few exceptions. Ac
exclusively in paper, mo
acts related to administr
independent public autho

The legal basis for pub
164 of February 20, 2004 o
acts established that the di
status as the paper edition
mission is access to the law
texts published in the offi
and tribunals. It also prov
treaties and internationa
modes for French law: the

The electronic Le Jou
is also equally authentic
cases XAdES with a high
as a non-intrusive signa
as an intrusive signature
requirements: uniquely
created in a way that the
which it relates in such
PKCS#7 refers to the pub
used to describe a gener
digital signatures and di
is used with the softwar
keys for the publication

15 See http://www,legifrance.

The Parliamentary Counsel's Office also digitally signs authorized documents, using digital signatures to encrypt electronic documents by applying a mathematical code, or private key, held securely by the PCO. A certificate (public key) confirms that the document was created by the PCO and that the document has not been changed since the document was last digitally signed. The public key can be downloaded from a digital signatures page on the website. Users need only to download the public key once because it will then apply to all digitally signed files on the legislation register. To use digital signatures, the user needs Adobe Acrobat 5.0 or Acrobat Reader 5.1 or a higher version of the reader.

The PCO indicates that digital signatures will be applied also to authorized copies of legislative materials, such as explanatory statements and bills presented to the Legislative Assembly. These documents have the same legal status as authorized legislation.

FRANCE—LE JOURNAL OFFICIEL

Le Journal officiel de la Republique francaise contains laws, decrees, orders, circulars, and nominal measures, listed according to the ministries responsible. It also includes collective agreements, parliamentary information, opinions and communications, judicial and legal announcements, concessions or requests for name changes, as well as other government-issued information. All text published in the paper edition also can be consulted digitally with a few exceptions. Acts related to the status and nationality of persons are published exclusively in paper, most likely to protect the privacy of the individual. Regulatory acts related to administration organization, public agents, the state budget, and other independent public authorities are published exclusively on the Internet.

The legal basis for publishing information in France is the Constitution. Ordinance 2004-164 of February 20, 2004 on the publication and enactment of laws and certain administrative acts established that the digital Le Journal officiel (in its authentic version) has the same legal status as the paper edition. Le Journal officiel is available via the website Legifrance,[15] whose mission is access to the law for the public. Legifrance provides access to French law, including texts published in the official gazette, collective agreements, and the jurisprudence of courts and tribunals. It also provides access to standards issued by the European institutions and treaties and international agreements binding on France. Legifrance offers three search modes for French law: theme (from the home page), simple, and expert.

The electronic Le Journal officiel, besides sharing official status with the paper edition, is also equally authentic, due to the use of two types of electronic signatures. In most cases XAdES with a high level of authentication (XML advanced electronic signature), as a non-intrusive signature, is used, and PDF (IETF 2315/5652, aka PKCS#7) is used as an intrusive signature. An AdES is an electronic signature that meets the following requirements: uniquely linked to the signatory; capable of identifying the signatory; created in a way that the signatory can maintain sole control; and linked to the data to which it relates in such a manner that any subsequent change of the data is detectable. PKCS#7 refers to the public key cryptography standard that is probably the most widely used to describe a general syntax for data that has cryptography applied to it, such as digital signatures and digital envelopes. A secure server with certificate and a time stamp is used with the software nCipher Appliance. A crypto box is used to secure the private keys for the publication signature.

15 See http://www,legifrance.gouv.fr/.

LEGAL GAZETTES GENERALLY

A legal gazette is typically the publication of a government that reports actions taken by its various branches, such as new legislation and regulations. The website of the European Forum of Official Gazettes provides detailed information about the official gazettes of various countries, including whether or not the country has taken steps to ensure the authenticity of the information provided in the digital version of the gazettes.[16] The European Forum of Official Gazettes was created in 2004 by the organizations responsible for publishing the official gazettes of the European Union member states and the Office for Official Publications of the European Communities. The objective of the Forum is to exchange ideas and information on publication processes, technology and best practices between the official publishers. For each country, the website provides the details of the legal gazette for that country such as what is included and whether or not the paper and digital editions are both legally binding. For example, in this section of the report about Estonia's legal gazette, it states: "Since June 2002 the paper and the electronic editions have been equally authentic. The Thawte web server certificate based on the HTTPS protocol is used to guarantee the workflow and authentication procedures of the electronically published text."[17] Other information provided in the entry for each member state's gazette includes the details of the publishing institution, the drafting and publishing procedures, the collections of consolidated legislation, and the legislative portals and online databases.

EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION

Although primarily directed to the "internal market" and with the needs of businesses and commerce as a primary purpose, Directive 1999/93 of the European Parliament and the Council of the European Union, dated December 13, 1999, established a European framework for digital signatures and encryption. The purpose of the Directive, as outlined in Article 1 of the Directive, is to "facilitate the use of electronic signatures and to contribute to their legal recognition. It [the Directive] establishes a legal framework for electronic signatures and certain certification-services in order to ensure the proper functioning of the internal marker." Article 2 includes definitions of electronic signature, advanced electronic signature, certificate, certification service provider, signatory and other terms used in the Directive. Article 2, section 2, defines an "advanced electronic signature" as an electronic signature that meets the following requirements: (a) uniquely linked to the signatory; (b) capable of identifying the signatory; (c) created using means that the signatory can maintain under his sole control; and (d) linked to the data to which it relates in such a manner than any subsequent change of the date is detectable.

Article 5 outlines the effect of electronic signatures in member states. This Article indicates that member states should ensure that advanced electronic signatures that are based on a qualified certificate and that are created by a secure signature creation device satisfy the legal requirements of a signature in relation to data in electronic form, just as a handwritten signature satisfies these requirements in relation to paper-based data.

16 See http://circa.europa.eu/irc/opoce/ojf/info/data/prod/html/index.htm.

17 *Id.*

Moreover, Article 5 states
evidence in legal proceedi

Although this Directiv
information, it does establ
the member states, an imp

HAGUE CONFERENCE C
CONTENT OF FOREIGN

On October 19–21, 2008,
a meeting of experts to
information. Experts atter
the library and informati
institutes ("free access to
individuals from the Perm
Law. One of the purpose
feasibility study on the "d
concerning the treatment

The attending experts
this access to foreign law p
authoritativeness of legal i
These relevant guiding pri

- State parties are enco
materials provided in
- State parties are enco
ensure that authoritat
with clear indications
- State parties are encou
in their courts.
- State parties are enco
their legal materials re

The Hague Conference rep
Legal Resources published

Many individual cou
Finland, France, Germany
and Spain, have passed d
For example, Finland's
Administration, defines t
signature and identifies s
the application to admini
digital signatures to vouc

18 Hague Conference on Privat
of Experts on Global Co-operation o
19–21, 2008), available at http://w

Moreover, Article 5 states that advanced electronic signatures should be admissible as evidence in legal proceedings.

Although this Directive does not focus on the authentication of government-issued information, it does establish a framework for the use of electronic signatures throughout the member states, an important part of any authentication system.

HAGUE CONFERENCE ON PRIVATE INTERNATIONAL LAW—ACCESSING THE CONTENT OF FOREIGN LAW

On October 19–21, 2008, the Hague Conference on Private International Law convened a meeting of experts to discuss global co-operation for disseminating digital legal information. Experts attending the session represented stakeholders and providers from the library and information communities, educational institutions, legal information institutes ("free access to law" movement), legal community, and others, including individuals from the Permanent Bureau of the Hague Conference on Private International Law. One of the purposes of the conference was to assist with the preparation of a feasibility study on the "development of a new instrument for cross-border co-operation concerning the treatment of foreign law."

The attending experts developed guiding principles as part of the feasibility study on this access to foreign law project. Several of these guiding principles deal with integrity and authoritativeness of legal information, and one guiding principle deals with preservation. These relevant guiding principles are:

- State parties are encouraged to make available authoritative versions of their legal materials provided in electronic form.
- State parties are encouraged to take all reasonable measures available to them to ensure that authoritative legal materials can be reproduced or re-used by other bodies with clear indications of their origins and integrity (authoritativeness).
- State parties are encouraged to remove obstacles to the admissibility of these materials in their courts.
- State parties are encouraged to ensure long-term preservation and accessibility of their legal materials referred to in paragraphs 1 and 2 above.[18]

The Hague Conference report cites the State-by-State Report on Authentication of Online Legal Resources published by the American Association of Law Libraries.

Many individual countries, including Australia, Austria, Bermuda, Brazil, Canada, Finland, France, Germany, Hong Kong, Italy, Korea, Malaysia, New Zealand, Singapore, and Spain, have passed digital signature laws. Most are similar in terms of the content. For example, Finland's digital signature law, the Act on Electronic Service in the Administration, defines the scope and structure of the elements of a PKI for digital signature and identifies specific exclusions, including the use of digital certificates for the application to administrative judicial procedures. Other countries, such as Brazil, use digital signatures to vouch for the authenticity of legal materials online. The Supreme

18 Hague Conference on Private International Law, *Accessing the Content of Foreign Law:* No 11B—*Report of the Meeting of Experts on Global Co-operation on the Provision of Online Legal Information on National Laws—Annex* (The Hague, Oct. 19–21, 2008), available at http://www.hcch.net/upload/wop/genaff_pd11b2009e.pdf.

