Legal Information Management, 8 (2008), pp. 35–42
 Printed in the United Kingdom doi:10.1017/S1472669607002150

Why Authentication Procedures Matter for US and UK Public Legal Resources on the Web

Abstract: Online legal resources are increasingly the sole official source. Authentication – the means to demonstrate that materials are what they purport to be – is inseparably interrelated with the official status of sources on the web. This article by Richard J. Matthews examines key features of the UK Statute Law Database, the US Government Printing Office future digital system (FDsys), and the Ohio Supreme Court database of judicial decisions that are relevant to assessing appropriate authentication procedures for those resources. Archival and computational authentication methods are reviewed. Overall findings of AALL's *State-by-State Report on Authentication of Online Legal Resources* and its recent national summit on authentic legal information on the web are analysed.
Keywords: online services; authentication; legislation; digital signatures

Introduction

The phrase "authentication procedures" appears no more than three or four times in the American Association of Law Library's recently released *State-by-State Report on Authentication of Online Legal Resources* (AALL etc. 2007a). Authentication is described there as a process - therefore authentication procedures are implied. But the report generally is uncommitted to any particular form of authentication, so long as the method is regarded as standard. Coinciding with the report, AALL convened a national summit titled *Authentic Legal Information in the Digital Age* (20–21 April 2007), intending to prompt the invited state officials and information policy leaders to explore and discover for themselves the best procedures.

The report's working definitions for "authentication" and "authentic" follow. The "authentication" of electronic documents "is a process involving computer technology or other means to verify a text as authentic." (AALL etc. 2007a, 209). Further:

> An "authentic" text is one whose content has been verified by a government entity to be complete and unaltered when compared to the version approved or published by the content originator. Typically an authentic text will bear a certificate or mark that conveys information as to its certification, the process associated with ensuring that the text is complete and unaltered when compared with that of the content originator. An authentic text can be validated, ensuring that it is what it claims to be. (Ibid)

These were the definitional starting points for the groundbreaking fifty-state authentication survey, which began in 2005 and concluded with the *State-by-State Report on Authentication of Online Legal Resources*. AALL's national summit similarly proceeded from those definitions. This article refines the concept of "authentication procedures" based on the national summit's responsive synergies.

A fuller understanding of authentication of legal resources on the web clarifies other concepts received somewhat uncritically by law librarians and the legal community. The notion of "official" status of legal resources is one such concept. A recent policy statement developed by the Association of Reporters of Judicial Decisions (ARJD), and addressed at the national summit, illuminates the relationship between authentication and official status.

According to ARJD's *Statement of Principles: "Official" On-Line Documents*:

> [O]n-line government documents should not be designated "official" unless they are (1) authenticated by encryption, digital signature, or some other computerized process to safeguard them

> from illegal tampering and (2) permanent in that they are impervious to corruption by natural disaster, technological obsolescence, and similar factors and their digitized form can be readily translated into each successive electronic medium used to publish them. So long as no computerized process guarantees such permanence, a governmental entity should not designate a non-print-published, electronic document 'official' unless that entity also undertakes to make whatever conversions are necessary in the future in order to perpetuate the document in an accessible, accurate, "official" form (Association of Reporters of Judicial Decisions 2007).

ARJD takes the view that "[p]rint publication, because of its reliability, is the preferred medium for government documents at present. For example, official court reports are relied upon as authoritative and definitive guidance in conducting legal dealings and affairs because of the reports' undoubted and demonstrable authenticity and their existence in a permanent, published form." (Ibid) While AALL does not insist that one version (either paper or digital, but not both), should *necessarily* be the sole official version, it otherwise holds a position similar to ARJD. As articulated in the *State-by-State Report on Authentication*, "online legal resources are inherently capable of being corrupted or tampered with at the level of the individual copy" and are, in that respect, "fundamentally different from print legal resources." (AALL etc. 2007a, 21).

The report's working definition of "official" status follows. An "official" version of an online resource such as statutes or court decisions "is one that has been governmentally mandated or approved by statute or rule. It might be produced by the government, but does not have to be. A text may be certified by a government or other entity as official when the content originator has authorised the entity to do so." (Ibid 210) This definition draws, in part, on *Black's Law Dictionary* (2004, 1327), specifically the entry for "official report," which is discussed further below.

