Massachusetts
Institute of
Technology

Electronic Notarization

Why It's Needed, How It Works, And How It Can Be Implemented To Enable Greater Transactional Security

Daniel J. Greenwood, Esq.

Director, E-Commerce Architecture Program
Massachusetts Institute of Technology
dang@media.mit.edu
www.civics.com

Published by the
National Notary Association

Electronic Notarization

Why It's Needed,
How It Works, And
How It Can Be Implemented
To Enable Greater Transactional Security

Table of Contents

Electronic Notarization

1. Introduction

A notarization, at its core, is just the process of a government-approved person[1] witnessing the signature of another person, and attesting to it by affixing a signature and seal on the signed document. Electronic[2] notarization, or "eNotarization," is simply the process of notarizing a signature on an electronic document by electronic methods. The methods that have been proposed to do this are varied and imaginative.

In a very simple example, a person seeking to have a digital[3] document notarized could type his name with a date at the bottom of the text, and then the notary could type his/her name, along with the date and the information on the notary seal. This process, however, lacks the security of the existing paper process, and would be prone to fraud and criminal exploitation. Without safeguards, of course, it would be possible for anyone to pretend to be a notary just by typing information on a screen.

The National Notary Association (NNA) defines electronic notarization as a notarial act, or any part thereof, that is executed electronically. By this definition, the NNA points out, eNotarization is already widespread throughout the United States, because record-keeping — one of the three key steps in any notarial act[4] — is already performed electronically around the nation by many notaries.

The current predominant method of paper-based notarization requires that the notary physically sign and stamp or emboss the paper document being notarized.[5] Such traditional notarizations can be difficult to forge, modify or erase, because the signatures and seals are impressed or embossed into the very fiber of the paper, and they explicitly track back to a government-commissioned notary who can verify the facts related to the notarial act. Though paper-based notarizations serve their purpose well, many of the documents now requiring notarization increasingly are visualized as part of electronic processes. This means that electronic notarizations are in ever-higher demand.

General laws at the state and federal level have cleared away some of the legal obstacles to electronic notarization.[6] However, significant hurdles remain, because the existing rules for paper-based notarial acts cannot accommodate the very different realities of non-physical media. While certain time-honored principles and practices of paper-based notarization still apply, such as screening the signer as a mandatory first step, rules for affixing a notary certificate on an electronic document and for keeping a digital record of an electronic act, the second and third key steps, have yet to be enacted in any widespread way among the states. New statutory and administrative rules are critically needed if electronic notarization is to be fully implemented, because eNotarization is distinctly different from traditional notarization.

The prospect of electronic notarization continues to raise many questions, including:

- Why would anybody want to notarize an electronic document in the first place? After all, aren't e-mails and word-processing documents informal and not legally binding?
- How can an electronic notarization be performed if digital documents are so easy to alter and typed signatures are so easy to forge?
- If there are reliable computers with protections like cryptography and authentication technologies, then why can't we just rely on that security and eliminate the human notary?

- If the technical and business processes now exist to perform electronic notarizations, are there any remaining legal or policy issues that could still cause problems?

- If notaries can secure and authenticate electronic documents, couldn't they also help protect other sectors of eBusiness?

Using these questions as an organizing framework, this white paper will provide a general primer on eNotarization and an introduction to the key security issues posed. This paper is intended for a general audience, including government and private sector decision-makers with responsibility over systems involving notarization. The paper will describe why eNotarization is needed in order to enable a wide range of transactions. It will also explain how a system of eNotarization can be implemented and how it might facilitate improvements and innovations in the way people work and interact. Finally, in view of the current prospects for eNotarization, we will present a range of recommendations.

This paper is the result of research at the E-Commerce Architecture Program of the Massachusetts Institute of Technology that has been supported by the National Notary Association. For more information, please consult those organizations at: http://ecitizen.mit.edu and www.nationalnotary.org.

2. From Pen and Paper to Keyboard and Console

Organizing Question: Why would anybody want to notarize an electronic document in the first place? After all, aren't e-mails and word processing documents informal and not legally binding?

Notarization has provided a highly valuable bulwark against frauds and identity crimes over the centuries.[7] Many sensitive instruments, ranging from real estate conveyances to powers of attorney to last wills and testaments, have always been vulnerable to exploitation by clever forgers and counterfeiters. This fact of life has not changed, but the methods of conducting important transactions are significantly different now. "Information technology"[8] is today a key tool for enabling all manner of business and government documents, communications and transactions. While it is certainly true that information technology is used to facilitate many unofficial and informal interactions along the way, there is also a variety of high-value, mission-critical, sensitive and official transactions that are now conducted electronically. Many of these transactions involve documents which must be notarized in order to prevent, detect and prosecute fraud.

The fact that notarization can be used not only to prevent fraud, but also to aid with the later investigation and prosecution of wrongdoers is important. The evidence of a transaction that is created and preserved as part of the normal notarial process, along with the potential testimony of the notary, can serve as a powerful deterrent to identity and other crimes, and as a tool for prosecutors seeking to convict those responsible.[9] Even if the wrongdoers have absconded to parts unknown, it is still sometimes very helpful to the victimized parties left behind to have positive proof that they were harmed by a crime and thus should not be held responsible for the resulting losses.

There are a number of security and enforceability advantages associated with notarization of paper documents. For example, the process of affixing a notary signature and seal on a paper document creates evidence linking the unique document to a particular signer. Also, notarization provides information about the particular government-commissioned notary who was present to witness and authenticate the signature. While witnessing the signature, the notary is also responsible for performing a rudimentary check that the signer of the document is acting without coercion and displaying awareness of the document

being notarized.[10] As important transactions involving notarized documents are conducted electronically, these types of security safeguards will continue to be needed. Thus, any electronic notarization will have to offer the same protective advantages as paper-based notarial acts, except a new combination of technology, policy, practices and standards will have to be used to effectuate the new method of notarization.

Any belief that e-mails and word processing documents are necessarily "informal and not legally binding" should have been dispelled by enactment of the federal "E-Sign" law[11] in 2000 and by the nearly universal legislative adoption of the UETA[12] by state governments, starting in 1999. These two acts accord electronic documents the same legal effect as paper instruments. Indeed, legal precedents have been in place even longer to recognize the enforceability of writings produced by electronic means.[13]

3. From Seal and Wax to Encryption and Hashing

Organizing Question: How can an electronic notarization be performed if digital documents are so easy to alter and typed signatures are so easy to forge?