Court of Justice in Brazil now publishes its decisions online with digital signatures affixed to them as an indication of their authenticity.

Authentication: Strategies and Next Steps

With more widespread recognition of authentication as a concern with digital government information, some action is underway. However, increased efforts are needed to address this rapidly growing problem. Initiatives are needed in the education, technology, legislative, and advocacy arenas. Particularly at the state or provincial level, opportunities for advocacy with legislators, judges, and other government officials should be explored. Librarians in all types of libraries should note the needs of their users for authentic government information and should share examples of situations where the integrity of sources has come into question. In the legal community, such examples might include situations in which evidentiary issues have been raised by attorneys and courts concerning unofficial, unauthenticated government sources of law in digital format.

Some recent progress and some ongoing and potential activities are outlined below.

EDUCATION

After its groundbreaking State-by-State Report on Authentication of Online Legal Resources, the American Association of Law Libraries convened a very successful National Summit on Authentication of Digital Legal Information in April 2007. Summit delegates included a carefully selected group of law librarians, judges, and representatives from the American Bar Association, and state and federal government officials, all of whom had expertise or interest in authentication issues. Also participating were technology and security experts who were able to speak knowledgeably about the authentication technology available in 2007. Since organizing and hosting the Summit, the AALL has taken further action, including the following efforts currently underway:

- Working with the National Conference of Commissioners on Uniform State Laws to research and draft a uniform act about authentication that could be distributed to state legislatures;
- Establishing state working groups to begin discussing the importance of the authentication issue with state legislators and other state government officials;
- Building alliances with other library associations, national and state, to enlist the support of librarians who are familiar with both legal and other types of government-issued information;
- Presenting programs about authentication at association conferences, including those held by the AALL itself, the Virginia Library Association, and the National Center for State Courts' Court Technology Conference; and
- Publishing articles about the authentication issue and the issues associated with non-authenticated digital information in journals directed to judges, lawyers, other librarians, technology groups, etc.

Importantly, AALL members, under the guidance of the Association's Electronic Legal Information Access and Citation Committee, in 2009-2010 revisited the previous state-

by-state research and pub
noting progress or lack th
legal materials in digital f
changes to online legal pu
making digital informatic
in favor of online only. T
states have eliminated the
digital format. Eight states
legal information by takir
version and time-stamping
now guarantee permanen
additional states have ad
materials in their states, p
the 2009-2010 updates is
websites, pointing out tha
warranted as official and/
almost certainly a direct re
explanations.

Other recent efforts to e
In 2000 the Council on Li
of the authentication of
on authenticity and publi
Digital Environment. In 2
Authentication White Pape
Legal E-Access Conference
legislation in Europe. The
by European countries to (a
legislative process; (b) incr
its legal status; (c) replace
(d) provide easy access to
legislation.[19] As mentioned
convened its meeting of ex
study on an access to forei
the Hague Conference late
the experts' responses to a

LEGISLATIVE

The National Conference o
its work on a uniform ac
legislatures. A NCCUSL wo

19 Aki Hietanen and Marika Seppiu
(Paris, France, Dec. 11, 2008), availal

20 Hague Conference on Private
Responses to the Questionnaire of Oct
Legal Information on National Laws (T
pd11b2009e.pdf.

by-state research and published updates to information provided in the 2007 report, noting progress or lack thereof for each state in regard to authentication of primary legal materials in digital format. These updates indicate that a few states have made changes to online legal publications, including adding official and authentic notations, making digital information more accessible, and even eliminating print publications in favor of online only. The updates show that since the 2007 report, four additional states have eliminated the print version of a legal publication in favor of exclusively digital format. Eight states have made changes to the availability of their official digital legal information by taking steps such as designating the digital version as the official version and time-stamping to certify court decisions as authentic. Four additional states now guarantee permanent public access to online state legal information, and two additional states have adopted a new vendor-neutral citation format for citing legal materials in their states, primarily court opinions. Another significant change noted in the 2009-2010 updates is that many more states have added disclaimers to their state websites, pointing out that the online content is for informational purposes and is not warranted as official and/or completely accurate. The addition of these disclaimers is almost certainly a direct result of AALL highlighting in its 2007 report the need for such explanations.