Given the fluid character of the digital medium, the official status of online legal resources is inseparably interrelated with authentication. That relation is a corollary to the working definition of "official." Consequently, the *State-by-State Report on Authentication* might have sidestepped complex questions concerning which online legal resources are official and could have categorically excluded all. The report, however, inquired as to which online resources relevant officials considered official and, further, what statutes, administrative rules, and other sources of law corroborate that understanding. The demonstrated disconnect between available "official" legal resources on the web and their authentication is the fundamental reason why authentication procedures matter.

Does official status actually matter? Why aren't online legal resources without authentication good enough? Are online legal resources really so at risk to warrant authentication procedures and is a selective risk analysis best? Why aren't practices supporting case-by-case authentication, when needed, sufficient? The national summit provided important insights on these issues, as discussed below.

Official status of legal resources

Authentication procedures matter where official status matters. Both the *State-by-State Report on Authentication* and ARJD's *Statement of Principles: "Official" On-Line Documents* acknowledge the importance of the paper medium. "Print *official* legal resources have generally served as a touchstone for authoritative and reliable statements of the law." (AALL etc. 2007a, 19). "An online *official* legal resource is one that possesses the same status as a print *official* legal resource." (Ibid). The ARJD gives print official publication a distinct priority because of its reliability. "For example, official court reports are relied upon as authoritative and definitive guidance … because of the reports' undoubted and demonstrated authenticity and their existence in a permanent published form." (Association of Reporters of Judicial Decisions 2007).

Is print truly a bedrock? Are official resources the ultimate touchstone? Not invariably. The definition of "official report" in *Black's Law Dictionary* (which has no entry for "official") includes a qualifying quotation from a seminal instructional text noting that "all reports are in a sense 'official' or to use the term 'official reports' as referring to any particular series of reports is a misnomer, for it is certainly misleading." A publication designated as official is not, in and of itself, "pre-eminent." (Black's Law Dictionary 2004, 1327). Nonetheless official legal resources invariably purport to be authoritative. They are often statutorily designated as a *prima facie* evidence of the law, entitled to judicial and administrative recognition (AALL etc. 2007a, 27–8). Official sources are authoritative, even if certain unofficial legal resources, sometimes easier to use, are similarly so regarded.

The *State-by-State Report on Authentication* determined that ten states – Alaska, Indiana, Maryland, Michigan, Minnesota, New Mexico, New York, Tennessee, Utah, and Virginia – plus the District of Columbia, have made no fewer than 23 sources of law available in online repositories that are considered official (Ibid 33). More important still, five of those states – Alaska, Indiana, New Mexico, Tennessee, and Utah – have declared the online versions of legal resources a substitute for the print official source. The online resource is therefore the sole official statement of the law (Ibid 37). This has happened primarily with administrative rules publications – generically, in US law, administrative codes and administrative registers. (Ibid)

As relatively recent developments, the UK has recognised as official *The Law Reports* series and specified

https://doi.org/10.1017/S1472669607002150 Published online by Cambridge University Press

a hierarchy of authoritative sources for citation in the court system. The Incorporated Council of Law Reporting publishes *The Law Reports*, as well as the *Weekly Law Reports*. The latter (along with the *All England Law Reports*) is authoritative for cases not published in the former. The Incorporated Council is a charitable organisation that nonetheless fully exercises a proprietary copyright in its publications. They are not freely available. (Matthews 2007, 23–4)

While the UK cannot be said to have official case law on the web, the situation with the newly released *Statute Law Database* (SLD) (at http://www.statutelaw.gov.uk/) is different. The SLD is an official database containing texts of all UK primary and secondary legislation that was in force as of the date (1 February 1991) when the print official *Statutes in Force* ceased being supplemented. (Holborn 2001, 54–5) The latter source, which constituted a subject arrangement of acts published as a loose-leaf, was discontinued altogether in 1996. (Ibid) The SLD provides an "Update status of legislation" page that currently explains that "[o]ver half of all items of revised legislation … already incorporate any effects on them contained in legislation made or enacted up to the present." (Ministry of Justice 2007a) A minority of items, which individually provide a warning notice, must be updated for "effects" – *i.e.* amendments and other applicable changes in laws – resulting from legislation covering 2002 to date. Moreover, some 28 acts have not been loaded into the database. Ibid) When the SLD is fully functional (projected to be late 2008), it will be current with all updating legislation.