The reason for paying careful attention to the technology, practices and standards used for eNotarization is that, without care, digital information is subject to the same kinds of fraudulent and exploitive attacks clever criminals launch against paper documents. For that matter, wholly new forms of assault are possible that are unique to digital systems.[14] In fact, surprisingly creative and efficient types of fraud can be perpetrated against computer-based systems. While there are good economic, business and cultural reasons for transitioning to electronic transactions and records, there are at the same time security and reliability vulnerabilities. For example, as mentioned earlier in this paper, there is almost no way to detect whether a typed signature or other information on a word-processing document has been altered, deleted or completely replaced. This would mean that an eNotarization consisting solely of the typed name of the signer, followed by the typed name of the notary along with all the information on the traditional notary seal could easily be forged or manipulated after the fact. To counterfeit or tamper with the seal or signature on a paper document, by contrast, leaves traces of incriminating evidence, such as abrasions and other surface inconsistencies or subtle but unique signature discrepancies. Forensic experts can detect these distinctions and thwart the fraud. On a digital document, by contrast, it may be impossible to determine whether, how or when a fraud took place unless new kinds of forensics are used and the underlying systems and applications create the right kind of evidence.

A digital image of the notary seal could be used and affixed to the digital document as part of an eNotarization process.[15] This would be a simple, though not necessarily very wise, method. Such a process does not speak to the need for some method of information security to detect whether the content has been altered and to authenticate the parties to the notarization. In addition, the process of simply affixing a digital image of a notarial seal by itself does not take advantage of the unique benefits of machine-readable data.

If the information on the seal were in some machine-readable form, such as ASCII[16] text or marked up in XML[17], then computer applications could access, store and act upon that data. For instance, a mortgage filing application at a county recorder's office could automatically detect whether a required eNotarization is present on the filing. In addition to performing the same sorts of checks that a clerk or other document handler would do on a notarized paper document, the device reading the application could validate the data on various other levels. The reader, for instance, could check whether the data on the document had changed since the notarization was performed, and it could

validate that the notary who conducted the notarization had a current commission at the time.[18]

While it is clear that merely using a digital image of a seal does not provide much value for eNotarization, it is also true that simply including the notarial information in machine-readable form by itself is of little utility. Rather, what is needed is some way to transmit that information within a secure, reliable and usable system. A system for eNotarization must at least perform the same functions as traditional notarization, and those functions must be supported and reflected by the surrounding technology, processes and standards. To understand how technologies, standards and business or government practices relate to eNotarization, the following examples are offered.

The Secure Closed System

A relatively simple and straightforward approach to the security problem is for a business utilizer of notarizations simply to employ secure software to facilitate its document work flow. Assuming that the partners of the business could access and use the application, then a wide range of long-established information security tools could be used to perform eNotarizations as part of an in-house system. For example, so-called "application layer security" includes many widely adopted protocols[19] and software modules that provide authentication, confidentiality, protection against tampering, and other features.

Application layer security can be implemented according to widely accepted open standards, such as SSL[20], SSH[21] and HTTPS[22], but it is more commonly found in proprietary or customized programs. This type of security can be finely tuned to integrate with existing software so as to ensure that individuals or groups are granted access and authorization to conduct particular transactions or functions. For example, a particular employee at a company could be designated as a notary based on his or her state-issued commission, and the company software could give this person account authorization rights to notarize documents for other employees. The eNotarization could use such security techniques as hash algorithms[23], encryption and application controls to show that an authorized notary performed the notarization, include the seal data, and detect whether any unauthorized changes had occurred. Additional layers of personnel procedures and internal controls could be set to ensure that only authorized notaries could perform an eNotarization and that the notary must have been physically present at the time of the document signing. Finally, secure computer logs can create archives of every event, indicating who notarized what and when, and company auditors can later review those logs to confirm they are in order.

The Secure Technology System

Some parties involved in eNotarization in the United States have advocated use of particular sophisticated technologies as a solution to the security issue. The most commonly advocated technology solution is called Public Key Infrastructure (PKI). In this complex system, cryptographic codes and third party service providers are supposed to effect mathematically provable trust. Using this process, any information scrambled by one code can only be unscrambled by a unique corresponding code.[24] Parties are identified by a "digital certificate" issued by a trusted third party — a "certification authority" — and containing one of those mathematical codes. Based on the name and the code in the digital certificate, other parties can know the identity of the person they are dealing with, and that confidentially encrypted data sent or received from that party has not been changed since the data was encrypted. Many state and national governments, as well as private sector entities, have attempted to use PKI as a method of creating secure, trusted relationships online. The prospect of using PKI to enable secure eNotarizations has often been entertained. However, because of the complexity, cost, infrastructure, slowness, relative immaturity, and

security flaws of the related technologies, PKI by itself has not arisen as a workable option, without compensating safeguards.

Biometrics is another often proposed secure technology approach. A biometric system measures the physiological attributes of a person, including such characteristics as fingerprints and retina or voice patterns. This data can be expressed as digital information and stored in a bar code, within computer memory fixed inside an eNotarization device, or even validated through a secure database over a network. Encryption can be used to prevent unauthorized individuals from accessing the digital copy of other representation of the biometric data. Some kind of access control or encryption is needed to prevent thieves from secretly copying the digitally represented biometric data and later feeding that information back into the computer system, effectively stealing the identity of another person. However, once biometric systems are secure, they can be very effective at authenticating individuals with a high degree of certainty. Electronic notarization systems have been proposed that contain biometric information from the notary and which allow the notary simply to apply a thumbprint to make an electronic signature as part of the notarization process.[25] Additional technologies are needed to tie the signatures of the notary and principal together and to affix or otherwise associate the information on the notary seal with the signed document.

The biometric component of eNotarization could fulfill the signature and authentication functions of a notarial act. Indeed, the technology of biometrics is so powerful at authenticating both the identity of the notary and that of the document signer that it can all but eliminate forgery when implemented securely. Conceivably, for example, a notarization might entail taking a digital image of the original signing of the document. This image, if framed correctly, could serve as a basis for facial recognition-based biometric authentication of the document signer in the event of a later dispute. One can imagine an implementation where the facial image of a person who signs a document could be matched against a database to ascertain and validate the signer's identity. The same validation could be based on a thumbprint or other biometric data.

The Document Authentication Number

The state of Colorado has pioneered a simple but effective solution to enable state regulation of electronic notarization.[26] It is called the Document Authentication Number, or DAN, and works like this:

In Colorado, this is an eleven-digit accounting number issued to each notary by the Secretary of State's accounting system. This number can be accessed and referenced by anybody. Like a white pages entry, it is unique but publicly accessible identification. The number will be searchable online to verify a notary's name, commission number, commission expiration date and other important information.

Second, each notary is issued multiple random numbers generated by the Secretary of State, who keeps a copy of each such number. Unlike the first number, these are kept confidential. They should be secured, just as is the notary's seal for paper-and-ink notarizations. One of these random, confidential numbers is used by the notary to "brand" every discrete eNotarization. The notary also has, associated with each confidential number, the relevant data that appears on the respective official seal, such as name, title, jurisdiction and commission expiration date. When used together, the Document Authentication Number and a randomly generated number assigned by the Secretary of State constitute the notary's electronic signature for a particular notarization.

In order to execute an eNotarization, the Colorado notary would simply affix to the electronic document both the private and public numbers, along with the

pertinent commission information. This could be done by manually "copying and pasting" the data from a document or spreadsheet or through easy-to-use software. Thereby, the notary has tied the document to the electronic notary signature. In effect, an electronic notarization has occurred.