Other recent efforts to educate and inform about authentication include the following. In 2000 the Council on Library and Information Resources highlighted the importance of the authentication of government-issued information by convening a conference on authenticity and publishing the proceedings in a report entitled Authenticity in a Digital Environment. In 2005 the United States Government Printing Office issued its Authentication White Paper in preparation for its work with FDsys. In 2008 the European Legal E-Access Conference was held in Paris, France, and one session focused on access to legislation in Europe. The speakers identified the many projects from 2004–2008 taken by European countries to (a) modernize the production of legislation and the workflow of legislative process; (b) increase the reliability of electronic official gazette and to confirm its legal status; (c) replace gradually the paper version with authentic electronic version; (d) provide easy access to electronic legislation; and (e) produce consolidated electronic legislation.[19] As mentioned earlier, the Hague Conference on Private International Law convened its meeting of experts in 2008 to address authentication as part of its feasibility study on an access to foreign law project. The experts developed guiding principles, and the Hague Conference later released three reports as a result of this meeting, including the experts' responses to an authentication question.[20]

LEGISLATIVE

The National Conference of Commissioners on Uniform State Laws (NCCUSL) continues its work on a uniform act about authentication and preservation to present to state legislatures. A NCCUSL working group was established in 2008 and concluded its research

19 Aki Hietanen and Marika Seppius, Lex Electronique, Lex Authentique, Lex Consolidee, *European Legal E-Access Conference* (Paris, France, Dec. 11, 2008), available at http://www.legalaccess.eu/IMG/pdf/00_seppiusparis08seppiushietanen.pdf.

20 Hague Conference on Private International Law, *Accessing the Content of Foreign Law*: No. 11C—*Compilation of Responses to the Questionnaire of October 2008 For the Meeting of Experts On Global Co-operation on the Provision of Online Legal Information on National Laws* (The Hague, Oct. 19–21, 2008), available at http://www.hcch.net/upload/wop/genaff_pd11b2009e.pdf.

in 2009 with a recommendation that NCCUSL form a Drafting Committee to draft a uniform law describing minimum standards for the authentication and preservation of online state legal materials. The Drafting Committee's prefatory notes to its current draft of Authentication and Preservation of State Electronic Legal Materials Act conclude

> ... this [act] addresses the critical need to manage electronic legal information in a manner that guarantees the trustworthiness of and continuing access to important state documents. ... A [uniform act] will allow state governments to develop similar systems of authentication and preservation, aiding the free flow of information across state lines and the sharing of experiences and expertise to keep costs as low as possible.

Importantly, section 5 of the draft act states that electronic legal materials, if they are authenticated in the manner set forth in the draft act, are presumed "to be a true and correct copy of the legal material."

The Drafting Committee presented its May 2010 draft of the uniform act to the Committee of the Whole of the NCCUSL on July 15, 2010. The Committee of the Whole debated the draft act, raising several questions and offering numerous comments. The main outcomes of the Commissioners' debates were a request for clarification of the relationship between the state's official publishers and commercial publishers, a desire by the Commissioners to include free access to preserved, historical materials as an option, and a clearer explanation regarding the Drafting Committee's intention regarding the effective date of the act. After the first reading and debate, the Committee of the Whole accepted the report of the Drafting Committee, including the draft uniform act. It also asked the Drafting Committee to meet again and consider the comments and questions from the Committee of the Whole. The Drafting Committee met in November 2010 to discuss an updated interim draft of the uniform act based on the comments of the Committee of the Whole and Drafting Committee members. The Drafting Committee reviewed and considered the questions and comments raised by the Committee of the Whole in July 2010 and debated additional questions and concerns raised by the Drafting Committee members. The Drafting Committee reporter and chair will prepare a revised draft uniform act based on the November 2010 meeting, will meet again in February 2011, and subsequently will prepare a revised draft uniform act to present to the Committee of the Whole again in July 2011.

The European Legal E-Access Conference session described earlier outlines many legislative actions affecting authentication that have occurred in Europe. Notably, France established a new kind of chain of custody (confidence) in the production of its Le Journal Officiel. Germany, Denmark, and the United Kingdom have established new workflow processes and tools for legislative drafting that establish complete chain of custody and use different data formats that can be authenticated. Greece has established secure server protocol, and the electronic text (PDF) of its gazette carries an integrated electronic signature and is, therefore, considered authentic. Austria, Denmark, and Spain publish no paper copies of their legal gazettes, and the electronic versions are the only authentic versions. Slovenia uses digital signatures with the electronic version of its *Uradni list Republike Slovenije*, which is, therefore, as authentic as the paper version. Hungary has implemented authentication of its electronic official gazette.

Two items would greatly benefit the authentication efforts of many governments: standards and best practices manuals. While it may be too early for the development of

a comprehensive and widely-accepted set of authentication standards, in their absence it would be helpful to governments pursuing authentication if some entity, either within or outside government, would compile and publish a "best practices manual." Such a manual could provide examples and guidance gleaned from state governments and countries that are currently authenticating and preserving their government-issued information, providing possible models for others to follow. Currently, no such manual exists, although the documents cited in the references and additional readings section of this chapter, when reviewed collectively, could certainly assist those who are trying to develop such best practices.