The SLD is very noteworthy as a freely available online means to identify current official statutes as of any given date since early 1991. Once the complicated database fully begins to live up to its potential, its lack of strong authentication procedures is likely to become a deeper concern. As it stands now, it provides a disclaimer stating that "the Ministry of Justice makes every effort to ensure the accuracy and comprehensiveness of the data" but "accept[s] no legal liability for any errors or omissions." (Ministry of Justice 2007b). In many respects the SLD is potentially the most important test case for the UK (as well as the US) for understanding why authentication procedures matter. Significantly, there is no exact official print equivalent for the SLD and the courts are poised to begin relying completely on its "accuracy and comprehensiveness."

Other developments in the UK concerning public online legal resources help show the importance of authentication. The House of Lords, which is the final court of appeal on points of law for the whole of the United Kingdom in civil cases and for England, Wales and Northern Ireland in criminal cases, publishes its decisions on the UK Parliament website. Judgments starting from late 1996 are represented; HTML files with links to the PDF text are available staring with 2005. In addition, Her Majesty's Courts Service website (at http://www.hmcourts-service.gov.uk/) contains the text of judgments, starting from 1996, selected by the authoring judges from the wide spectrum of courts within that service.

These unofficial legal resources represent an important break from the British mould whereby the selection of court judgments for publication had previously always been solely in the hands of editors of independently published law reporters (Clinch 2001, 101). Equally important, government-published resources on the web represent a new form of official materials – referred to by some as "little o" official documents. There is an immediate connection between publishers and users on the web. When a court publishes a decision on the web, it can scarcely deny that it is an official publication, absent elaborate qualifications. Distinctions between "big O" official and "little o" official documents are arbitrary and meaningless to citizen users (Matthews 2007, 21).

What authentication procedures are required for official status? The *State-by-State Report on Authentication*, which appends a reprint of the U.S. Government Printing Office's final *Authentication* white paper (GPO 2005), was inspired by the federal government's efforts to define specifications for the FDsys, a system intended eventually to replace the bulk of print distribution of government information.

Such a total system demands strong authentication procedures. Specifications for the FDsys call for encryption, digital signatures, and public key infrastructure (PKI) technologies, described in the *Authentication* white paper and elsewhere (GPO 2006). ARJD, in its commitment to exclusive, single-source authority, calls for online court decisions authenticated by similar computerised processes, which will be sufficient to protect the documents from tampering and corruption. AALL's prescriptions are open-ended, although it is clear authentication ensuring the integrity of the particular digital copy delivered to users' own computer screens demands strong authentication procedures.

Context for authentication procedures

The national summit addressed strong authentication procedures and substantial background research and analysis and this and other aspects of authentication have informed the AALL stance from the very beginning of the survey project (*See* AALL etc. 2007a, 227).

To say an online legal resource is authentic is, in general, claiming one or the other (or both) of two things. Online materials are authentic insofar as they are preserved and made accessible through record-keeping systems and other repositories that are created and maintained according to rigorous archival standards. Because such repositories may not be a sufficient basis to ensure authenticity in certain contexts, encryption technologies, including digital signatures and PKI, are important additional tools. Those technologies may be incorporated

https://doi.org/10.1017/S1472669607002150 Published online by Cambridge University Press

into trusted repositories. For some materials or uses, they are indispensable. Where the latter is the case, those online materials are authentic to the extent that they can be authenticated – computationally shown to be unaltered.

AALL's national summit, which was unique in many respects, was not the first library-world event ever to be dedicated to authentication issues. The Council on Library and Information Resources convened a notable conference on authenticity – with proceedings published in *Authenticity in a Digital Environment*. (Cullen et al. 2000) The Council is a Washington, DC-based independent, non-profit organisation supporting new approaches to managing digital and other resources.

