ARTICLE:

JUSTICE AND SHERIFF: PRACTICAL AND AUTHORITATIVE METHODS FOR THE ELECTRONIC ISSUANCE OF OFFICIALLY CERTIFIED DOCUMENTS IN THE UNITED STATES

By **Timothy Reiniger, Esq.** and **Jacques R. Francoeur**

Practical methods have been established in the United States for issuing officially certified electronic documents, including confidential documents.[1] These developments fill voids that had previously prevented fully electronic court e-filing systems, including official attestation signatures. Examples of such methods include the first digitally signed judicial order in the United States federal court system, electronic state court processes for completing and issuing charging documents and domestic violence protective orders, authorization for court clerks to issue electronic certified records under electronic seals of court, and secure electronic notarization implementation. As discussed in this article, performing official acts electronically must include practices for creating authoritative source records so as to permit the logical extension of the legacy common law trust framework for authenticating paper documents to the digital equivalent.

At the same time, using the term "Open Government," President Barack Obama's Administration has called for government to use information technology, including cloud computing[2] and web service platforms, to enhance services to the citizen and promote greater citizen participation.[3] On June 25, 2010, the Obama Administration made available for public comment a "National Strategy for Trusted Identities in Cyberspace".[4] Both public and private sector participants view trust in on-line access to networks, the secure exchange of authentic information, and the overall identity ecosystem as essential to enable greater citizen use of government data and participation in the digital economy data.[5] In particular, for electronic documents to be reliable over time, a persistent document-level control and protection mechanism in the form of a self verifiable electronic seal or

[1] *This paper recognizes the distinction between certification and authentication of a document. An authenticated document is not necessarily certified. See, Taylor v. Commonwealth, 502 S.E.2d 113 (Va.App. 1998). (A certification involves an official representation or attestation that a particular act has or has not been done or that a certain fact is true while "[a]uthentication addresses the genuineness of a document.").*

[2] *CHARLES BABCOCK, MANAGEMENT STRATEGIES FOR THE CLOUD (McGraw Hill, 2010) at 4-16 and 221-225. Generally defined as non-client computer services, including infrastructure, software applications, platforms, and archiving maintained by third part providers.*

[3] *For example, see EXECUTIVE OFFICE OF THE PRESIDENT, ANALYTICAL PERSPECTIVES, BUDGET OF THE U.S. GOVERNMENT, FISCAL YEAR 2010 at 158 (Feb.26, 2009) at 158, available at http://www.gpoaccess.gov/usbudget/fy10/pdf/spec.pdf ("Initial [cloud computing] pilots conducted in collaboration with Federal agencies will serve as test beds to demonstrate capabilities, including appropriate security and privacy protection at or exceeding current best practices, developing standards, gathering data, and benchmarking costs and performance.").*

[4] *http://www.whitehouse.gov/blog/2010/06/25/national-strategy-trusted-identities-cyberspace.*

[5] *National Strategy for Trusted Identities in Cyberspace, at 4-6 and 23.*

There are two primary proof hurdles for authenticating digital documents — authenticity (origin and integrity) and reliability.

"trustmark" is necessary.[6]

Maturing methods and practices that combine persistent document-level detective controls (mechanism to detect alteration) and preventive controls (mechanism to prevent alteration), applied to electronic documents issued from trusted or authoritative official sources, best enable contemporary demands for open government and a digital economy and in a manner consistent with the foundational common law trust framework. Furthermore, these electronic information assurance methods are well positioned to providing the most effective techniques in meeting evidentiary self-authentication requirements.

Common law foundations

"Be ye ever so high, the law is above you"[7]

Document trust framework

An instructive record of early common law methods for creating reliable official paper documents is contained in *Justice and Sheriff*,[8] a book well known to generations of New Hampshire attorneys. Justice Bell quotes an early nineteenth century New Hampshire law that addresses a fundamental trust issue with paper documents – forgery:

> If any person shall falsely make or counterfeit, or fraudulently alter any public record, any writ process or proceeding of any court of this State; any certificate or attestation of a justice of the peace, notary public, clerk of any court, town clerk or other public officer, in any matter wherein such certificate or attestation may be received as legal proof...with intent that any person may be defrauded, he shall be punished by solitary imprisonment not exceeding six months, and by confinement to hard labor not less than three years nor more than seven years.[9]

The common law trust framework for official paper documents historically has consisted of certificates, signatures, and seals from reliable sources (i.e. judges, sheriffs, justices of the peace, notaries public, and constables). It is interesting to observe that the book contains 62 references to seal usage, 48 references to official certificates, and 42 references to signatures by hand.[10]

Document authentication

Digital evidence is subject to the same admissibility tests as paper records.[11] The Federal Rules of Evidence and the evidence rules of nearly every state provide that "[t]the requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."[12] However, the ephemeral nature of digital evidence and the ease with which digital objects can be undetectably modified make the problem of authentication much more complex than that of paper records and consequently even more critical in an electronic judicial system and digital economy.[13]

There are two primary proof hurdles for authenticating digital documents — authenticity (origin and integrity) and reliability.[14] Authenticity requires proof of origin (identification of the creator or authorized signer), content integrity (whether the document has been altered since its creation), and the time the assertion or attestation was made, executed, or issued.[15] A critical part of the authentication inquiry is whether effective safeguards have been implemented

[6] *National Strategy for Trusted Identities in Cyberspace, at 13-17 and 34 ("To maintain trustmark integrity, the trustmark itself must be resistant to tampering and forgery, participants should be able to both visually and electronically validate its authenticity.").*

[7] *GEOFFREY ROBERTSON, THE TYRANNICIDE BRIEF (Anchor Books, 2005) at 18. Rallying cry used in opposition to Charles I.*

[8] *SAMUEL D. BELL, JUSTICE AND SHERIFF: PRACTICAL FORMS (Concord, 1843).*

[9] *SAMUEL D. BELL, JUSTICE AND SHERIFF: PRACTICAL FORMS (Concord, 1843) at 418.*

[10] *For an analysis of the effect of custom and experience on the development of the substantive framework of common law practices and theories, see FREDERIC R. KELLOGG, OLIVER WENDALL HOLMES, JR., LEGAL THEORY AND JUDICIAL RESTRAINT (Cambridge University Press, 2007) at 46-60.*

[11] *Paul W. Grimm, Michael V. Ziccardi and Alexander W. Major, Back to the Future: Lorraine v. Markel American Insurance Co. and New Findings on the Admissibility of Electronically Stored Information, 42 Akron L. Rev. 357 (2009) at 362.*

[12] *FED. R. EVID. 901(a).*

[13] *STEPHEN MASON, ELECTRONIC EVIDENCE (LexisNexis Butterworths, 2nd edn, 2010) at § 2.04. See also PAUL, FOUNDATIONS OF DIGITAL EVIDENCE (American Bar Association, 2008) at 21.*

[14] *MASON, ELECTRONIC EVIDENCE, at §§ 4.08, 4.10, 4.19, 4.25.*

[15] *WINN & WRIGHT, THE LAW OF ELECTRONIC COMMERCE, § 20.05 (4th edn, Aspen Publishers, Inc., 2007); See generally George L. Paul, The 'Authenticity Crisis' in Real Evidence, 15 Prac. Litigator No. 6 (2004) at 212-13.*

by a reliable or trustworthy source to assure the continuing accuracy and integrity of the originally created record.[16] Thus identity, integrity, and time, recognized as the three main components of authenticity, must be implemented in a fashion that will allow strong tests, or verifiable proof, in the future when authentication is required as a prerequisite for admissibility or should questions of authenticity arise.[17]

A successful argument to establish a foundation of authenticity relies on a combination of extrinsic controls such as application and system access controls and audit logs, and intrinsic controls, such as encryption, time stamping, and digital signatures.[18] It should be noted that arguing authenticity solely through the use of extrinsic controls is complex and costly, and involves establishing the reliability of several external controls to the document systems and applications over time. On the other hand, the use of intrinsic content-level controls to prevent modification (such as encryption), to prevent and log access and use (for example document rights management),[19] and to detect modification (by the use of time stamps and digital signatures), provide a strong argument for the foundation of authenticity that does not depend on the reliability of external systems, other than those required to apply the intrinsic controls.