One issue that arises when discussing authentication is whether all government information requires the same high level of authentication or whether there are certain types of information that merit full authentication, while a lesser standard might be adequate and reasonable for other types of information. As discussed previously in this chapter, legal information is one category for which the highest level of authentication is essential. Other categories for which a high level of assurance is necessary are government research data, budgetary information, and statistics. The integrity and chain of custody for these categories of information must be assured. If necessary, a lesser standard of assurance might be justified for information of a less-sensitive nature or information, which is frequently updated or replaced. Another question is: what would the different levels of authentication be? Are some types of digital government information ephemeral, requiring no intentional authentication? If authentication is possible for some, but not all, categories of government information, how should government publishers prioritize the provision of authentication? Much more discussion needs to occur on these matters.

TECHNOLOGY

Technology to authenticate digital government information is currently available. For purposes of electronic commerce, governments in many countries have implemented systems using digital signatures. However, in most instances those same governments have been slow to employ similar technological or other means to ensure that the legal and other information they produce in digital format is authenticated and reliable. These governments have been particularly concerned about the potential costs associated with implementing and maintaining authentication systems. An additional concern to governments is how quickly various types of technology become obsolete. For example, some technologists by late 2010 were regarding Message-Digest algorithm 5 (MD5), mentioned earlier in the chapter and used by Utah to confirm the integrity of its administrative code and other administrative publications, as an obsolete technology that no longer provides sufficient assurances.

At least one technological initiative is necessary—governments need to adopt relevant existing standards and assist in the development of additional standards for authentication. One aspect of this initiative is a determination by governments regarding how much standardization is necessary. Efforts among member states in the European Union are leading the technology initiative. Those member states have taken significant steps through the European Legal E-Access Conference to address standards. Also, the experts at the Hague Conference on Private International Law "Accessing the Content of Foreign Law" meeting identified the following as one of their guiding principles: "State parties are encouraged to cooperate in the development of common standards

for metadata applicable to legal materials, particularly those intended to enable and encourage interchange." In fact, one of the experts at the Hague Conference commented, "I also hope that the Hague Conference can become a stakeholder in helping to create a standard for the authentication of official digital law."[21]

Furthermore, article 8 of the NCCUSL draft uniform act addresses the question of standards: "In implementing the requirements of this act, the official publisher shall consider: (1) standards and practices of other jurisdictions; (2) any standards on authentication and preservation of records adopted by national standard-setting bodies; and (3) the needs of electronic records users." In the comments after this article, the NCCUSL stresses the importance of efficiency in order to encourage states within the United States to communicate and coordinate the development of authentication, preservation, and permanent access standards. The NCCUSL also suggests that national organizations consider the promulgation of best practices statements and standards and share their work. NCCUSL concludes its comments with this statement: "International organizations may also be tackling this issue and, to the extent that their work is relevant to the US states, it could also be considered."[22]

For such sharing to be effective, governments in all countries should do more than simply consider what other governments are doing. They should work together to establish national and international best practices and standards and then adopt procedures and processes to implement those practices and standards. Certainly, governments should consider the World Wide Web Consortium (W3C) XML authentication standards and the Internet Engineering Task Force (IETF) 5652 digital signature standards. As some people have pointed out, any government that is adopting XML for its government information is effectively creating a standard as well.

ADVOCACY

Cooperative efforts by librarians and their professional organizations are needed to convince governments of the importance of authenticating and preserving their digital information and to provide examples of cost-effective means to do so. Lobbying efforts with government legislative bodies are crucial. To accomplish this goal, librarians and library organizations must build alliances with other groups and must extend the scope of their alliances to include groups with whom librarians may not have worked previously. For example, in the United States, the American Association of Law Libraries, recognizing the importance of working with groups such as the Council of State Governments, the American Bar Association, the National Association of Secretaries of State, the National Conference of Commissioners on Uniform State Laws, state archivists, and groups of judges, has been developing those relationships. The AALL also has created state working groups to ensure access to digital legal information by taking three actions: (1) oppose any plan to eliminate state official print legal resources unless the digital version is authenticated and preserved permanently; (2) ensure that a disclaimer is added to any legal resources on state websites, indicating that the information is not official or authentic if the state has not taken actions to make the information official and authentic; and (3)

21 *Id.* at 59.

22 National Conference of Commissioners on Uniform State Laws (Uniform Law Commission), *Prefatory Note, Authentication and Preservation of State Electronic Legal Materials Act* (2010).

participate in the development of a national inventory of all primary legal resources at every level of government.