That conference invited experts from various disciplines to address a common set of questions. Insofar as the tenor of the interchange was the appreciation of multiple perspectives, the Council noted in its introduction to the proceedings:

> "Authenticity" in recorded information connotes precise, yet disparate, things in different contexts and communities. It can mean being original but also being faithful to an original; it can mean uncorrupted but also of clear and known provenance, "corrupt" or not. The word has specific meaning to an archivist and equally specific but different meaning to a rare book librarian, just as there are different criteria for assessing authenticity for published and unpublished materials. In each context, however, the concept of authenticity has profound implications for the task of cataloging and describing an item. It has equally profound ramifications for preservation by setting the parameters of what is preserved and, consequently, by what technique or series of techniques. (Ibid, vi)

The contribution of AALL's authentication survey and national summit to understanding of authenticity and authentication is inevitably informed by perspectives and values of law librarians and their allies concerned with legal information policy. Their approach includes advocacy of permanent public access, a far-reaching information policy to ensure "current, continuous and future public access" to government information on the web (AALL etc. 2003, 2). Such a concept demands archival control of materials.

Inevitably, authenticity and techniques for preservation and access are bound together, as archivists have demonstrated in the landmark InterPARES Project, discussed below. How online resources are maintained in record-keeping systems and other repositories ensures authenticity and, in turn, determines how resources are shown to be authentic. Ultimately, the archivist's way of answering what it means to say that online materials are authentic is demonstrating that those materials have been preserved and made accessible according to archival standards. The concerns of law librarians and others, regarding preservation and access, match up with archivist standards. Authentic materials are those bound to trusted repositories – trusted because they are created and maintained according to rigorous standards.

Archival methods

The InterPARES Project is a comprehensive exploration of archival foundations for authenticity. Archivists participating in the effort were systematically raising for the first time, for the archival profession, the question of authentication in the digital environment – particularly authentication of electronic records.

Searching for the right analytical approach for the topic, archivists initially determined to focus on the record level. The approach was a "theoretical and deductive one, based on contemporary archival diplomatics" (MacNeil 2002, 25). What does that mean? The archivists defined what an ideal archival record would consist of and prescribed it as the principal model for analysis. An authentic record could be said to be one that possesses the prescribed characteristics. Systems, if they are to maintain authentic materials, *should* have records with those ideal characteristics. To find a record with those ideal characteristics is to know it is authentic.

For evident reasons, this analytical approach has value – but it is not the complete picture, especially when dealing with web systems and web repositories, which may have unstructured characteristics. It is certainly possible that a record is authentic – that it is what it purports to be – without having the ideal characteristics.

The archivists' second analytical approach was "an inductive and empirical one that employed selected case studies of live electronic systems." (Ibid). What does that mean? They looked at the real world and identified characteristics of systems (not the records per se) that ensure authentic records. An authentic record is one that comes from a system with appropriate archival controls.

This too has merits, but also serious limitations, as the archivists ultimately recognised themselves. A powerful insight, well phrased:

> Empirically, it is not possible to preserve an electronic record: it is only possible to preserve the ability to reproduce the record. That is because it is not possible to store an electronic record in the documentary form in which it is capable of serving as a record. There is inevitably a substantial difference between the digital representation of the record in storage and the form in which it is presented for use. It is always necessary to use some software to translate the stored digital bits into the documentary form of the record. This entails an inevitable risk that, regardless of how well the digital data were protected in storage, the

https://doi.org/10.1017/S1472669607002150 Published online by Cambridge University Press

> record may be inappropriately altered when the stored bits are retrieved and presented for use as a record. (US-InterPARES Project, Preservation Task Force 2002, 5).

This insight points to encryption techniques as an indispensable authentication tool. At the end of 2006, archivists conducted a follow-up study to the InterPARES Project that fully explored the implications of digital materials found in varied formats and storage contexts. The title is InterPARES 2: Experiential, Interactive and Dynamic Records. The project was scheduled for completion in December 2006. A symposium reporting preliminary findings was recently held (23 February 2007) in Victoria, BC, Canada; another is planned for later in the year in Toronto. (Ministry of Labour and Citizens' Services 2007). A final report is not yet available.