A third party may validate the notarization, even years after the fact, through reference to the pertinent information on file with the Colorado Secretary of State. If a dispute arises regarding the notarized document, it is possible to identify the notary in question and review that notary's journal, which would include the name of the original signer and other key information about the transaction. Of course, it is also possible to have the notary personally report, or even testify if needed, as to the relevant facts.

While Colorado has developed the system described above as a simple and cost-effective initial method for enabling electronic notarizations, the state has also indicated that particular parties may apply additional technologies, practices and standards to their electronic notarizations. For example, if contracting parties wish to secure an electronically notarized document to ensure that any future unauthorized change to its text is detectable, they could agree on such measures as encrypting a message digest of the document. This is analogous to existing paper notarization, which allows notaries and signing parties to heighten the security of a notarized paper document through such tamper-preventive techniques as embossing its pages together, or putting the original document in a safe deposit box.

Advantages and Disadvantages

The approaches described above all offer certain advantages and disadvantages. The secure technology approaches, while offering theoretical reliability and non-repudiation[27] by participating parties, do not speak to the underlying business models, practices and policies needed to sustain a system of state-regulated notaries public. The secure closed system can offer unlimited flexibility, precisely because each company can develop or customize such systems to meet its particular needs; but closed systems are based on highly proprietary solutions and are often not particularly scalable or interoperable. Even so, standards such as those developed by the Mortgage Industry Standards Maintenance Organization (MISMO) and the Public Records Industry Association (PRIA) can be leveraged to increase the number of parties that could theoretically join a closed system. However, such private sector arrogation of the public sector role in oversight of notaries public may pose insoluble problems from a policy, legal and practical standpoint. How can notary regulators manage the advent of a large number of radically different closed implementations? Where will they find sufficient expertise and staff time to meaningfully protect the public and discharge their duties under statute?

On the other hand, a state-regulated system for eNotarization, such as those developed by Colorado and Arizona[28], can offer direct accountability and certain public protections. Yet, development of permanent technology and standards architectures governing eNotarization on a state-by-state basis, with gaps, inconsistencies and potential conflicts between them, can create significant impediments to interstate commerce and fly in the face of common sense.[29] To encourage statutory uniformity between states and to discourage electronic procedures that violate basic principles of traditional notarization (e.g., the necessity for the signer to appear before the notary at the time of the notarial act), the National Notary Association developed and published the Model Notary Act of 2002.[30] This model statute integrates paper-based and electronic procedures and contains the first comprehensive set of rules for registering electronically capable notaries and regulating their electronic acts. Eventually, harmonization of private sector approaches and public sector regulatory oversight will have to occur.

For the time being, however, the advent of a rich variety of different options is seeding a competitive and highly innovative young market for eNotarization.

4. From Humans to Machines and Back Again

Organizing Question: If there are reliable computers with protections like cryptography and authentication technologies, then why can't we just rely on that security and eliminate the human notary?

Some technology vendors insist that their systems are so secure that they may replace or be labeled as "eNotarization" and dispense with the human notary altogether. In fact, it is true that certain functions associated with the role of the electronically capable notary may be efficiently carried out without direct human intervention, such as protecting the integrity of an electronic document. And there are many examples of internal corporate systems that use tight control of employees and highly secure practices and systems to safeguard the integrity of their corporate records. However, there are other functions served by a notary that relate to screening signers for identity, volition and awareness that, as yet, no machine has been reliably and affordably able to accomplish.

A seminal article on the indispensability of the conscientious and well-trained human notary was written by Charles N. Faerber of the National Notary Association for *The John Marshall Law Review* (see 31 J. Marshall L. Rev. 749). As Mr. Faerber notes in "Being There: The Importance of Physical Presence to the Notary," a wide variety of frauds, crimes and exploitations are directly attributable to improper notarizations that occur without the personal presence of the notary at the time of the document's signing or acknowledgment. In other words, the active, hands-on role of a notary as a witness to the affixation or acknowledgment of a signature, and the role of the notarization as the official act describing and formalizing that witnessing, comprise a formidable bulwark against wrongdoers. In the typical scenario of document fraud, one person trying to steal from another by creating a falsely notarized document may — by cajolery, intimidation, deception, threat or other wile — influence a less-than-conscientious or untrained notary to attest untruly that an absent signer was present or that a stranger without evidence of identity was satisfactorily identified. In this way, a duped or duplicitous notary may be influenced to notarize a forged signature. By contrast, the knowledgeable and ethical notary public will reject any blandishments or bullying whose aim is to wrest a false attestation from the notary.[31]

"Satisfactory evidence of identity," according to the Model Notary Act of 2002 (§ 2-17) is:

> (1) at least one current document issued by a federal, state, or tribal government agency bearing the photographic image of the individual's face and signature and a physical description of the individual, though a properly stamped passport without a physical description is acceptable; or
>
> (2) the oath or affirmation of one credible witness unaffected by the document or transaction who is personally known to the notary and who personally knows the individual, or of 2 credible witnesses unaffected by the document or transaction who each personally knows the individual and shows to the notary documentary identification as described in Subparagraph (1) of this section.

When identity documentation is presented, the notary can leverage to the utmost the signer's in-person appearance and the valuable opportunity for close-up scrutiny by an experienced and reasoning human. Most obviously, the notary may refuse to proceed with a requested notarial act if the signer fails to produce required[32] or convincing evidence of identity. Through careful and clever inspection of an identity document, the notary may determine that the ID has been fraudulently altered to conform with the physical

appearance of the person presenting it, or that the document was obtained under false pretenses.[33] In addition, the conduct of the person when challenged to produce identity documents may reveal suspicious behavior.[34] These clues can help the notary decide whether to proceed with a notarization or to refuse due to compelling doubts about the identity and intent of the would-be signer. As a society, we may never be able to stop criminals from obtaining fraudulent identification documents, but notaries can pose a formidable obstacle and deterrent to these criminals and provide an independent record that may be the only evidence prosecutors have to convict a forger. Indeed, in protecting our identities from misappropriation, notaries are one of the most powerful weapons we have against the ever-increasing onslaught of identity crimes.

In addition to identifying and watching a particular person sign or acknowledge a document, the notary is also charged with the duty to ensure that the transaction is proper[35] in certain other respects related to the intent and volition of the signer. This duty is born of centuries of bitter experience and based on the fact that alert notaries can avert countless tragic injustices. Thus, notarization affords a kind of forward-deployed, preemptive, defensive protection against certain adverse eventualities.