Self-Authentication

Under the Federal Rules of Evidence and the evidence rules of nearly every state, public documents under seal are admitted without further proof.[20] Specifically, FED. R. EVID. 902(1) requires that documents under seal of a public officer, including a judge, be treated as self-authenticating. The drafters of the Federal Rules of Evidence recognized that the risk of forgery is reduced by the requirement of authentication by a public officer who possesses and affixes a seal.[21]

Authentication of a document under seal involves the inference of three items: (1) the public officer is who he or she claims to be and is trusted; (2) the signature and seal are genuine; and (3) the signature and seal were affixed by the named public officer.[22] The seal must be kept under the exclusive possession and control of the public officer and not be used by any unauthorized person.[23] Therefore, sole control over the seal is required, whether in the manner of exclusive possessory control with a physical seal or strong access control in the case of an electronic seal.

Because an official act under seal is self-proving, both paper and electronic documents with a completed official certificate are rendered self-authenticating and admissible in court on their face.[24] The evidentiary effect of self-authentication is to permit admissibility by creating a rebuttable presumption of the authenticity of the document.[25] In addition to removing the need for a testifying witness, self-authentication also shifts the evidential burden to the opposing party of challenging the authenticity of the document.[26]

Digital trust framework: The authoritative source record

"Authoritative source record" refers to the official version issued by a reliable and mandated source, the

[16] *See In re Vinhnee, American Express Travel Related Service Co. Inc. v. Vinhnee, 336 B.R. 437 (9th Cir. B.A.P. 2005) (proponent failed to authenticate computer generated business records because of an inability to assure content integrity from the time they were originally created). See also, MASON, ELECTRONIC EVIDENCE, at § 4.19 ("In essence, reliability is associated with the degree of control exercised over the procedures that permit the data to be created.").*

[17] *GEORGE L. PAUL, FOUNDATIONS OF DIGITAL EVIDENCE, at 36.*

[18] *PAUL R. RICE, ELECTRONIC EVIDENCE LAW AND PRACTICE (American Bar Association 2005) at 249-256; note the difficulties with long-term conservation of digital signatures, in Stefanie Fischer-Dieskau and Daniel Wilke, 'Electronically signed documents: legal requirements and measures for their long-term conservation', Digital Evidence and Electronic Signature Law Review, 3 (2006) 40 – 44.*

[19] *STEPHEN MASON, ELECTRONIC SIGNATURES IN LAW (Tottel 2nd edn, 2007) § 15.43 (PKI infrastructure is useful for demonstrating the integrity of a message and providing confidentiality to a document).*

[20] *The following state rules of evidence incorporate in whole or in part FED R. EVID. 902 (1), (2), and (8), rendering as self-authenticating a document under a public officer's seal of office: ALA. R. EVID. 902; ALASKA R. EVID. 902; ARIZ. R. EVID. 902; ARK. R. EVID. 902; COLO. R. EVID. 902; DEL. UNIF. R. EVID. 902; FLA. ANN. STAT. § 90.902(1)(a) (acknowledgment act provision not included); HAW. R. EVID. 902; IDAHO R. EVID. 902; IND. R. EVID. 902; IOWA R. EVID. 90; KY. R. EVID. 5-902; LA. CODE EVID. ANN. ART. 902; MA RULES: MA GUIDE TO EVIDENCE , 902; ME. R. EVID. 902; MD. R. 5-902; MICH. R. EVID. 902; MINN. R. EVID. 902; MISS. R. EVID. 902 ; MONT. R. EVID 902; NEB. REV. STAT. § 27-90; N.H. R. EVID. 902; N.J. R. EVID. 902; N.M. R. EVID. 902; N.C. GEN. STAT. §8C-9-902; N.D. R. EVID. 902; OHIO R. EVID. 902; OKLA. STAT. TIT. 12 § 2902; OR. R. EVID. 902; PA. R. EVID. 902; R.I. R. EVID. 902; S.C. R. EVID. 902; S.D. R. EVID. 19-17-2 AND 19-17-9; TENN. R. EVID. 902; TEX. R. EVID. 902; UTAH R. EVID. 902; VT. R. EVID. 902; WASH. R. EVID. 902; W.VA. R. EVID. 902 ; WIS. STAT. § 909.02; WYO. R. EVID. 902. See also CAL. EVID. CODE § 1451 and § 1452(f).*

[21] *Advisory Committee Notes to FED. R. EVID. 902(2) (1972 Proposed Rules). See also Karla J. Elliott, The Notarial Seal – The Last Vestiges of Notaries Past, 31 J. Marshall L. Rev. 903, at 908 (1998) ("The embosser seal provides maximum safeguards against forgery and fraud by providing and obvious, tactile means by which to verify an original document.").*

[22] *7 JOHN WIGMORE, EVIDENCE § 2161 (1978).*

[23] *ALASKA STAT. § 44.50.064; ARIZ. REV. STAT. § 41-313(C)(1); ARK. CODE ANN. § 21-14-107(e); CAL. GOV' T CODE § 8207; COLO. REV. STAT. § 12-55-115; CONN. GEN. STAT. ANN. § 3-94j(a); 29 DEL. CODE § 4310(f); FLA. STAT. § 117.05[1](c); 5 ILL. COMP. STAT. ANN. § 312/7-107; MASS. GOV. EXEC. ORDER NO. 455 5[c] (April 2004); MISS. ADMIN. RULES § ; NEB. REV. STAT. § 64-113[1]; N.M. STAT. ANN. § 14-12A-18(A); N.D. CENT. CODE § 44-06-0; 57 PA.*

[24] *See generally EDWARD W. CLEARY, MCCORMACK ON EVIDENCE § 228 (3rd edn, 1984).*

[25] *EDWARD W. CLEARY, MCCORMACK ON EVIDENCE at 700; see also RICE, ELECTRONIC EVIDENCE LAW AND PRACTICE, at 248, 249.*

[26] *FED. R. EVID. 301. In many states, the presumption of due execution can be defeated only by clear and convincing evidence to the contrary. For example, see In Re: Adoption of X.J.A., 284 Kan. 853 (2007); Thompson v. Shell Western E&P Inc., 607 So.2d 37, 40 (Miss. 1992); Dencer v. Erb, 142 N.J. Eq. 422, 426 (Ch. 1948); Chianese v. Meier, 285 A.D.2d 314, 320, 729 N.Y.S.2d 460, 466 (1st Dept 2001); Wayt v. Urbigkit, 157 P.3d 1057, 1061 (Wy. 2007).*

reference, the single and only version of the truth, irrespective of who controls the document.[27] Specifically, an authoritative source record is an information object irrespective of format that is:

a) Designated by a public officer as the official and the only version of a fact or content being asserted.

b) Controlled and documented according to a clear and auditable document rights management policy governing access and use rights.

c) Demonstrably admissible in legal proceedings and compliant with applicable regulations, with an intrinsically derived chain of custody from the time the authoritative source record is declared until its final disposition (the chain of custody no longer depends on external systems and parties).

d) Verifiable as to its source (for instance via a validated digital certificate from the court clerk, county recorder, or Secretary of State) and authenticity (that it can be demonstrated to be what it purported to be at the time the assertion or attestation was made, an order executed or, more generally, e-mail was sent, contract was signed, report approved).