Computational methods

According to the *Authentication* White Paper (GPO 2005), as well as GPO's *Strategic Vision* (2004) and *Future Digital System (FDsys) Concept of Operations* (2005), the Government Printing Office plans to create "an authentication system to verify the authenticity of digital content within the FDsys, and certify this to users accessing the content." Although its progress has been halting, in the nearer term, GPO is "implementing a Public Key Infrastructure (PKI) initiative to ensure the authenticity of … content on *GPO Access*." It recently released, for beta testing, authenticated versions of public and private laws for the 110th Congress (GPO 2007b).

GPO's public key infrastructure initiative employs digital signatures, in particular signatures to be associated with the superintendent of documents, certifying that signed materials are official and authentic. The science behind all of this ensures that a certified document is the uncorrupted text it purports to be.

How does it work? There are many easy-to-understand sources discussing digital signatures and PKI. *Records Management Guidance for PKI Digital Signature Authenticated and Secured Transaction Records*, a publication prepared for the federal cross-agency Chief Information Officers (CIO) Council and the National Archives and Records Administration (NARA etc. 2005), frames the issues squarely within our context. But a work such as *Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption*, by Warwick Ford and Michael Baum (2001), assumes less background knowledge.

Tracking Ford and Baum's overview, one starts with the concept of encryption. Fundamentally, encryption transforms ordinary content (words and numbers) into unintelligible data. Decryption results in the regeneration of the original text. An encryption key is responsible for the first transformation. Decryption requires a decryption key. A key is a seemingly random string of bits, a number to be plugged into the mathematical function (cryptographic algorithm) responsible for encryption or decryption (Ford and Baum 2001, 101). A public key "cryptosystem," which has one key kept secret and one key publicly disclosed, can be used for authentication. One can use the secret key to encrypt a text and distribute public keys to others who may wish to decrypt the encrypted text (Ibid, 105). By successfully decrypting a text with a public key, one can be certain the original text was encrypted with the secret key and that the decrypted text has integrity (Ibid, 107).

A digital signature is a data item that accompanies, or is logically associated with, an encrypted text and can be used to ascertain the originator of the text and show that the text has not been modified since it left the originator (Ibid, 109). It is the infrastructure part of the public key infrastructure that ensures a digital signature can be trusted. Ultimately, trust reposes in a third party certification authority – an institution functioning like a bank in the commerce system – that ensures a digital signature is that of a particular person (*See generally* ibid., 251–88).

The "near term" authentication system promised by GPO involves Adobe Acrobat technology and steps taken by GPO to utilise a third party certification authority. This is designed to ensure the integrity of certified PDF documents and a trustworthy connection between GPO and any such documents available on *GPO Access*. Documentation for the authenticated public and private laws beta release (GPO 2007b) describes the nature of the authentication procedures:

> When GPO certifies a PDF document, they attest to its content and disallow any changes to the document. This means that a document will no longer be certified if users replace, highlight, insert, underline, or cross-out text. Furthermore, the document will no longer be certified if users add pages, delete pages, or add comments. When GPO certifies a document, users will still be able to select text and then copy and paste text into a new document. [But the authenticity of the original will not carry over to the new document].
>
> 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 saves a document as certified and signed, 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 … (GPO 2007c).

The documentation provides instructions for validating digital signatures and includes PowerPoint presentations that demonstrate the validation process. (Ibid) Since

https://doi.org/10.1017/S1472669607002150 Published online by Cambridge University Press

access to the beta release materials has been irregular, it is worth noting that GPO has produced several certified PDF documents on its website, illustrating the features described for the beta test (GPO 2007d).

It appears GPO has made substantial progress on the FDsys. GPO reports that it has reached a stage of development where the system for all-digital publication will be publicly released for beta testing near the end of this year (GPO 2007a).

AALL's national summit addressed a variety of computational approaches to authentication (see AALL 2007b; Wrosch 2007). Encryption, digital signatures and PKI are leading technologies. Given the uptake of e-commerce and the wide adoption of provisions of the *Uniform Electronic Transactions Act* (UETA), related laws and institutions required for implementation of digital signatures and PKI are widely in place.

Computational authentication technologies vitally shape the concept of official status, although wisdom would dictate that no specific technology be named in laws requiring authentication measures. Technologies evolve too rapidly for that.