One of the key reasons for requiring a signer to appear in person before a notary is the opportunity to screen this individual for duress. In the classic case, a person who signs with a gun to the head would be deemed ineligible for a notarization. However, most cases are not so simple. A notary's ability to detect signs of distress is only limited by that notary's experience, acuity, sensitivity and training. Another reason for the notary's in-person screening of document signers, as previously mentioned[36], is to ensure that the signer is aware of the document he or she is executing. Machine reasoning and artificial intelligence have not yet achieved the precision and reliability necessary to determine whether persons truly comprehend what they are doing when signing a document. Another human, however, may readily pick up on body language and other clues revealing incomprehension.[37] When necessary, a notary may proactively intervene and ask the signer probing questions to determine whether he or she is under duress and aware of what is going on.[38] The power of human signals processing and, if you will permit the term, human intuition, have time and again been shown to be effective obstacles to wrongdoing. While notaries are not responsible for anything like a full psychological assessment, the mere fact that they are present and screening for basic red-flag behaviors is a significant value.

5. From Generic Law to Specific Rules

Organizing Question: If the technical and business processes now exist to perform electronic notarizations, are there any remaining legal or policy issues that could still cause problems?

Great strides have already been made toward legally enabling eNotarization in the United States. However, because significant legal and policy challenges remain, the field of eNotarization, overall, is still in a relatively early stage of development. As mentioned[39], federal and uniform state statutes governing electronic signatures and transactions have eliminated some obstacles to the use of eNotarization, but more hurdles remain with respect to the need for detailed public law and policy guidelines. The remaining legal and policy issues to be resolved include the following:

1. GENERIC RULES AND GUIDELINES on eNotarization for state governments regulating notaries.

2. NON-GENERIC LEGAL REFORMS related to security that are specific to regulated vertical markets.

3. PUBLIC POLICY MECHANISMS to coordinate legal evolutions across states and economic sectors.

The maturing of a national legal infrastructure supporting eNotarization must develop hand in hand with innovations in technology, business models and practices related to eNotarization. To some extent, certain additional legal refinements will need to await further definition in the marketplace of eNotarization providers, users and relying parties. On the other hand, further legal reforms that will promote and support investment by the private sector in the technology and lines of business utilizing eNotarization are clearly necessary. The following key issues merit careful consideration by policy and lawmakers in government.

The Model Notary Act and the Uniform Real Property Electronic Recording Act

To enable and facilitate eNotarization, the Model Notary Act of 2002, or a substantially similar piece of legislation, must be enacted[40] in a uniform manner across the 50 states. In addition, the Uniform Real Property Electronic Recording Act (URPERA)[41], along with other helpful industry-specific reforms, should be enacted uniformly across the nation. While there exist today some basic statutes at the federal (i.e., E-Sign) and state (UETA) levels recognizing the legal efficacy of electronic signatures used by notaries public in performing official acts[42], these statutes fall far short of actually enabling and authorizing notaries to perform those acts. They also fail to define an electronic notarization, provide procedures for performing such an act, or to prescribe rules for qualifying and empowering eNotaries.[43] While the federal E-Sign law and state uniform laws clearly stipulate that a notarization will not be invalidated if it is performed by electronic means, the laws fail to address the many aspects of eNotarizations that need to be regulated.[44] Indeed, UETA's own "Draft Prefatory Notes" stress the Act's incompleteness:

> The deference of the Act to other substantive law does not negate the necessity of setting forth rules and standards for using electronic media.

Consider that states have long carefully regulated the mechanisms, processes, technology and practices related to paper-and-ink notarization. These regulations frequently include technical specifications related to the notarial seal and requirements that notaries sign their notarial certificates by hand.[45] Simply maintaining the same level of oversight and control that states currently exercise over paper-based notarization will require enactment or adoption of new rules for eNotarization.

One of the most important statutes governing implementation of eNotarization in the United States is the widely adopted Uniform Electronic Transactions Act. UETA was the model on which the federal Electronic Signatures in Global and National Commerce Act was based. UETA, as well as URPERA, both depend on designated government agents to develop and promulgate more detailed rules that are technology-specific, and that will be amended regularly to keep pace with changes in the markets for those technologies.[46] The matters that these regulators are expected to take into account include:

- TYPES OF TECHNOLOGY, including formats chosen and systems used, by which the electronic records, transactional data and signatures are generated, sent, communicated, received and stored.

- CONTROL PROCESSES AND PROCEDURES applicable to the data and transactions for adequate preservation, disposition, integrity, security, confidentiality and auditability.

- INTEROPERABILITY with other jurisdictions and organizations, including harmonization of technology implementations, consistency of business practices, and use of open standards or agreed proprietary standards.

The first two bullet points above address basic information technology-related factors that determine

whether an eNotarization should be considered valid or not. The third point addresses the concern that the detailed standards developed by government and industry not be allowed to evolve into conflicting regimes. UETA and URPERA both directly address this concern by including language promoting "interoperability" and "harmony" related to technology, procedures and practices across jurisdictions and industries.

On the question of which current state official or agency is best positioned to oversee development and implementation of rules for eNotarization, it would seem reasonable that it be the state officials and agencies now overseeing the notaries who perform paper-based notarizations. Indeed, the National Association of Secretaries of State, meeting in St. Paul, Minnesota, in July of 2005, issued a resolution affirming "the role of the Secretary of State or other notary commissioning entity as the sole authority to establish standards enabling electronic notarizations that will protect signature credibility, avoid identity fraud and provide accountability to the public in order to promote secure electronic commerce."

While E-Sign and UETA open the door to use of eNotarization nationally, they do not provide all of what is needed legally to walk fully through it.

Electronic Notarization Qualifies for Advantages of a 'Security Procedure'

While neither UETA or E-Sign expresses preference for particular technologies, there are some advantages attributed by these acts to the use of information security procedures in general. Under UETA, electronic notarization seems clearly to qualify as a security procedure, which the Act (§ 2[14]) defines as:

> (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.

As part of the eNotarization process, of course, a notary must authenticate the identity of the signer, either by reference to identification documents, or based upon personal knowledge. This is a procedure employed for the purpose of verifying that the electronically notarized record was in fact executed by the person whose name appears on it as principal. In addition, it is possible that a court would find that the notarization process, depending on how the electronic notarization was implemented, also constituted a procedure for detecting changes in the notarized record.

Assuming an electronic notarization qualifies as a security procedure, UETA provides several helpful legal advantages. First, this statute indicates that if the effectiveness of the security procedure can be shown, then the record may be legally attributed to the person who purportedly signed it. This means that, in the event a signer of an electronically notarized record were later falsely to deny having signed, then showing the efficacy of the electronic notary process used would be sufficient to bind that person to the record. Of course, the alleged signer would always be free to introduce evidence that, in the particular case, he or she was not in fact the signer, such as proof of an improperly utilized eNotarization device.

In addition to legal attribution of the signed record to the actual signer, UETA also allows for the shifting of responsibility for errors or changes in a record if a security procedure were used. Specifically, the statute (§ 10[1]) provides:

> If the parties have agreed to use a security procedure to detect changes or errors and one party has conformed to the procedure, but the other party has not, and the nonconforming party would have detected the change or error had that party also conformed, the conforming party may avoid the effect of the changed or erroneous electronic record.