The persistent authenticity and control of an authoritative source record is based on intrinsic detective and preventive control mechanisms. A public officer declares an authoritative source record by the application of an intrinsic document-level mechanism such as a digital signature, an electronic seal, or time stamp. The authoritative source record is independent of the file container in which it is preserved.[28] The declaration event, which is an important component of the creation of an authoritative source record, cryptographically binds the document to its metadata, security and retention policies, trusted time, and source.

The authoritative source record is self-contained and self-verifiable and does not depend on any external system or application to determine its authenticity. This assumes the technology behind the creation of the record has been deemed reliable to a specific assurance level by an independent and credible third party.

The application of any required confidentiality or access and use restrictions is an intrinsic property of an authoritative source record. The court's document rights management policy aims to ensure persistent protection and control of the official act after it is created. Most importantly, usage rights prevent those individuals that have been granted rights of access from performing functions that may pose a risk (such as copying or printing). Access and usage rights are dynamic and can be immediately revoked or changed by the court at any time. This ensures that the generating public officer or court can, at all times, provide continual protection and dynamic content-level control and full audibility, even while the document is under the logical control of another individual or entity.

Official electronic signature: authoritative signature

"Caesar had his Brutus; Charles the First his Cromwell; and George III may profit by their example"[29]

System-Controlled signature

Digitally signing court orders with a high assurance digital certificate and time stamp has the effect of establishing each record as a "reference" or "authoritative source record" for relying parties.[30] This ensures the ability to test the authenticity and reliability of the information that was intended to be the equivalent of a paper "original."[31] Although the federal Electronic Signatures in Global and National Commerce Act ("E-SIGN") exempts court orders and filings from its scope,[32] the widely enacted Uniform Electronic Transactions Act ("UETA")[33] grants broad legal recognition, admissibility, and reciprocity to electronic

[27] *This is to be distinguished from the logic of a unique 'original' in the paper context. Some legal commentators consider the concept of an original to be meaningless as applied to digital objects. See MASON, ELECTRONIC EVIDENCE, at § 4.09, PAUL, FOUNDATIONS OF DIGITAL EVIDENCE, at 48, and Steven W. Teppler, 'Digital Data as Hearsay', Digital Evidence and Electronic Signature Law Review 6 (2009) 7 – 24, fn 18 at 9.*

[28] *Note the comments of Nicholas Bohm pertaining to challenges around linking information to a file container when a detached signature is used outside at trusted environment, 'Watch what you sign!', Digital Evidence and Electronic Signature Law Review, 3 (2006) 45 – 49.*

[29] *JAMES M. ELSON, PATRICK HENRY IN HIS SPEECHES AND WRITINGS AND IN THE WORDS OF HIS CONTEMPORARIES (Warwick House Publishers, 2007) at 55. Patrick Henry made this statement in opposition to the Stamp Act on May 30, 1765 before the Virginia House of Burgesses.*

[30] *PAUL, FOUNDATIONS OF DIGITAL EVIDENCE, at 56-59; Jacques Francoeur, Master Information Management and the Authoritative Source Record Life-Cycle Management Methodology, at 7 (SAIC, 2009) available at http://www.saic.com/news/resources.asp#.*

[31] *Paul W. Grimm, Michael V. Ziccardi and Alexander W. Major, Back to the Future: Lorraine v. Markel American Insurance Co. and New Findings on the Admissibility of Electronically Stored Information, 42 Akron L. Rev. 357 (2009) fn. 14 at pp 412-417.*

[32] *Electronic Signatures in Global and National Commerce Act ("E-SIGN") 15 U.S.C.A. §§ 7001 and following.*

[33] *UNIF. ELEC. TRANSACTIONS ACT ("UETA") § 11 (National Conference of Commissioners on Uniform State Laws 1999). The UETA has been adopted in every state and the District of Columbia except Illinois, New York, and Washington.*

signatures including court orders and electronic filings in both state and local federal courts.[34] In addition, UETA authorizes courts to specify the form of electronic signatures to be used.[35]

Under UETA, authentication of the origin and contents of a document to a particular individual is termed "attribution".[36] While not requiring the use of any one method to prove that an electronic signature is attributable to a person or document, the UETA importantly provides that attribution may be proved by means of a security procedure.[37] A certified official act performed in the manner of a security procedure both attributes the signature to the authorized person and renders the document self-proving.[38] As defined by section 2(14) of UETA, a security procedure is:

> A procedure employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the information in an electronic record. The term includes a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, or callback or other acknowledgment procedures.

Just as in the paper world, the signing act or certification by an official authenticates document by proving attribution of the electronic signature and document to the authorized signatory.[39]

Case studies

District of Columbia United States District Court – Court Orders

On August 26, 2009 in Washington, D.C., the Honorable John M. Facciola, Magistrate Judge for the U.S. District Court in the District of Columbia, became the first United States judge to digitally sign a judicial order.[40] Since that first event, Judge Facciola has been digitally signing official court orders. "The capability to sign electronically an order or other document should create in the people who see it an assurance that the document was signed by the judge and eliminate corrupt attempts to use forged, electronically created documents for improper ends," said Judge Facciola.[41] The judicial use of digital signatures in signing court orders signals a ground breaking opportunity for U.S. courts which, despite the widespread use of electronic filing systems, still require handwritten signatures by judges on paper. The ability to implement reliable digital signatures for court filings deals with this problem, while providing the legal confidence necessary to rely on documents that have been signed electronically.