Ohio approach and components of a model

Ohio's approach in publishing judicial decisions on the web incorporates components of a model for authentication of US and UK online legal resources. Ralph W. Preston, the Reporter of Decisions for the Supreme Court of Ohio, and the court's network and resources department have quietly put in place encryption-based authentication procedures for all decisions, available as PDF files, searchable in the database on the Supreme Court website (at http://www.sconet.state.oh.us/). Preston, who participated in AALL's national summit, is currently co-chair of ARJD's Electronic Publishing Committee.

Ohio's judicial decisions on the web are unofficial. The state's approach to status and authentication has been very deliberate, although its use of authentication procedures is undocumented on the Supreme Court website. The High Court's database contains Supreme Court, Court of Appeals and other decisions starting from 1992. The formatting of decisions, which includes unique web citation information and numbering of paragraphs, enhances users' ability to cite the material in accord with the state's universal citation system. Where an opinion is also published in the state's print official reporter or the Thomson West unofficial regional reporter, the online version includes citation information for locating the text in those sources.

Pursuant to applicable court rules, selected Court of Appeals and other opinions are published in the print official *Ohio Appellate Reports* and the *Ohio Miscellaneous Reports*. According to Rule 9(C) of the *Ohio Rules of Court, Rules for Reporting of Opinions*:

> Should the Supreme Court cease publication of the Ohio Appellate Reports and the Ohio Miscellaneous Reports in a paper medium (which event shall not occur prior to July 1, 2006), the Supreme Court website may be designated the Ohio Official Reports for those opinions (Ohio Supreme Court 2007).

The date limitation mentioned in the rule corresponded to provisions of the state's contract with its official publisher, Thomson West. The contract has now been renewed for another five years. The print official publications will continue for at least as long.

The Ohio court rules potentially still could form the basis for designating certain online court opinions as official. Using authentication procedures positions the state for such a move. Additional steps, including a state official's certification of online texts as conforming to express standards for completeness and accuracy, might be essential to ensure official, authenticated court decisions in accord with the broad standards of AALL's *State-by-State Report on Authentication*.

As set forth in the final report of the fifty-state authentication survey, the Reporter of Decisions has described the process thus:

> Each new opinion to be added to the database published on the Supreme Court website comes to the Reporter of Decisions either as an MS Word or a WordPerfect document. Those in WordPerfect format are converted to MS Word prior to processing. Paragraph numbering and the opinion's web citation information are added to the document, and the opinion is then run through a software routine developed by the court's network and technology resources department. The software routine creates a version of the opinion in PDF format, removes any metadata and non-viewable information, adds the Supreme Court's digital signature to the document's metadata (encoded in the metadata using a hash function), and places the document in a "queue," ready to be released to the web server. At such time as the document is to be made accessible to the public, it is simply released from the "queue" and is then automatically moved by the software to the web server where it becomes visible in the index and retrievable from the web server (AALL etc. 2007a, 157a).

Prior to 2004, opinions had been published on the Supreme Court's website as MS Word documents without authentication. The Reporter of Decisions has indicated that "It was discovered in early 2004 that certain information thought to be non-viewable (hidden comments, tracked changes, etc.) could actually be seen when a document was opened by a much older version of a word processing program." Preston writes, "The

https://doi.org/10.1017/S1472669607002150 Published online by Cambridge University Press

Supreme Court decided that the correct approach going forward would be to make opinions available electronically only in PDF format and to digitally sign all opinions for authenticity purposes" (Ibid, 157b). Thus, in mid-2004, "all 30,000 previously-posted opinions were converted to PDF format, verified that accuracy had been maintained during the conversion, digitally signed, and reposted to the court's web page" (Ibid). Ohio now has approximately 50,000 opinions available on the web.

The Supreme Court website currently gives an "as is" disclaimer and makes no mention of authentication. Each court decision opened in Adobe Reader (version 7.0 or higher) has a tab, either labelled "signatures" or identified by an icon representing a pen and paper, incorporated into the document's frame. Under that tab, notations indicating that the document is "signed by the Supreme Court" are evidence of the court's use of authentication procedures.

The Ohio approach is not ideal in all respects. The judicial decisions are the only online legal resources known to utilise authentication procedures. The approach therefore represents important components of a model as contemplated by the *State-by-State Report on Authentication*. Use of strong authentication procedures is not necessarily costly or cumbersome. Encryption-based authentication avoids serious real-world problems encountered by publicly available legal resources on the web (AALL etc. 2007a, 157–157b).