The ability to avoid the legal effect of a changed or erroneous electronic record may be of significant value. Thus, it may be worthwhile for parties defensively to use electronic notarization as a security procedure in order to help control liability exposure and manage risk in electronic transactions. One must keep in mind, however, that this exemption from responsibility is relatively narrow, and only applies when the counter party has not used the security procedure to detect the error or change when it could have been detected.

E-Sign, UETA Inadequate by Themselves to Enable, Facilitate eNotarization

While E-Sign and UETA remove some hurdles to implementation of eNotarization nationally, they do not remove all of them. It continues to be true that states regulate, authorize and oversee the commissions of notaries in the United States, and they do so through statutes, regulations and official directives. UETA and URPERA both expressly envision the need for more detailed rules and policies in order for eNotarization to mature fully over the next several years. Statutes like URPERA, providing the next level of specificity at a vertical market level, and the Model Notary Act, providing needed detail on the authorization and oversight of eNotaries, are needed to complete the panoply of public laws supporting eNotarization.

An implementation of eNotarization that fails to address the matters highlighted above related to technology, process and interoperability would be prone to fraud, error and inefficiency. Those who regulate notaries public would be derelict in their duty if they failed to effect the rule-making necessary to transition to a reliable system of eNotarization. Failing to exercise oversight and control in this area would be akin to failing to provide and enforce safety rules for hydrogen or hybrid cars because the new technology is different from the old.

Leaving those who rely upon notarizations to guess whether any general implementation of eNotarization is adequate may also raise constitutional problems. The Due Process and Equal Protection clauses of the U.S. Constitution require laws with criminal penalties to be sufficiently clear and precise so that any reasonable person would know what conduct was permitted and prohibited. Failure to provide a requisite level of detail risks the chance that courts will strike down the laws for vagueness or excessive breadth.

As there are criminal penalties related to misconduct in performing notarial acts, it is a matter of good public policy and plain common sense to require that state regulators of notaries provide at least the same level of regulatory clarity for eNotarization as has been provided for traditional notarization. Failing to provide minimally adequate guidance and controls governing notarization — in both traditional and electronic forms — will result in increased fraud, crime and exploitation targeting business, government and the citizenry. From real estate conveyances to international adoptions to last wills and testaments, people and institutions rely upon notaries to be intelligently regulated by government as a front line of defense protecting our property and rights under the law.

6. From eNotarization to Other Roles in eBusiness

Organizing Question: If notaries can secure and authenticate electronic documents, couldn't they also help protect other sectors of eBusiness?

In the future, one can imagine a robust suite of additional roles and services provided by electronically capable notaries. For instance, a notary who is physically present with an end-user of a highly secure system could verify that the person signing on, or executing a command, on that system is in fact the individual that he or she purports to be. The need for secure sign-on, including highly reliable authentication

and authorization linkages, is one of the key challenges to the online conduct of important, high-value and sensitive transactions. If eNotarization could be leveraged as a relatively inexpensive and accessible method of ensuring the integrity of important electronic transactions in business and government, much time and money could be saved. Currently, it is not unusual for high-ranking executives and public officials to fly across continents and oceans in order to formalize the execution of a contract or the closing of a negotiation. Of course, the human, social and ceremonial element of in-person contact at the start, middle and end of a negotiation serve important purposes. However, the inordinate reliance on travel and overnight courier services currently adding to the cost of doing business constitutes a considerable aggregate drag on the economy, as well as on individual businesses and government agencies. Cost and time-saving solutions are needed, and it is possible that "electronic notaries" are one such solution.[47]

Other potential additional value-added roles for eNotaries could include the secure original enrollment of a person into a digital system. For example, if a trusted, trained and professional electronically capable notary were to attest to identity and other facts related to a person's enrollment on an online transactional system, much more confidence could be had that the users of that system were not sophisticated con artists. In addition, electronic notaries could provide trusted reputation or introduction services for people interacting online. The weight of a reputation, based on trusted people who are personally known to other trusted people, is a heavy benefit for an online system. Currently, the value of being personally known to a notary is already afforded greater weight under the law, because such people do not need to present the notary with identity documents. One can also imagine the increased future need for a trusted, regulated party to certify digitally the accuracy and integrity of official or important electronic information. By providing an electronic notarization of sorts to digital video, databases and other electronic systems, it is possible to determine whether the data has changed since a given point in time. The specter of losing trust in video and other digital systems due to the ease with which images, sounds and other symbols can be edited in or out is growing. Electronically capable notaries could provide one of the countermeasures to ensure that our official and important records are trustworthy over time.

7. Next Steps

In view of the important role eNotarization holds in the current economic, governmental and societal shift into the information age, a sound strategy for transitioning to this valuable new mechanism is needed. The strategy requires actions by government, industry, vendors, professional associations and academia. Government will have to adopt more complete legal standards, including model and uniform statutes governing eNotarization, as well as the more detailed rules, guidance and policy necessary to implement those laws. These statutes, regulations and other mechanisms of public policy will need to be coordinated across local and state jurisdictions to ensure that consistent and harmonious national infrastructures develop. Balkanization between localities or states would be deleterious to interstate commerce and against basic national public policy.

In addition, businesses that rely heavily on paper notarization now must work closely with all the relevant stakeholders as they determine which technologies, standards and practices they will adopt for their business, their vertical market and their sector of the economy. Interoperability and consistency across the many different private sector systems will eventually be necessary to prevent stratification of approaches that are too numerous, complex and different to be overseen effectively by governmental officials. Similarly, technology vendors and other providers will need to

play an even more active role in creating products, services and standards as solutions that are efficient and interoperable.

It will be particularly important for proactive involvement by the open standards organizations that develop the basic specifications and protocols defining Internet data and communications. Open standards, developed according to fair, transparent and representative processes, have been a critical aid to the maturation of eCommerce, and can serve an equally fundamental role for eNotarization.

Finally, it will be necessary to attract, train, develop and retain the dedicated corps of individuals necessary to keep eNotarization professional, reliable and effective. The National Notary Association and other professional associations for notaries must play their role, as must academia, in defining and teaching the correct bodies of knowledge, skill and behavior. From law schools to business schools, and from vocational courses to engineering or computer science curricula, a body of highly trained, skilled and trustworthy individuals will need to step forward as stewards of eNotarization in order to provide secure authentication and effective electronic transactions in this burgeoning digital age.

8. End Notes

1. This "government-approved person" is commonly called a "notary public." Here are two different definitions of the modern notary's role in the United States: (a) "A notary is a person of proven integrity commissioned by the state to serve the public as an official, impartial witness. In the most basic of terms, the notary has the power to witness the signing of documents and to administer oaths. Most often, the notary's duties involve signed documents and require the notary to ensure a signer's identity and willingness to sign." (*Notary Home Study Course*, 9th Ed., 2003, National Notary Association) (b) "A (notary is a) public officer whose function it is to administer oaths; to attest and certify, by his hand and official seal, certain classes of documents, in order to give them credit and authenticity in foreign jurisdictions; to take acknowledgment of deeds and other conveyances, and certify the same; and to perform certain official acts, chiefly in commercial matters, such as the protesting of notes and bills, the noting of foreign drafts, and marine protests in cases of loss or damage." (*Black's Law Dictionary*, Rev. 4th Ed., 1968, West Publishing Co.)