Although the federal courts nationwide have made great strides in enabling the e-filing of pleadings, in the minds of many legal experts, they are overdue for a reliable, end-to-end electronic process that includes signing. In fact, otherwise efficient and cost-effective processes break down from a security viewpoint when paper-based signatures are required. Currently, in most courts only a "/s/" or typed name is needed for an electronic signature. "A fully electronic filing system -- that includes electronic [digital] signatures -- makes sense for America's courts," Judge Facciola said. "This is the next logical development in the transition from paper to electronic filing."[42]

To ensure judicial orders signed electronically are reliable and resistant to fraud and manipulation, Judge Facciola's signing method relies upon on a high

[34] *UETA § 7 ("A record or signature may not be denied legal effect or enforceability solely because it is in electronic form."), § 11 ("If a law requires a signature or record to be notarized, acknowledged, verified, or made under oath, the requirement is satisfied if the electronic signature of the person authorized to perform those acts, together with all other information required to be included by other applicable law, is attached to or logically associated with the signature or record."), and § 13 ("In a proceeding, evidence of a record or signature may not be excluded solely because it is in electronic form."). The three non-UETA states similarly grant legal recognition and reciprocity to electronic signatures: 5 ILL. COMP. STAT. ANN. § 175/5-110 and 5-130; 57-A of the New York Consolidated Laws, Article III Electronic Signatures and Records Act §§ 304 (2) and 306; NYCRR 540.1 (e); and WASH. REV. CODE ANN. § 19.34.320 and 321 (digital signatures only).*

[35] *UETA § 18.*

[36] *UETA, note 34, at § 9(a) and Comment.*

[37] *UETA, note 34, at § 9(a) and Comment.*

[38] *UETA at § 2(14); ARIZ. REV. STAT. § 41-351(9); DANIEL J. GREENWOOD, ELECTRONIC NOTARIZATION: WHY IT' S NEEDED, HOW IT WORKS, AND HOW IT CAN BE IMPLEMENTED TO ENABLE GREATER TRANSACTIONAL SECURITY at 10 (National Notary Association 2006) available at http://www.nationalnotary.org/commission; Paul, FOUNDATIONS OF DIGITAL EVIDENCE, at 212. The three states that have not enacted the UETA also recognize attribution by security procedure: 5 ILL. COMP. STAT. ANN. § 175/10-110(b) (authentication by security procedure expressly incorporated); 9 NYCRR 540.5(d) (procedures by government entities and public officers required for ensuring authenticity and integrity of records); and WASH. REV. CODE ANN. § 19.34.340 (authentication by digital signature).*

[39] *UETA at § 2(14); ARIZ. REV. STAT. § 41-351(9); DANIEL J. GREENWOOD, ELECTRONIC NOTARIZATION: WHY IT' S NEEDED, HOW IT WORKS, AND HOW IT CAN BE IMPLEMENTED TO ENABLE GREATER TRANSACTIONAL SECURITY at 10 (National Notary Association 2006)*

[40] *Timothy Reiniger and Jacques Francoeur, Federal Magistrate Sets Example for Digitally Signed Official Court Orders, EDDE Journal (Newsletter of the ABA Section Science & Technology Law) Volume 1 Issue 1 (Winter 2010), 14.*

[41] *Timothy Reiniger and Jacques Francoeur, Federal Magistrate Sets Example for Digitally Signed Official Court Orders, EDDE Journal (Newsletter of the ABA Section Science & Technology Law) Volume 1 Issue 1 (Winter 2010), 13.*

[42] *Timothy Reiniger and Jacques Francoeur, Federal Magistrate Sets Example for Digitally Signed Official Court Orders, EDDE Journal (Newsletter of the ABA Section Science & Technology Law) Volume 1 Issue 1 (Winter 2010), 14.*

assurance signing credential and process[43] comprising of a secure storage device containing the private key over which Judge Facciola has sole control by means of a two factor authentication process; a digital certificate based on strong in person identity vetting; a trusted time stamp from an accredited source; and a signing and rendering (viewing) application that provides any relying party with the ability to easily verify the authenticity of the order.[44] The judge's signing credential is issued and secured in accordance with an assurance level equivalent or greater to what the United States federal authorities refer to as Medium Assurance Hardware -- Federal Bridge Cross Certified.[45] That certification level is based on a high standard of reliability defined by the Federal PKI Management Authority.

A critical prerequisite before any digitally signed record should be relied upon is the verification of its authenticity. This is achieved by validating the digital signature which is accomplished by most applications by simply opening the document. The important validation questions are: whether the document has changed since it was signed, when was it signed, and whether it was signed by the person indicated in the digital certificate. Unfortunately, the process of reaching a judgment on the authenticity of a digitally signed document is still complex, because it is in part based on making a judgment on whether the digital certificate of the signatory was reliable at the time of signing. This is achieved by verifying the status of the digital certificate at the time of signing.[46] In order to make it easy for relying parties to validate a digital signature, the objective should ideally be that they do not need to know anything [e.g., about PKI] or do anything such as make configuration changes to their signing application or make any judgments about whether to trust the certificate and its source.

For validation to be automatic, critical information relating to the trust to be given to the document must already be included in the signature itself and the application in which the document is created, which is beyond the scope of this article.[47] It is possible to achieve this by using the current improvements of the most recent versions of the relevant application (for instance, Adobe). Ideally, the signature validation process should simply involve two steps – opening the document and looking for the "valid" indication icon that states the document is authentic (normally a green check mark). Any actions beyond this are more than the relying party should be expected to do. This assumes that the operational reliability of the issuing Certificate Authority can be determined and meets a specific assurance level. The reliability of the Certificate Authority is in part defined by its governing Certificate Policy or Certificate Practice Statement and independent third party audit assessments.[48] In the case of Judge Facciola, this trust level issue was established through the issuance of a Medium Assurance Hardware Federal Bridge Cross Certified signing credential, which has a prescribed and verified high level of assurance designed to mitigate forgery.

Minnesota e-Charging service

In March 2009, the Minnesota Bureau of Criminal Apprehension launched an e-Charging Service pilot

[43] *Jacques Francoeur and Ed Chase, Digital Assurance and the Digital Chain of Evidence, at 4 (SAIC and Adobe, 2008) (describing a reference architecture that measures the level of reliability of a digitally signed record) available at http://www.saic.com/news/resources.asp#.*

[44] *MASON, ELECTRONIC SIGNATURES IN LAW, at § 15.38 ("A digital signature can provide for the authenticity of information.").*

[45] *Appropriate uses for relying parties are described in the X.509 Certificate Policy for the Federal Bridge Certification Authority (Version 2.17 June 10, 2010) Section 1.4.1, available at http://www.idmanagement.gov/fpkipa/documents/FBCA_CP_RFC3647.pdf – "This level is relevant to environments where threats to data are high or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk." The introductory text to paragraph 1.4.1 provides that "Relying Parties must evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to accept based on the sensitivity or significance of the information. This evaluation is done by each Relying Party for its application and is not controlled by this CP." In addition, paragraph 1.3.6 in relation to Relying Parties, states in part: "A Relying Party uses a Subscriber's certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the Subscriber. The Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. A Relying Party may use information in the certificate (such as certificate policy identifiers) to determine the suitability of the certificate for a particular use."*

[46] *See ABA INFORMATION SECURITY COMMITTEE, SCIENCE AND TECHNOLOGY SECTION: DIGITAL SIGNATURE GUIDELINES (American Bar Association, 1996) at 14-15 and sections 1.8, 1.22, 1.29, 1.36, and 1.37. the certificate status information is included in the digital signature as either 1) a time stamped Certificate Revocation List (CRL) which indicates indirectly that the certificate of the signatory was not revoked prior to the time the signature was created or 2) an Online Certificate Status Protocol (OCSP) response which checks the actual validity status of the signatory's certificate.*

[47] *Jacques Francoeur and Ed Chase, Digital Assurance and the Digital Chain of Evidence, at § 3 (providing a neutral technical description of these requirements).*

[48] *Note the explanation provided by the Federal Bridge Certification Authority, available at http://www.idmanagement.gov/fpkia/crosscert.cfm: "When a PKI cross-certifies with the Federal PKI Architecture, and is an affiliate in good standing, a Relying Party operating an online application that utilizes digital certificates for electronic identity authentication may choose to trust that PKI's digital certificates at the Level(s) of Assurance asserted by those certificates. No other trust requirements are needed for the Relying Party to make that determination."*

program in St. Louis County for electronically preparing, signing, filing, and approving all criminal charging documents.[49] On June 30, 2010, the Minnesota Supreme Court approved the program for state-wide implementation with adoption of enabling amendments to the criminal procedure rules.[50] Criminal charging documents are now being signed, notarized, and filed electronically and in real time. Using the Minnesota Criminal Justice Data Network, system controlled digital signatures are used by the police officer, the notary (before whom the police officer signs the charging document under oath), the prosecutor, and the judge. The eCharging Service has resulted in an increase in the accuracy of entering the date entry, a reduction in lost police officer time spent traveling great distances to court, and a reduction in delays in holding individuals pending the decision to file a complaint and then obtaining approval from the court.