Leaders in other disciplines such as science and medicine need to be engaged in discussions on the importance of authentication of government data and statistics on which their work depends. Members of the public must be made aware of the difference between government information that appears on a commercial website and the authenticated version of that same information found on a government website – that they can rely on the latter but not the former. Librarians and library organizations must develop marketing and promotional materials that indicate clearly why authentication of government-issued information is such an important issue and how it affects the daily lives of citizens, as well as lawyers, judges, researchers, scholars, and government officials.

Keeping attention focused on authentication must be a collaborative effort; an alliance of advocates is more likely to be effective than groups working individually. It would certainly be beneficial for additional stakeholders to be engaged in advocacy on authentication. For example, the library and information community, governments, and others interested in authenticating digital government information in various countries might benefit by partnering with the "free access to law" movement. "Free access to law" is the umbrella designation for a collection of legal information institutes (LIIs) throughout common law countries that have been organized to provide free and open online access to legal information, such as case law, statutes, and regulations. Many legal information institutes throughout the world, including the World Legal Information Institute, the Australasian Legal Information Institute, the British and Irish Legal Information Institute, the Canadian Legal Information Institute, and the Southern African Legal Information Institute, are part of this "free access to law" movement.

In October 2002, the LIIs met in Montreal at the Fourth Law via Internet Conference and issued a joint statement of their philosophy of access to the law, including the following three points:

- Public legal information from all countries and international institutions is part of the common heritage of humanity. Maximizing access to this information promotes justice and the rule of law;
- Public legal information is digital common property and should be accessible to all on a non-profit basis and free of charge;
- Independent non-profit organizations have the right to publish public legal information and the government bodies that create or control that information should provide access to it as that it can be published.

Providing access to digital information is a significant goal of the LIIs. An equally significant goal should be ensuring that the information used by citizens is authentic, reliable, and trustworthy. It seems reasonable that the "free access to law" movement has a major stake in the authentication of digital government information and could be a cooperative partner for librarians and others in efforts to ensure that the information accessible through LIIs is reliable and trustworthy. At a recent workshop at Princeton University about open government and transparency, a participant, who also is a leader in the "free access to law" movement, made the connection between the free access movement and the authentication issue in his remarks. When discussing his Law.gov project, he emphasized the importance of lobbying the US federal government for the authentication of digital

legal information by requiring "... each law-making federal entity to authenticate all digital legal information it produces."[23] Many others from the LIIs would likely join him in collaborating with librarians and others in lobbying efforts with government legislative bodies to emphasize the importance of the authentication issue.

Summary and Conclusion

Digital authentication of government-issued information is not yet a widespread practice, although procedures to do so are becoming more common, especially in Europe. Until a government can ensure that a digital document it issues is exactly what the document purports to be, reliance on that digital version carries an inherent risk. This is a particular concern with certain types of information, such as primary sources of the law—court opinions, legislative enactments and administrative regulations—but also for statistical and research data of interest to those in other disciplines.

In 2006 a law partner with a large United States law firm described the digitization of information as a "societal sea change." Using legal materials, information records, photographs, and other types of evidence that an attorney might want to introduce into court proceedings as examples, he expressed concern about the lack of authenticity of digital materials and images. He concluded: "Now, more purely stored and easily manipulated information is pervasive in our society's informational records. All these records—used to document communications, transactions and the appearance of reality—must be capable of 'authenticity testing.' Otherwise, tribunals will be unable to provide their most basic functions."[24] Courts, he continued, must face the fact that the old authenticity paradigms, such as seals and the printed format, are disappearing, and judges and court administrators must encourage legislators and others to come up with solutions for authentication, which might possibly turn out to be superior to the old paradigms.

The Association of Reporters of Judicial Decisions (ARJD) came to a similar conclusion in 2007 in its Statement of Principles: "Official" On-Line Documents (revised in 2008):

> [a]n on-line government document, even one designated "official," cannot be considered authoritative if it does not satisfy ... authentication criterion. ... As long as only the print version of an official document meets the foregoing authentication and permanence criteria, the print version ... should control and be considered authoritative ...

AALL's State-By-State Report on Authentication Of Online Legal Resources, published in 2007, raised the same concerns about state-level primary legal resources on the Web and concluded that unless proper authentication procedures are in place, such government-hosted legal information in digital format is not sufficiently trustworthy.

All levels of government within the United States and governments in other countries must now face this reality: familiar types of authentication that everyone trusts

23 *Open Government: Defining, Designing, and Sustaining Transparency: a Two-Day Workshop at Princeton University* (Princeton, NJ: Center for Information Technology Policy, Jan. 21-22, 2010), available at http://citp.princeton.edu/open-government-workshop/.