2. In using the word "electronic," this paper adopts the definition of the Uniform Electronic Transactions Act (UETA), as adopted by the National Conference of Commissioners on Uniform State Laws in 1999: "'Electronic' means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities." The paper also adopts UETA's definition of an "electronic signature" as "an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record." UETA eschews the term "electronic document" in favor of "electronic record," which it defines as "a record created, generated, sent, communicated, received, or stored by electronic means."

3. "Digital" in this paper refers to computer-generated or computer-related systems. The term derives from the fact that computer data is expressed through digits or numbers — namely, the positive number 1 and the non-positive number zero. This "on-or-off" system contrasts with analog systems that express data through modulation of a continuous spectrum of values.

4. The other two key steps of a notarial act are screening the document signer for identity, volition and awareness, and completing a certification on

the document. A full discussion of the steps may be found in the *Notary Home Study Course* — see Note 1 above — in Part II, "The Essential Steps." This paper has addressed most lengthily the third step, completing a certification on the electronic document, the part of an eNotarization that the uninitiated often regard as comprising the totality of the notarial act.

5. Seal use by notaries is the rule rather than the exception, with 44 out of 56 U.S. states and territorial jurisdictions having a law requiring a physical imprint of an official embossing seal or inking stamp or both. Eleven of the remaining 12 jurisdictions that do not have a formal seal requirement have a law that notaries must "print, typewrite, or stamp" (N.Y. Exec. Law § 137) such information as the notary's name, county, and commission expiration date on each document the notary signs and notarizes — a seal requirement in all but name only. Since the Uniform Electronic Transactions Act requires seal "information" to be attached to or logically associated with the notary's electronic signature on the electronic record, seal use by notaries on paper and electronic documents is universal, with the exception of the state of Vermont. For further information on seal and other requirements for notaries in the United States, see *U.S. Notary Reference Manual*, 2006–2007 Ed., National Notary Association).

6. These laws recognize that electronic documents and signatures, including signatures affixed in an official capacity by notaries, can have the same legal effect as paper documents and pen-and-ink signatures. The federal statute is the Electronic Signatures in Global and National Commerce Act of 2000 (15 U.S.C.A. §§ 7001 *et seq*.), widely known as "E-Sign." The state laws are the various adaptations of the Uniform Electronic Transactions Act (UETA) legislatively enacted in virtually every state, starting with California in 1999. E-Sign is modeled after UETA and adopts many of its definitions. See also Notes 2 and 11.

7. The origins of the office of notary public actually date back over 2,000 years to the days of the Roman Empire, when scribes using a shorthand system known as *notae* were called *notarii*. For an authoritative history of the notary office, see *Origen e Historia del Notariado*, Eduardo Bautista Ponde, Depalma (1967).

8. "Information technology" refers to the computer hardware, software and other associated systems and processes that are used to store, retrieve and manipulate data. Today, "IT" departments in business and government organizations are commonplace.

9. A dramatic example of the value of a notary journal as a deterrent and a prosecutorial tool occurred in the state of California in the early 1990s. To help deter unscrupulous home repair salesmen from victimizing inner city homeowners in the wake of the Los Angeles riots, a three-year pilot program required Los Angeles County notaries to secure in their journals the right thumbprint of each real property deed signer. The program was so successful in reducing real estate fraud in the county that the California Legislature enacted the journal thumbprint requirement statewide, effective January 1, 1996. See California Government Code § 8206(G).

10. Ensuring that document signers are entering into transactions "with eyes wide open" is a statutory requirement for notaries in some states and a common sense practice for notaries everywhere. In the state of Georgia, for example, notaries must not notarize for any signer "whose demeanor causes compelling doubts about whether the person knows the consequences of the transaction requiring the notarial act." (Ga. Code Ann. § 45-

17-18[b]) *The Notary Public Code of Professional Responsibility* (1998), promulgated by the National Notary Association as an ethical code for the nation's notaries, states: "The notary shall not notarize for any person if the notary has a reasonable belief that can be articulated that the person at the moment is not aware of the significance of the transaction requiring a notarial act." (Standard III-C-1)

11. Using an electronic signature, fittingly, President Bill Clinton signed the federal Electronic Signatures in Global and National Commerce Act ("E-Sign") into law (15 U.S.C.A. §§ 7001 *et seq*.) in 2000. Modeled in large part after the Uniform Electronic Transactions Act (UETA), this federal statute recognizes that electronic documents and signatures, including signatures affixed in an official capacity by notaries, can have the same legal effect as paper documents and pen-and-ink signatures.

12. See Notes 2, 5 and 6 above.

13. Electrically produced writings have been accepted as legal documents as far back as 1869 — Howley v. Whipple, 48 N.H. 487 (1869): "(W)hen a contract is made by telegraph, which must be in writing by the statute of frauds…it makes no difference whether (the company's) operator writes the offer or the acceptance in the presence of his principal and by his express direction, with a steel pen an inch long attached to an ordinary penholder, or whether his pen be a copper wire a thousand miles long. In either case the thought is communicated to the paper by the use of the finger resting upon the pen; nor does it make any difference that in one case common record ink is used, while in the other case a more subtle fluid, known as electricity, performs the same office."

14. Such a digital assault was brought to light in March of 2005 when the San Diego (California) District Attorney began prosecution of a local company for using the digitally stored notary seal image of a former employee to create false notarizations on hundreds of affidavits.

15. The State of California, for example, requires any electronic notary seal to contain every graphic element of an inking seal used to authenticate a paper document — including the Great Seal of California. See Cal. Gov. Code § 8207.

16. ASCII is the acronym for the American Standard Code for Information Interchange, which is a system for representing English-language characters as numbers, with each letter given a number designation from 0 to 127. The ASCII designation for uppercase "B," for example, is 66. Because most computers use ASCII codes to represent written text, information can be readily transmitted between these computers.

17. XML is the acronym for Extensible Markup Language, a system for inserting "tags" in digital documents to dictate how the documents are to be formatted. A stripped-down version of SGML (Standard Generalized Markup Language), XML was designed specifically for Web documents by the W3C (World Wide Web Consortium), an international consortium of companies who want to develop open standards for the Internet to prevent its splintering.

18. With the "Electronic Notary Seal" (ENS) system developed by the National Notary Association, for example, the state that commissioned the notary has effective electronic control over the authentication of each electronic seal, which cannot be validated online as current and in good standing if it has expired or if it has been suspended pending an investigation into the notary's conduct.

19. In the computer world, a protocol is a standard or convention allowing communication or data transfer between two points.

20. SSL abbreviates Secure Sockets Layer, a protocol developed by Netscape for transmitting private documents over the Internet.