Illinois Orders of Protection

Since 2006, the Kane County Circuit Court in Illinois has been electronically processing and issuing domestic restraining orders or "Orders of Protection."[51] Utilizing the ease of use of the web and automated routing, a request for an order of protection can be initiated electronically by representatives of domestic violence victims, court personnel, attorneys, or victims themselves at one of four locations – the courthouse, the clerk's office, the sheriff's office, or a domestic victim's shelter. Regardless of who originates the order request, the forms then need to be acted upon by a judge, court clerk, and sheriff, all of whom sign with a digital signature. The clerk electronically certifies and stamps the finalized orders with a device controlled by the system before sending the orders to the sheriff. Because of the automated process, an order signed by a judge is instantly received by the sheriff's office. The Kane County Circuit Court has experienced a five-fold reduction in the time it takes to submit and process restraining orders.

Official electronic certificate: reliable record

"Sic semper tyrannis"[52]

Document integrity

As public officers, the official acts and certificates of judges and court clerks enjoy an evidentiary presumption of having been validly performed.[53] Accordingly, in the absence of rebuttal evidence, the official certificate or signature is self-proving, and the document is received into evidence without further proof of the official's authority or seal.[54] However, the certificate is not effective unless the signature and seal of the official are affixed.[55] The certificate, to which the official's signature and seal are affixed, provides prima facie or presumptive evidence of all attested facts including the identity and attribution of the principal.[56] With a quasi-judicial or notarial act, successful rebuttal

[49] *The story is available at http://www.govtech.com/gt/695238.*

[50] *MINN. R. CRIM. P. 1.06.*

[51] *The story is available at http://www.govtech.com/gt/articles/641095.*

[52] *Code of Virginia, Title 7.1, Chapter 4, Section 7.1-26. Motto of the Commonwealth of Virginia attributed to Brutus upon slaying Caesar.*

[53] *For instance, see Eveleigh v. Conness, 933 P.2d 675, 682 (Kan. 1997) ("[P]resumption that a public officer has performed the duties of his or her office faithfully"); Gombach v. Department of State, 692 A.2d 1127, 1132 (Pa. Commonw. Ct. 1997) ("[A] notary commission notifies the public that the Commonwealth believes the notary can be trusted properly."); In re Medlin, 201 B.R. 188, 192 (E.D. Tenn. 1996) ("[P]resumption that sworn public officers have properly executed their duties absent evidence to the contrary.").*

[54] *By statutory means, the following states presume the official character of the notary and the lawful performance of the duties: ALASKA STAT. § 09.63.060; ARIZ. REV. STAT. § 33-502(A); CAL. EVID. CODE § 1453(c) and § 1452(f) (notary's signature and seal presumed genuine); COLO. REV. STAT. § 12-55-204(1); 29 DEL. CODE § 4323(c); D.C. CODE ANN. § 42-143(c); GA. CODE ANN. § 9-10-113; 765 ILL. COMP. STAT. ANN. § 30/3(a); IND. CODE ANN. § 34-37-1-5; KAN. STAT. ANN. § 53-504; ME. REV. STAT. ANN. tit. 4 § 1012(1); MICH. COMP. LAWS § 565.263(1); MINN. STAT. ANN. § 358.43(c); MONT. CODE ANN. § 1-5-604(4); NEV. REV. STAT. ANN. § 240.1635(3); N.H. REV. STAT. ANN. § 456-B:3 III; N.M. STAT. ANN. § 14-14-3(C); N.C. GEN. STAT. § 10B-99(a) (notarial acts are given a presumption of regularity); N.D. CENT. CODE § 47-19-14.2(1); OKLA. STAT. ANN. tit. § 49-114(C); OR. REV. STAT. § 194.525(3); S.C. CODE ANN. § 25-1-630(E); VA. CODE ANN. § 55-118.2(a); WASH. REV. CODE ANN. § 42.44.080(9); W. VA. CODE ANN. § 39-1A-2(a); WIS. STAT. ANN. § 706.07(3)(c).*

[55] *Osborn v. Kemp, (Del. Ch. 8-20-2009) (the mere signature and seal of a notary public does not give rise to a presumption of genuineness to a photocopy).*

[56] *For instance, see CAL. EVID. CODE § 1451 (a certificate of acknowledgment or proof of a writing other than a will is prima facie evidence of the facts recited in the certificate and the signatures contained in the underlying document); COLO. REV. STAT. § 38-35-101(2) (prima facie evidence of proper execution of deed); IND. CODE ANN. § 32-21-9-2 and § 33-42-2-6 (certificate under seal is prima facie evidence of due execution); LA. CIV. CODE PROC. ART. 1836 (prima facie proof of due execution); MICH. COMP. LAWS § 55.307(1); MO. ANN. STAT. § 490.410 (prima facie evidence of due execution of deed); N.J. STAT. ANN. § 2A:82-17 (prima facie evidence of due execution); N.Y. CONS. LAWS § 137 Exec. (presumptive evidence of facts in certificate); 21 P. S. § 46 (certificate under seal is presumptive evidence of facts in certificate); UTAH CODE ANN. § 78-25-7 (2006) (prima facie evidence of due execution); WASH. REV. CODE ANN. § 64.08.050 (certificate under seal is prima facie evidence of due execution); WIS. STAT. ANN. § 134.01(4)(c) (presumptive evidence facts in certificate); and WYO. STAT. ANN. § 32-1-104(a) (presumptive evidence of facts in certificate). See also, UTAH CODE ANN. § 69-1-4 (2006) and WASH. REV. CODE ANN. § 5.52.050 (electronically transmitted instrument under seal is prima facie proof of due execution of the original). See also, Briggs v. Glass, 420 So.2d 46, 47 (Ala. 1982); Fares v. Morrison, 54 Cal.App.2d 773, 775 (1942); Westmoreland v. Tallent, 274 Ga. 172, 174 (2001); Curtis v. Curtis, 75 N.E.2d 881 (Ill. 1949); Valeriano-Cruz v. Neth, 14 Neb.App. 855, 861 (2006); Smith v. Smith, 44 A.D.3d 1081 (NY 3d Dept 2007); Limor v. Fleet Mortgage Group (In re Marsh), 12 S.W.3d 449, 453 (Tenn. 2000); Goodman v. Wachovia, 260 S.W.3d 699 (Tex. App.5th 2008) (acknowledgment proves or verifies identity of the signer); and Mortgage Associates, Inc. v. Hendricks, 51 Wis.2d 579 (1971).*

requires clear and convincing evidence by a disinterested witness of lack of physical appearance, failure to verify identify of the signer, or fraud.[57]