24 George L. Paul, The "Authenticity Crisis" In Real Evidence, *Law Practice Today*, March 2006, available at http://apps.americanbar.org/lpm/lpt/articles/tch03065.shtml.

are disappearing quickly as gov
exclusively in digital format.
trust government-issued inform
what it purports to be. Governm
they issue by adopting appropr
trustworthiness and reliability.

References and Additio

Babette Aalberts and Simone van
Approaches Toward Electronic A
simone/Digsigbl.pdf.
Information Security Committee, An
Help Assess and Facilitate Interoper
Association of Reporters of Judicial
(issued Feb. 2007 and revise
StatementofPrinciples_May2008.p
M. Anderson Berry and David Lierna
Jan. 21, 2010, available at http://w
02439301020&slreturn=1&hbxlog
Kamini Bharvada, Electronic Signatu
Computers and Technology 265 (200
David M. Cieslak, Greater Precautions
available at http://www.wordinfo.i
Timothy L. Coggins, Virginia Law: I
2008, at 35.
Charles T. Cullen et al., *Authenticity i*
and Information Resources, May 2
Herbert B. Dixon, Jr., The Lack of E
Information and Documents, *Judg*
Working Group on Authenticity, E
Legislation—Towards Authenticity: Fi
http://circa.europa.eu/irc/opoce/oj
European Parliament and the Counci
Parliament and of the Council (Dec. 13
directive.pdf. (For follow-up about
Report From the Commission to the E
1999/93/EC on a Community Framew
Hague Conference on Private Internatio
– *The Need for the Development of a Gl*
of the Meeting of Experts on Global Co
Laws; and No. 11C—*Compilation of*
Experts On Global Co-operation on the
Oct. 19–21, 2008), available at http:/

are disappearing quickly as governments switch to making their information available exclusively in digital format. Without the necessary authentication, citizens cannot trust government-issued information and can never be sure that the information is what it purports to be. Governments have an obligation to authenticate the information they issue by adopting appropriate practices, standards, and technology to ensure its trustworthiness and reliability.

References and Additional Reading

Babette Aalberts and Simone van der Hof, Digital Signature Blindness: Analysis of Legislative Approaches Toward Electronic Authentication (Nov. 1999), available at http://rechten.uvt.nl/simone/Digsigbl.pdf.

Information Security Committee, American Bar Association, *PKI Assessment Guidelines: Guidelines To Help Assess and Facilitate Interoperable Trustworthy Public Key Infrastructure* (June 18, 2001).

Association of Reporters of Judicial Decisions, *Statement of Principles: "Official" On-Line Documents* (issued Feb. 2007 and revised May 2008), *available at* http://arjd.washlaw.edu/ARJD-StatementofPrinciples_May2008.pdf.

M. Anderson Berry and David Liernan, Authenticating Web Pages as Evidence, *Law Technology News*, Jan. 21, 2010, available at http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202439301020&slreturn=1&hbxlogin=1.

Kamini Bharvada, Electronic Signatures, Biometrics and PKI in the UK, 16 *International Review of Law Computers and Technology* 265 (2002).

David M. Cieslak, Greater Precautions To Protect Vital Information Are Available, *Information Technology*, available at http://www.wordinfo.info/words/index/info/view_unit/3986/?letter=-I&spage=3.

Timothy L. Coggins, Virginia Law: It's Online, But Should You Use It?, *Virginia Lawyer*, June/July 2008, at 35.

Charles T. Cullen et al., *Authenticity in a Digital Environment* (Washington, D.C.: Council on Library and Information Resources, May 2000).

Herbert B. Dixon, Jr., The Lack of Effort to Ensure Integrity and Trustworthiness of Online Legal Information and Documents, *Judges Journal*, Summer 2007, at 42.

Working Group on Authenticity, European Forum of Official Gazettes, *Electronic Publishing of Legislation—Towards Authenticity: Final Report of the Working Group* (Helsinki, June 2007), available at http://circa.europa.eu/irc/opoce/ojf/info/data/prod/data/pdf/Helsinki2007-authenticity-final.pdf.

European Parliament and the Council of the European Union, *Directive 1999/93 EC of the European Parliament and of the Council* (Dec. 13, 1999), available at http://iportal.etsi.org/esi/Documents/e-sign-directive.pdf. (For follow-up about this Directive, see Commission of the European Communities, *Report From the Commission to the European Parliament and the Council On the Operation of Directive 1999/93/EC on a Community Framework For Electronic Signatures* (Brussels, March 15, 2006).