Other questions and conclusion

Other questions addressed by AALL's national summit concern the extent of the actual need for the management overhead and expense involved in using authentication procedures. As discussed above, the case for authentication procedures is strongest where the online version of a legal resource is the sole official source of the information. The standard for official status of online case law set forth by ARJD's *Statement of Principles* (2007) essentially restates the strongest case. Official legal resources on the web should be the sole source if they are official and, moreover, they should be authenticated.

AALL may differ from ARJD on the question of multiple official sources. Where both online and print versions are official sources, is there less need for authentication procedures? Assessing the need for computational authentication procedures and an assurance that the particular copy delivered to a particular computer screen is authentic appears to turn on our understanding of how citizens and law researchers actually use online legal resources and, in the longer run, how they might use them were they assuredly reliable. There are pragmatic, as well as forecasting, even visionary, elements in this assessment.

The *State-by-State Report on Authentication* generally is uncommitted to any particular form of authentication, so long as the method is regarded as standard. That means that archival methods that may contemplate authentication on a case-by-case basis when the authenticity of an item is contested may be sufficient in some contexts. This must be understood against the growing recognition that online legal resources are increasingly the sole official source for citizens, regardless of the availability of print alternatives. They turn to the web rather than other sources. Equally important, limiting authentication to case-by-case methods limits the enormous potential of public legal resources on the web while the rest of the world is increasingly all-digital. The GPO specifies encryption-based authentication because the future digital system (FDsys) is a totalising effort to replace print. The path on which both the US and the UK appear to be embarked for the long term demands new ways of thinking about the trustworthiness of public online legal resources.

The impending all-digital future – the one that law librarians have a substantial stake in helping to create – is ultimately the reason why authentication procedures matter.

References

AALL, Access to Electronic Legal Information Committee and Washington Affairs Office. (2007a) *State-by-State Report on Authentication of Online Legal Resources*. Chicago, American Association of Law Libraries (as amended June 4, 2007). Available at http://www.aallnet.org/aallwash/authenreport.html.

AALL. (2007b) Authentic Legal Information in the Digital Age: AALL National Summit [webpage at http://www.aallnet.org/summit/default.asp]. Chicago, American Association of Law Libraries.

AALL, Government Relations Committee and Washington Affairs Office. (2003) *State-by-State Report on Permanent Public Access to Electronic Government Information*. Chicago, American Association of Law Libraries. Available at http://www.ll.georgetown.edu/aallwash/State_PPAreport.htm.

Association of Reporters of Judicial Decisions. (2007) *Statement of Principles: Official On-line Documents*. Available at http://arjd.washlaw.edu/ARJD_E-Pub_Committee_Authentication_Pos_Paper_FINAL_2–12–07.pdf

Black's Law Dictionary. 8th ed. (2004) St. Paul, MN, Thomson West (Bryan A. Garner, editor in chief).

Clinch Peter. (2001) *Using a Law Library: a Student's Guide to Legal Research Skills*. 2nd ed. London, Blackstone Press.

Cullen et al. (2000) *Authenticity in a Digital Environment*. Washington, DC, Council on Library and Information Resources. Available at http://www.clir.org/PUBS/reports/pub92/pub92.pdf.

https://doi.org/10.1017/S1472669607002150 Published online by Cambridge University Press

Ford Warwick and Michael S. Baum. 2nd ed. (2001) *Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption.* Upper Saddle River, NJ, Prentice Hall.

GPO, Office of Information Dissemination, Program Development Service. (2005) *Authentication* [agency white paper]. Washington, DC, US Government Printing Office. Available at http://www.gpoaccess.gov/authentication/AuthenticationWhitePaperFinal.pdf.

GPO, Office of the Chief Technical Officer. (2006) *Requirements Document (RD V2.1) for the Future Digital System (FDsys)*. [Washington, DC], US Government Printing Office. Available at http://www.gpo.gov/projects/pdfs/FDsys_RD_v2.1.pdf.

GPO. (2007a, as visited) Future digital system (FDsys), Current status [webpage at http://www.gpo.gov/projects/fdsys_status.htm]. Washington, DC, US Government Printing Office.