An international e-document authenticity standard has emerged for an electronic public document that reflects the evidentiary need for electronic documents to have the capability of testing the authenticity of the document.[58] This standard requires that any relying party be able to verify the origin and integrity of the electronic public document.[59] Establishing the authenticity of an electronic judicial order thus requires the capability, in perpetuity, of independently authenticating the origin of the document, and verifying whether the content of the electronic document is complete and unaltered. When the electronic official certification process is performed in the manner of a security procedure, by incorporating encryption or similar technology, subsequent changes to the electronic signatures and document can be detected.[60]

Case studies

Virginia Circuit Court Clerks[61]

Effective July, 2010, circuit court clerks in Virginia, who already had court e-filing and land title e-recording capabilities, may now issue official certificates and certified records electronically of any document maintained by the clerk. This marks the first time the circuit court clerks will be sending electronic official documents outside the court system's managed environment. In addition, the circuit court clerks may specify the security procedures, as defined by UETA 2(14), for attorneys to electronically file signed or notarized documents.[62] For an officially certified electronic document, the circuit court clerks use a digital signature and seal to enable detection of subsequent unauthorized alterations. Intrinsic document-level controls are required to enable dynamic and constant security of the document outside of the managed environment.[63]

Secretaries of State – Certificates of Authority

When a document executed in one jurisdiction is to be submitted in a court or office of another state or foreign jurisdiction, certification of the notary's identity and official status with a Certificate of Authority or an apostille may be required as a prerequisite for that document to be recognized or received into evidence in the other court or office.[64] State, county, and judicial officials have the legal obligation, when requested, to verify the authority of a notarial officer.

Standards for electronic Certificates of Authority have been established by the National Association of Secretaries of State ("NASS"). To maintain functional equivalence with certified public documents, including notarized documents, NASS has determined that certified electronic public documents and notarizations must meet certain basic requirements to ensure non-repudiation: the fact of the issuance of the certification must be independently verifiable and the certification must be invalidated if the underlying document is improperly modified.[65] Virginia and Delaware have enacted laws requiring that their respective Secretaries of State issue electronic certifications and apostilles under the secure electronic seal of the state.[66] The source of the document (the secretary of state's office), as reflected in the secretary's electronic signature and seal, must be capable of independent verification and the certificate must be invalidated if the underlying document is modified.

Kansas Secretary of State – Electronic Apostille Program

To effectuate legal recognition of notarized documents

[57] *For instance, see Colburn v. Mid-State Homes, Inc., 266 So.2d 865 (Ala. 1972) (the acknowledgment is conclusive of the facts therein absent proof of fraud or duress); Witt v. Panek, 97 N.E.2d 283, 285 (Ill. 1951) ("the certificate of acknowledgment can be overcome only by proof which is clear, convincing and satisfactory, and by disinterested witnesses"); Waitt Bros. Land, Inc. v. Montange, 257 N.W.2d 516 (Iowa 1977); Jensen v. Skibiski, 28 So.2d 328 (Fl. 1947) (being a quasi-judicial act, the acknowledgment is conclusive of the facts therein absent proof of fraud or duress); Murdock v. Nelms, 212 Va. 639, 641 (1972) (the acknowledgment is a judicial act that imparts absolute verity and cannot be impeached except for fraud); Evans v. Bottomlee, 148 S.E.2d 712 (WV 1966) (being a quasi-judicial act, the acknowledgment is conclusive and cannot be impeached except for clear and satisfactory proof of fraud or collusion).*

[58] *FIRST INTERNATIONAL FORUM ON E-NOTARIZATION AND E-APOSTILLES, Conclusions 15 and 18 (National Notary Association 2005) available at http://www.e-app.info/.*

[59] *FIRST INTERNATIONAL FORUM ON E-NOTARIZATION AND E-APOSTILLES, Conclusions 15 and 18 (National Notary Association 2005); see also NATIONAL E-NOTARIZATION STANDARDS, NATIONAL E-NOTARIZATION STANDARD (National Association of Secretaries of State 2006) Standards 14 and 15, available at http://www.nationalnotary.org/commission.*

[60] *ABA SUBCOMMITTEE ON ETRUST: ENW WHITEPAPER ON ENOTARIZATION at 3.3 (American Bar Association 2006) available at http://www.nationalnotary.org/commission. ("[T]he document being proffered must contain or be accompanied by evidence that it has not changed since it was first generated in its final form (see Section 12, UETA), or if it has changed, what those changes were and their significance, if any.").*

[61] *VA. CODE ANN. § 17.1-258.3:2.*

[62] *VA. CODE ANN. § 17.1-258.3.*

[63] *VA. CODE ANN. § 59.1-496(3).*

[64] *Keith D. Sherry, Comment, Old Treaties Never Die, They Just Lose Their Teeth: Authentication Needs of a Global Community Demand Retirement of the Hague Public Documents Convention, 31 J. MARSHALL L. REV. 1045-1083 (1998).*

[65] *NATIONAL E-NOTARIZATION STANDARDS, Standard 13.*

[66] *VA. CODE ANN. § 47.1-11.1(A) and 29 DEL. CODE § 4329 (a).*

that cross national borders, The Hague Conference on Private International Law (the "Hague Conference") oversees the Convention Abolishing the Requirement of Legalization for Foreign Public Documents (the "Convention"). The Hague Conference has determined that the spirit and letter of the Convention do not pose an obstacle to use of technology, and that the interpretation of the Convention in the light of functional equivalence permits competent authorities to issue electronic apostilles.[67] The Hague Conference encourages all competent authorities to issue e-apostilles.[68]

Under the auspices of the Electronic Apostille Pilot Program (e-APP) between the Hague Conference on Private International Law and the National Notary Association (USA), on February 15, 2007, the Kansas Secretary of State became the first competent authority in the United States join the e-APP and issue e-apostilles attached to electronically notarized documents.[69] The Secretary uses a digital certificate to affix the official digital signature and seal. For e-apostilles and electronically notarized documents, the Hague Conference has determined that electronic apostilles and notarial acts must ensure non-repudiation. Accordingly, the fact of issuance of an electronic public document, apostille, or notarial certificate must be independently verifiable and be invalidated if improperly modified.[70] These requirements do not mandate the use of a particular technology.[71]

Official electronic seal: trusted source

"Ense petit placidam sub libertate quietem"[72]

Document level control

The seal is a particular sign or written mark made to attest the formal execution of a document.[73] Information contained in the seal identifies the individual as a duly appointed public officer imbued with authority to perform official acts.[74] The seal authenticates or attributes the official act as the act of a notary.[75] The seal appears in one of four forms: 1) impressed or embossed sign, 2) imprinted or stamped sign, and 3) handwritten (scrolled) or typed mark, and 4) electronic image.[76]

By attaching the seal information to an electronic document in a manner that enables an independent verification of the officer, and provides a mechanism to demonstrate whether the document has been tampered with, the evidentiary function of rendering documents self-authenticating is preserved.[77] While *physically*