Hague Conference on Private International Law, *Accessing the Content of Foreign Law* (three parts): No. 11A – *The Need for the Development of a Global Instrument In This Area: a Possible Way* Ahead; No 11B—*Report of the Meeting of Experts on Global Co-operation on the Provision of Online Legal Information on National Laws*; and No. 11C—*Compilation of Responses to the Questionnaire of October 2008 For the Meeting of Experts On Global Co-operation on the Provision of Online Legal Information on National Laws* (The Hague, Oct. 19–21, 2008), available at http://www.hcch.net/upload/wop/genaff_pd11b2009e.pdf.

Hague Conference on Private International Law, *Accessing the Content of Foreign Law and the Need for the Development of a Global Instrument in this Area—A Possible Way Ahead* (2009), available at http://www.hcch.net/upload/wop/genaff_pd11a2009e.pdf.

Aki Hietanen and Marika Seppius, Lex Electronique, Lex Authentique, Lex Consolidee, *European Legal E-Access Conference* (Paris, France, Dec. 11, 2008), available at http://www.legalaccess.eu/IMG/pdf/00_seppiusparis08seppiushietanen.pdf.

D. Richard Kuhn et al., *Introduction to Public Key Technology and the Federal PKI Infrastructure* (Washington, D.C.: National Institute of Standards and Technology, Feb. 26, 2001).

Law Reform Commission, *Report on Statute Law Restatement* (2008).

Kathy Lyons-Burke, *Federal Agency Use of Public Key Technology for Dignature Signatures and Authentication* (Special Publication 800-25) (Washington, DC: National Institute of Standards and Technology, Oct. 2000).

Richard J. Matthews, Why Authentication Procedures Matter for US and UK Public Legal Resources on the Web, 8 *Legal Information Management* 35 (2008).

Richard J. Matthews and Mary Alice Baish, *State-By-State Report on Authentication of Online Legal Resources* (Chicago, IL: American Association of Law Libraries, 2007). For the 2009-2010 Updates to the 2007 Report, see the AALL Electronic Legal Information Access and Citation Committee (recently renamed the Digital Access to Legal Information) Web site, *available at* http://www.aallnet.org/Documents/Government-Relations/authen-rprt-updates/2009aallauthenticationreportupdates.pdf.

Mirella Mazzeo, Digital Signatures and European Laws, *Security Focus* (Jan. 26, 2004), available at http://www.symantec.com/connect/articles/digital-signatures-and-european-laws.

National Association of Secretaries of State, *National E-Notarization Standards* (Washington, D.C.: NASS, adopted July 12, 2006), *available at* http://nass.org/index.php?option=com_content&task=-view&id=46&Itemid=229.

National Conference of Commissioners on Uniform State Laws (Uniform Law Commission), *Authentication and Preservation of State Electronic Legal Materials Act—May 2010 Interim Draft* (Chicago, IL: NCCUSL, 2010).

National Conference of Commissioners on Uniform State Laws (Uniform Law Commission), *Uniform Electronic Transactions Act* (Chicago, IL: NCCUSL, final version approved and recommended for enactment in states of the United States, July 23–30, 1999) (definitions section used in the definition section of this chapter). (Forty-six states plus the District of Columbia and the Virgin Islands have adopted UETA. Only Georgia, Illinois, New York and Washington have not adopted UETA as of June 2009.)

National Institute of Standards and Technology, *Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology* (Special Publication 800-63, version 1.0.2) (Washington, D.C.: NIST, April 2006) (guidelines for e-authentication, the process of establishing confidence in user identifies electronically presented to an information system).

George L. Paul, The "Authenticity Crisis" In Real Evidence, *Law Practice Today*, March 2006, available at http://apps.americanbar.org/lpm/lpt/articles/tch03065.shtml.

The PKI Page, available at http://www.pki.page.org.

St. Clair v. Johnny's Oyster & Shrimp, Inc., 76 F. Supp. 2d 773 (S.D. Tex. 1999).

United States Government Accountability Office, *Public Key Infrastructure: Examples of Risks and Internal Control Objectives Associated with Certification Authorities* (Letter to House of Representative member Tom Davis from Keith A. Rhodes, Chief Technologist) (Washington, D.C.: US GAO, Aug. 10, 2004).

United States Government Printing Office, *White Paper on Authentication* (Washington, D.C.: Government Printing Office, Oct. 13, 2005).

CHAPTER 10

Introduction

Information flows permea
scale and complexity of th
and diversity of public sec
and reformers rightly see
making public sector infor
describes some methods a
toward more open and col

Background

Directives, reporting, mon
government process involv
it can be helpful to classify
in policy making processes
can be many examples wh
information flows in this
requirements needed to re

- *Data to Inform Policy*:
  significant inputs outs
  from the scientific an
  officials in governmen
  inform policy making.
  to social and economi
  with different regulat
  aim of impacting polic
  may have other prima
  collection methodolo
  data can be hotly con