21. SSH stands for Secure Shell, a protocol allowing secure encrypted communication over an insecure computer network.

22. HTTPS is the secure version of HTTP — Hyper Text Transfer Protocol — the primary method for conveying data on the Internet.

23. A "hash" is used to verify that a transmitted message has not been tampered with. Also called a message digest, the hash is produced when a mathematical formula (an algorithm) reduces a lengthy message text into a much shorter unique numeric value. The sender then encrypts the hash and the original message and sends both; the recipient decrypts the message and hash, produces another hash from the received message, and compares the two hashes to see if tampering has occurred.

24. For a fuller explanation, see "Electronic Document Certification: A Primer on the Technology Behind Digital Signatures," David L. Gripman, *The John Marshall Journal of Computer & Information Law*, Vol. XVII, Spring 1999, No. 3, pp. 769–796: "Public key encryption systems use two different keys, one private and one public, to encrypt and decrypt messages. The private and public key are mathematically linked to each other so that if one key is used for encrypting, then the other key is used for decrypting. Unlike private key encryption, the sender and receiver do not need to share a secret key. Instead, Mary (the receiver) generates a public key and a private key pair. The public key is available in a publicly available database called a repository. The private key stays in Mary's possession and is only known to her. Then, John downloads Mary's public key and uses it to encrypt a message that he subsequently sends to Mary. The message cannot be read without the corresponding private key. However, using her private key, Mary can decrypt the message that John sent her." Gripman points out that, while messages encrypted with the receiver's public key can be decrypted only with the corresponding private key, it is not computationally feasible to determine the private key code from the public key and vice versa. See also "Electronic Commerce Legislation: From Written on Paper and Signed in Ink to Electronic Records and Online Authentication," Daniel J. Greenwood and Ray A. Campbell, 53 *The Business Lawyer*, 1997, American Bar Association, pp. 307-338. However, see also note 27 below regarding a significant failing of the PKI system.

25. The "Electronic Notary Journal of Official Acts" (Enjoa®) system developed by the National Notary Association in collaboration with Interlink Electronics, Inc. requires the notary record-keeper to submit a biometric scan — a fingerprint — before being allowed to access and enter notations in the journal.

26. See Co. Rev. Stat. §§ 12-55-106.5 and 12-55-112; and the state's "Rules Concerning Electronic Notarization," 8 CCR 1505-11.

27. An often heard term, "non-repudiation" was supposed to have meant that a written agreement, particularly one executed over the Internet, cannot later be disavowed by one of the signing prinipals. Years of experience with the concept and the systems that are supposed to implement the concept, such as Public Key Infrastructures, have demonstrated that parties remain at liberty to disavow transactions despite even the highest

levels of computer and network security. For example, parties may have a legal ground, such as unenforceablility of the transaction due to a consumer protection rule, or there may be confusion regarding the technology used to conduct the transaction. A classic example is the so-called "non-repudiation" bit within a Public Key Certificate, according to the X.509v3 protocol. There was no consensus on the meaning of this bit, and whether it was set to "on" or "off" apparently served primarily to confuse parties who bothered to parse this element of the certificate. The vast majority of parties, however, were completely unaware of this and many other aspects of Public Key Infrastructures, and were therefore unaffected by the underlying impossiblility of this concept. The confusion and other difficulties surrounding Public Key Infrastructures have since led to the repeal of state statutes that had referenced such technology, including in the state of Florida, and it has been reported that the state of Utah will also repeal its Public Key Infrastructure oriented Digital Signature Law. States now enjoy consensus around the simple, common law, uniform, commercially oriented UETA statute.

28. While the state of Arizona has a well-developed statutory system for eNotarization, it has drawn considerable criticism and scant use for authorizing so-called electronic "notarizations" that are based on a signer's mere use of a digital certificate rather than on the signer's appearance before and screening by a commissioned notary public. See Ariz. Rev. Stat. § 41-356.

29. For a discussion of how "our jarringly different state notary laws are increasingly an impediment to commerce and law," see "Unifying Our Nation," *The National Notary*, July 2005, pp. 16–21.

30. The Model Notary Act of 2002 is a significant updating and expansion of two earlier model statutes created and promulgated by the National Notary Association: the Model Notary Act of 1984 and the original Uniform Notary Act of 1973, which was drafted in a special collaboration with Yale Law School. Over the course of three decades, legislators and notary-regulating officials have borrowed extensively from the 1973 and 1984 models in reforming state and territorial notary laws. Like its two predecessors, the Model Notary Act of 2002 was produced by a national panel of state officials, law professors, county recorders, surety executives and, in the case of the 2002 Act, computer software experts.

31. To ensure that notaries are properly trained on their official duties before undertaking them, the Model Notary Act of 2002 (§ 4-3) requires every commission applicant to take a course of instruction of at least three hours and to pass a written examination. To provide a comprehensive set of ethical guidelines for American notaries, the National Notary Association has published and promulgated *The Notary Public Code of Professional Responsibility*. Pertinent to the discussion, Standard III-A-1 of the Code stipulates: "The notary shall insist that the signer and any witness identifying the signer be present before the notary at the time of the notarization."

32. Increasingly, state statutes provide a list of documents that notaries may rely on to identify signers. For example, the Florida Statutes (§ 117.05[5]) permit "reasonable reliance" on any of the following documents, if it is current or has been issued within the past five years and bears a serial or other identifying number: a driver's license or non-driver's identification card from Florida or other U.S. state or territory, Canada or Mexico; a U.S. or properly stamped foreign passport; a U.S. military identification card; an inmate identification card; a U.S. federal immigration card.

33. According to the National Notary Association, some tip-offs to a fraudulently altered identification card are inconsistent typefaces within a single card, "bumps" on the card surface, and the bearer's unfamiliarity with information on the card (e.g., birth date, residence address). A tip-off to identification cards that may have been obtained using a false identity are the fact that all cards presented are brand new and issued at about the same time.

34. According to the National Notary Association, such suspicious behavior may be inordinate laboring to create a signature on the document and in the notary's journal that matches a signature on a stolen identification card.

35. However, as a ministerial official, a notary has no authority to investigate and determine the propriety or legal efficacy of a transaction requiring a notarial act.

36. See Note 10 above.

37. According to the National Notary Association, the notary's most effective observational technique in gauging a signer's basic awareness is to draw the individual into a simple conversation. A person who can respond coherently and appropriately to such mundane questions as, "How are you today?" or, "What would you like me to notarize?" should be considered sufficiently competent for the notary to proceed with the notarization.

38. Such incidents of notary proactivity are regularly reported in National Notary Association membership publications, especially when they result in arrest of criminal exploiters: "I had an instance where an elderly man's estate was threatened when a couple tried to steal ownership from him. After he started to cry at the mention of his (dead) wife's name, I became suspicious. I did not complete the act and notified the authorities." See *The National Notary*, Jan. 2005, p. 25.