[67] *FIRST INTERNATIONAL FORUM ON E-NOTARIZATION AND E-APOSTILLES, fn. 51, Conclusion 1.*

[68] *FIRST INTERNATIONAL FORUM ON E-NOTARIZATION AND E-APOSTILLES, Conclusion 13.*

[69] *For more information about the e-APP, see Christophe Bernasconi and Rich Hansberger, "Electronic Apostille Pilot Program (e-APP): memorandum on some of the technical aspects underlying the suggested model for the issuance of electronic apostilles (e-apostilles)" available at http://www.hcch.net/upload/wop/genaff_pd18e2007.pdf.*

[70] *FIRST INTERNATIONAL FORUM ON E-NOTARIZATION AND E-APOSTILLES, Conclusions 15 and 18.*

[71] *FIRST INTERNATIONAL FORUM ON E-NOTARIZATION AND E-APOSTILLES, Conclusions 16 and 19.*

[72] *Massachusetts General Laws, Part 1, Title 1, Chapter 2, Section 1. Motto of the Commonwealth of Massachusetts contained in state seal based on the writing of Algernon Sidney, who Charles II executed in 1683.*

[73] *See CAL. CODE OF CIVIL PROCEDURE § 1930; MONT. CODE ANN. § 1-4-201; OR. REV. STAT. § 42.110; Van Den Borre v. State, 596 So.2d 687, 691 (Fla. App. 4. Dist. 1992); and King v. Guynes, 42 So. 959,960 (La. 1907) ("The purpose of a 'seal' is to attest in a formal manner to the execution of an instrument."). See also BLACK' S LAW DICTIONARY (West 1979) at 1210.*

[74] *"The seal ensures that the Notary's credentials are present and legible," Douglas M. Fischer, The Seal: Symbol of Security, NATIONAL NOTARY MAGAZINE, November 1995, at 12.*

[75] *ALA. CODE § 36-20-4; ALASKA STAT. § 44.50.062(5); ARIZ. REV. STAT. § 41-313(C)(3); CAL. GOV' T CODE § 8207; D.C. CODE ANN. § 1-1204; FLA. STAT. § 95.03; GA. CODE ANN. § 45-17-6; HAW. REV. STAT. ANN. § 456-3; 5 ILL. COMP. STAT. ANN. § 312/3-101; IND. CODE ANN. § 33-42-2-4(b) ("All notarial acts not attested by a seal as described in subsection (a) are void"); KAN. STAT. ANN. § 53-105; MD. CODE ANN. STATE GOV' T. § 18-108(a); MASS. GEN. LAWS ch. 59, § 31; MINN. STAT. ANN. § 359.03 SUBDIV. 1; MISS. CODE ANN. § 25-33-3 ("[A]nd his official acts shall be attested by his seal of office"); NEB. REV. STAT. § 64-210; NEV. REV. STAT. ANN. § 240.040; N.M. STAT. ANN. § 14-12A-18(B); N.D. CENT. CODE § 6-02-05; OKLA. STAT. ANN. tit. 49, § 5; OR. REV. STAT. § 194.152 (a document without an imprint of the official seal of the notary shall be of no effect); 57 PA. CONS. STAT. ANN. § 158; TENN. CODE ANN. § 66-22-110 (acknowledgment without a seal is void); TEX. GOV' T CODE ANN. § 406.013(a); UTAH CODE ANN. § 69-1-4; WASH. REV. CODE ANN. § 65.52.050; WIS. STAT. ANN. § 137.01(4)(b) WYO. STAT. ANN. § 32-1-106(a).*

[76] *See CORBIN, CONTRACTS §3241 (one volume edn, 1952) and RESTATEMENT (SECOND) OF CONTRACTS § 96 cmt. a (1981). Note that the legal construct of the official seal may also be denoted according to the device used to affix or attach the seal's image. An example of this is found in the Revised Uniform Law on Notarial Acts as approved by the National Conference of Commissioners on Uniform State Laws on July 16, 2010 § 2(8) available at http://www.nccusl.org ("Official stamp" means a physical image affixed to or embossed on a tangible record or an electronic image attached to or logically associated with an electronic record."). See also, MINN. STAT. ANN. § 359.03 SUBDIV. 2 (b) ("The official notarial stamp required by this section, whether applied to the record physically or electronically, is deemed to be a 'seal' for purposes of the admission of a document in court.").*

[77] *NATIONAL E-NOTARIZATION STANDARDS, "Form and Manner of Performing the Electronic Notarial Act," Comment ("Although UETA, URPERA, and the federal E-SIGN law can be read to have eliminated the need for a physical seal image as a requirement for determining whether an electronic document is an 'original' versus a copy, the seal requirement remains essential to authenticating documents under federal and state rules of evidence."). See also, H.R. 3808, 111th Cong., 2d Sess., 111 CONG. REC. S7558 (2010) ("Each court that operates under the jurisdiction of a State shall recognize any lawful notarization made by a notary public licensed or commissioned under the laws of a State other than the State where the court is located if...in the case of an electronic record, the seal information is securely attached to, or logically associated with, the electronic record so as to render the record tamper-resistant") available at http://thomas.loc.gov/cgi-bin/query/z?c111:H.R.3808:. For additional legislative background on H.R. 3808, see Hearing on H.R. 1458 Before the Subcommittee on Courts, the Internet, and Intellectual Property of the House Committee on the Judiciary, 109th Cong., 2d Sess., 4-8 (2006) (testimony of Timothy Reiniger) available at commdocs.house.gov/committees/...000/hju26412_of.htm.*

affixing the imprint or impress of the paper seal image does not apply to an electronic document, the information concerning the seal, including an image, nevertheless must be contained in the signature or the content of the document.[78] E-SIGN and the UETA defer to other state laws and regulations for direction on how the notary's electronic signature and seal information is to be attached to or contained in a document.

Case studies

DC Federal Court – Court Orders

This marks the first time a United States federal judge has adopted a process for issuing self-authenticating official documents in digital form.[79] Signed judicial orders and other official court certifications created from a high-assurance signing credential with a tamper-evident court seal image are self-proving, thus rendering the attached contents self-authenticating under Rule 902 of the Federal Rules of Evidence.[80] Judge Facciola's approach of including an intrinsic detective control in the document permits relying parties to test the document's origin, integrity of contents, and date and time of issuance without any need for extrinsic evidence. No external evidence is necessary because all the validation evidence, such as the validity status of the digital certificate at the time of signing, is included in the digital signature itself. Such a self-contained signature does not depend on external information to determine authenticity. After the validation establishes that the document is authentic, how the information is used depends on the relying party and the use to which the document is put.

Judge Facciola's manner of enabling self-authentication with respect to public documents is consistent with emerging laws and standards in the U.S. for officially certified electronic documents, including electronic notarization. The National e-Notarization Standards, issued by NASS, require an electronic notarization to give relying parties the ability to independently verify the notary and detect alterations to the signatures and document.[81] Laws reflecting this requirement have recently been enacted in Delaware, Florida, and Virginia. This standard reflects the need for a notarial act, like a judicial act, to be self-proving and to provide the capability of document authenticity testing and non-repudiation.[82]

State Court Clerks

To authenticate official acts and certifications in electronic form, court clerks in Hawaii must use an electronic seal that is "electronically imprinted" and is controlled by the clerk.[83] The certificate must also include an electronic image of the "electronic facsimile signature."[84] With effect from July 2010, every judge and circuit court clerk in Virginia must attach a secure electronic seal when signing or certifying an electronic document.[85] "Official electronic seal" is defined as "an electronic image of a seal or stamp, respectively, of the court or clerk, which is produced by software applications authorized by the clerk that are protected by system credentials to which only the clerk or persons authorized by the clerk have access." This authorizes judges and circuit court clerks to apply controls to a document that prevent changes being made without reference to the judge or clerk, thus enhancing the assertion of authenticity.