GPO. (2007b, as visited) GPO access, Authenticated public and private laws: Main page – beta release [webpage at http://fdlpdev.gov/plaws/index.html]. [Washington, DC], US Government Printing Office.

GPO. (2007c, as visited) GPO access, Authenticated public and private laws: About/help – beta release [webpage at http://fdlpdev.gov/plaws/index.html]. [Washington, DC], US Government Printing Office.

GPO. (2007d, as visited) GPO access, Authentication [webpage at www.gpoaccess.gov/authentication/]. [Washington, DC], US Government Printing Office.

Holborn Guy. (2001) *Butterworths Legal Research Guide*. 2nd ed. London, Butterworths LexisNexis.

MacNeil Heather. (2002) Providing grounds for trust II: The findings of the Authenticity Task Force of InterPARES. *Archivaria* 54 (Fall), 24–58. Available at http://journals.sfu.ca/archivar/index.php/archivaria/article/viewFile/12854/14078.

Matthews Richard J. (2006) The smart citizen's search for state law on the web: AALL authentication survey seeks to find out if there are official, authentic digital sources. *AALL Spectrum* 10(9), 20(5). Available at http://www.aallnet.org/products/pub_sp0607/pub_sp0607_Smart.pdf.

Matthews Richard J. (2007) When is case law on the web the "official" published source? Criteria, quandaries, and implications for the US and the UK. *Amicus Curiae: Journal of the Society for Advanced Legal Studies*. 69 (Spring), 19–25.

Ministry of Justice. (2007a, as visited) Update status of legislation [on UK statute law database website at http://www.statutelaw.gov.uk/Revised.aspx]. London, the Ministry.

Ministry of Justice. (2007b, as visited) Disclaimer [on UK statute law database website at http://www.statutelaw.gov.uk/Disclaimer.aspx]. London, the Ministry.

Ministry of Labour and Citizens' Services. (2007, as visited) InterPARES 2 Symposium. Victoria, BC, Government of British Columbia, the agency.

NARA, Federal Public Key Infrastructure Steering Committee Legal/Policy Working Group. (2005) *Records Management Guidance for PKI Digital Signature Authenticated and Secured Transaction Records*. [Washington, DC, National Archives and Records Administration. Available at http://www.archives.gov/records-mgmt/pdf/pki.pdf.

Ohio Supreme Court. (2007, as visited) *Ohio rules of court, Rules for reporting of opinions* [as amended effective 1 May 2002]. Available at http://www.sconet.state.oh.us/Rules/reporting/.

US-InterPARES Project, Preservation Task Force. (2002) *Preservation Task Force report*. In *Findings on the preservation of authentic electronic records: Final report to the National Historical Publications and Records Commission (grants # 99–073 and # 2001–005)*. US-InterPARES Project. Available at http://www.interpares.org/book/interpares_book_f_part3.pdf.

Wrosch Tom. (2207) Authentic legal information in the digital age: A national summit, Resources, Technologies [handout on file with author]. Chicago, American Association of Law Libraries. Bibliography identifies examples and further information on the following technologies: public record certification (e.g., technologies used by Kansas and Arizona to ensure authenticity of state-issued certificates of corporate good standing); high assurance/extended validation SSL certificates (e.g., Geotrust, Thawte, and Verisign); hashing and time-stamping (e.g., U.S. Postal Service Electronic Post Mark), PKI solutions (e.g., Adobe Acrobat).

Biography

Richard J. Matthews, J.D., M.L.I.S., was a 2006–2007 Visiting Fellow in Law Librarianship at the Institute of Advanced Legal Studies, University of London. As Chair of the 2005–2006 Access to Electronic Legal Information Committee, he led AALL's Authentication Survey and was Editor-in-Chief of the *State-by-State Report on Authentication of Online Legal Resources*. Matthews was a delegate and moderator-panelist at AALL's recent national summit titled *Authentic Legal Information in the Digital Age*. He has been a law librarian and administrator in various academic, court, and law firm libraries in the United States. Contact: rjmatthews2005@aim.com.

https://doi.org/10.1017/S1472669607002150 Published online by Cambridge University Press