E-Notarization – Governmental Trusted Source for Seal

The Kansas legislature specifically authorized the Secretary of State to promulgate rules and regulations establishing procedures for an electronic notarization.[86] The rules, published with effect from December 30, 2005, require notaries to perform electronic notarial acts using only state-provided digital certificates.[87]

Delaware law now requires the electronic notarial act to be performed in the manner of a security procedure.[88] Specifically, the act must be independently verifiable and prevent subsequent alterations to the notarial

[78] *ABA SUBCOMMITTEE ON ETRUST: ENOTARIZATION, at 1.0.*

[79] *Lorraine v. Markel American Life Ins. Co., 241 F.R.D. 534 (D. Md. 2007) (recognizing that electronically stored information is subject to self-authentication under Rule 902 in its entirety). See also, Paul W. Grimm, Michael V. Ziccardi and Alexander W. Major, Back to the Future: Lorraine v. Markel American Insurance Co. and New Findings on the Admissibility of Electronically Stored Information, 42 Akron L. Rev. 357 (2009) at 384 (observing that courts and attorneys have been surprisingly slow to use Rule 902 when authenticating online records); note the comments of Brian W. Esler, 'Lorraine v. Markel: unnecessarily raising the standard for admissibility of electronic evidence', Digital Evidence and Electronic Signature Law Review, 4 (2007) 80 – 82.*

[80] *Paul, FOUNDATIONS OF DIGITAL EVIDENCE, at 211-212.*

[81] *NATIONAL E-NOTARIZATION STANDARDS, Standards 5 through to 11.*

[82] *NATIONAL E-NOTARIZATION STANDARDS, Standard 13 (National Association of Secretaries of State 2006). The American Bar Association defines the term "non-repudiation" as "[s]trong and substantial evidence of the identity of the signer of a message and of message integrity, sufficient to prevent a party from successfully denying the origin, submission or delivery of the message and the integrity of its contents." DIGITAL SIGNATURE GUIDELINES § 1.20 (American Bar Association 1996); note the discussion of 'non-repudiation' in MASON, ELECTRONIC SIGNATURES IN LAW, at § 14.20.*

[83] *HAW. REV. STAT. ANN. § 606-3(a).*

[84] *HAW. REV. STAT. ANN. § 606-3(b).*

[85] *VA. CODE ANN. § 17.1-258.4 (C).*

[86] *KAN. STAT. ANN. § 16-1611(b).*

[87] *KAN. ADMIN. REG. § 7-43-1(c) and § 7-43-2(c). Similarly, the Commonwealth of Pennsylvania requires notaries to use state-approved digital certificates to fulfill the electronic notary seal requirement. See 35 PA. B. 7068 (December 31, 2005) available at http://www.pabulletin.com/secure/data/vol35/35-53/2416.html.*

[88] *29 DEL. C. § 4322 (f).*

certificate and the underlying document. The Secretary of State requires notaries to use a state-issued digital certificate placed on a smart card. The performance of the electronic notarial act is protected by a two factor sole control authentication: the smart card (something you have) and a pass code (something you know) only known by the signatory. A unique aspect of the law is that it has extraterritorial reach throughout the United States.[89] Electronic notarial acts may be performed anywhere in the country, providing the notary is sponsored by a regulated industry, including banks, law offices, and title companies. Federal employees may also qualify.[90]

For court e-filing purposes, Wisconsin requires notaries to only use electronic signatures and seals issued by the court.[91] The electronic signing credentials and seals are confidential and must remain under the notary's exclusive control. Consistent with the common law trust framework for paper documents, the digital signature and seal from the electronic filing system satisfy the self-authentication provisions.[92]

The Electronic Seal or Trustmark: logical extension of common law trust framework

"Sigillum est cera impressa; quia cera, sine impressione non est sigillum."[93]

The creation of an authoritative source record produced through 1) the application of a digital seal or trustmark as the intrinsic detective control and 2) the application of a rights management policy as the intrinsic protective control, allows a court to provide its relying parties with a self verifying authentication method and to constantly dictate who has access to the authoritative source record, when it may be viewed or when it expires, and what may or may not be done with the record. Thus the information can be transmitted across the internet without the risk of modification or unauthorized access.

Officially certified electronic documents generated with "detective controls" (mechanisms to detect but not prevent unauthorized alterations) such as digital signatures, trustmarks, or trusted time stamps offer several benefits — for example, the ability to verify the source and authenticity of the document, the ability to prove that the document is what it purported to be from the time the assertion was made (that is, when the order was signed, the court record was attested, the contract was executed, or the approval was given), the ability to preserve relevant evidence such as access and usage activity and intrinsically derived chain of custody, and the ability to authenticate the document under the Federal Rules of Evidence without requiring that the organization's information management systems be demonstrated to be reliable, except those involved in the application of the detective controls such as digital signatures and preventive controls (mechanisms to prevent unauthorized access) such as encryption and document rights management technology.

Officially certified electronic documents generated with intrinsic document-level "preventive controls" measurably reduce the risks related to unintended disclosure or unauthorized access, since even if these undesirable events occur, the information remains protected and under control. These preventive controls are also dynamic in that access and usage rights that are initially granted can be changed over time and with immediate effect. In addition, access to the most current document can be ensured even if outdated versions have already been distributed. Methods in the United States for issuing officially certified electronic documents and judicial orders or, as referred to in this article, as authoritative source records, integrate both detective and preventive control technologies to enable official electronic documents to have persistent and dynamic content level protection and control irrespective of where they are located or under whose control they are.

Timothy Reiniger is an attorney specializing in information security and digital evidence, licensed to practice in California and New Hampshire. A member of the EDDE Committee, he is an Executive Vice President of Information Assurance Corporation and leads the Digital Services Consulting Group at FutureLaw, LLC, which is based in Richmond, Virginia. He contributed to George Paul, FOUNDATIONS OF DIGITAL EVIDENCE.

http://www.futurelaw.net
treiniger@futurelaw.net

Jacques Francoeur is Senior Director of Identity and Information Assurance, Commercial Business Services, at SAIC. He has written numerous industry white papers in the area of electronic evidence, including "Master Information Management and the Authoritative Source Record Life-Cycle Management Methodology" (2009) and "Digital Signature Assurance & Digital Chain of Evidence" (2008).

JACQUES.R.FRANCOEUR@saic.com

[89] *29 DEL. C. § 4322 (f).*
[90] *29 DEL. C. § 4322 (f).*
[91] *WIS. STAT. ANN. § 801.17 (11)(b).*
[92] *WIS. STAT. ANN. § 801.17 (11)(e).*
[93] *RESTATEMENT (SECOND) OF CONTRACTS § 96 cmt. a (1981). Common law legal principle developed by Lord Coke and quoted in Pierce v. Indseth, 106 U.S. 546, 549 (1882).*