39. See Notes 6 and 11 above.

40. Significant parts of the paper-based provisions of the Model Notary Act of 2002 — Articles I and II — were already legislatively enacted into law in New Mexico in 2003 through House Bill 612. In that same year, similar provisions of the Act were also adopted as a code of conduct for Massachusetts notaries through Governor Mitt Romney's Executive Order 455 (03-13). Notably, North Carolina's Senate Bill 671 was signed into law on September 13, 2005; this landmark legislation, effective December 1, 2005, enacts significant parts of *both* the paper-based and electronic provisions of the Act — Articles I, II and III.

41. The Uniform Real Property Electronic Recording Act was adopted by the National Conference of Commissioners on Uniform State Laws at its meeting of July 30–August 6, 2004, in Portland, Oregon.

42. The widely enacted Uniform Electronic Transactions Act (§ 11) states: "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." The federal E-Sign statute contains similar language, but makes reference to "a signature or record relating to a transaction in or affecting interstate or foreign commerce."

43. The Model Notary Act of 2002 (§15-2) requires current paper-based notaries who want to notarize electronically merely to register their capability and qualifications to do so, including proof of passage

of a course of instruction on eNotarization, with the state or territorial notary-regulating authority; a separate commission is not required.

44. A January 2005 white paper by the law firm of Arnold & Porter, LLP, headquartered in Washington, D.C., is instructive on this point: "The Uniform Electronic Transactions Act ("UETA") and federal Electronic Signatures in Global and National Commerce Act ("E-Sign") recognize electronic contracts and signatures as valid writings. However, the potential of electronic commerce for sensitive transactions is still limited by legacy state laws and regulations concerning the form and manner of notarial acknowledgment, and limiting recordable documents to ones that are in writing or on paper or are originals. UETA and E-Sign address only the medium of contracting and not impediments imposed by these legacy laws…. To enable sensitive electronic transactions, states should adopt Article III of the Model Notary Act as well as URPERA."

45. For example: "The certificate shall be signed by the notary public in the notary public's own handwriting." (Cal. Gov. Code § 8205[2])

46. In UETA, these agents are specified in §§ 17-19; in URPERA, in § 5.

47. Contrary to widespread supposition, *electronic* notarization does not mean *remote* notarization, with one signer in location A, another signer in location B, and the notary in location C. However, the model of one signer and notary before a computer in location A, and another signer and notary at location B looking at the same electronic document on another computer, could save business considerable travel and courier service costs and fully comply with eNotarization principles of the Model Notary Act of 2002: "(T)he fundamental principles and processes of traditional notarization must remain the same regardless of the technology used to create a signature. No principle is more critical to notarization than that the signer must appear in person before a duly commissioned notary public to affix or acknowledge the signature and be screened for identity, volition, and basic awareness by the notary. While technology may be perfectible, the basic nature of the human beings who use it, unfortunately, is not. Any process — paper-based or electronic — that is called notarization of a signature must involve the personal physical appearance of a principal before a commissioned notary." (Art. III, "Comment")

About the Author — Daniel J. Greenwood, Esq.

Daniel Greenwood, Esq. has been a lecturer on eGovernment and eCommerce policy and information architecture since 1997 at the Massachusetts Institute of Technology (MIT) School of Architecture and Planning, most recently teaching in the MIT Media Lab. Since 1999, he has also served as the Director of the MIT eCommerce Architecture Program (http://ecitizen.mit.edu/).

For nearly six years, Mr. Greenwood served as Deputy General Counsel for three Chief Information Officers of the Commonwealth of Massachusetts, concluding his government tenure as Acting General Counsel. Mr. Greenwood has testified several times before the U.S. House and Senate on matters of electronic commerce, electronic signatures and public policy in a federalist system.

Currently, in conjunction with his academic practice, Mr. Greenwood consults to government and private companies on authentication and electronic transaction systems, policy and law in association with the CIVICS.com consultancy, which included his appointment as a Special Deputy Attorney General for Electronic Authentication in the State of Idaho and various other engagements with Fortune 500 companies and public sector entities.

Mr. Greenwood also serves on the Boards of Directors of various eBusiness and eGovernment related trade and technical associations, chairs the eContracts Technical Committee of OASIS/LegalXML, and chairs various committees and task forces dealing with information security, business automation and public policy for Bar Associations at the state and national levels. He serves as an e-arbitrator under the Internet Corporation for Assigned Names and Numbers, where he arbitrates Internet domain name disputes. Mr. Greenwood has also developed legal processes for online mediation used by eBay and others.

Mr. Greenwood is a frequently quoted expert, appearing on national television, in the *Wall Street Journal,* and other media on policy, technology, and strategy related to eGovernment and eBusiness.

About MIT and the MIT E-Commerce Architecture Program

Massachusetts Institute of Technology (MIT) — a coeducational, privately endowed research university — is dedicated to advancing knowledge and educating students in science, technology and other areas of scholarship that will best serve the nation and the world in the 21st century.

MIT is committed to generating, disseminating, and preserving knowledge, and to working with others to bring this knowledge to bear on the world's great challenges. Pursuant to this mission, the Institute is devoted to providing its students with an education that combines rigorous academic study and the excitement of discovery with the support and intellectual stimulation of a diverse campus community.

The Institute has more than 900 faculty members and nearly 10,000 undergraduate and graduate students, and is organized into five Schools — Architecture and Planning, Engineering, Management, Science, and Humanities, Arts and Social Sciences — and the Whitaker College of Health Sciences and Technology. Its five schools and one college encompass 34 academic departments, divisions and degree-granting programs, as well as numerous interdisciplinary centers, laboratories and programs whose work cuts across traditional departmental boundaries.

The School's activities range widely across architecture, urban studies and planning, real estate, media arts and sciences, and the visual arts. The School values design excellence, technological inventiveness and imaginative scholarship, and believes that design and policy interventions should be grounded in unwavering commitment to equity, social justice and making a positive difference in the everyday lives of real people.

The MIT E-Commerce Architecture Program (eCAP), at ecitizen.mit.edu, is an initiative to explore the legal, business, policy and technical inputs to information architectures of eGovernment and eBusiness.

About the National Notary Association

The National Notary Association (NNA), a non-profit professional organization, has served the nation's over four and a half million notaries since 1957 with a wide variety of services and advocacy initiatives to strengthen and professionalize the notary public office.

Public trust in the security and integrity of the transactions of commerce and law rests in large part in the hands of America's notaries. By working with educational institutions such as the Massachusetts Institute of Technology, Yale Law School, John Marshall Law School and Northern Illinois University, with governmental organizations such as the Federal Bureau of Investigation and the U.S. Department of Justice, with industry organizations such as the Mortgage Bankers Association and the American Bar Association, and with standards-setting bodies such as the Mortgage Industry Standards Maintenance Organization, the NNA has been at the forefront of the effort to set high professional standards for the notary public office for almost half a century.

As the country's clearinghouse for, and preeminent publisher of, information on notarial laws, customs and practices, the NNA educates notaries through publications, seminars, its annual conference and a unique Notary Information Service. In addition, the NNA is a valuable resource for lawmakers, law enforcement, industry leaders, members of the media and the public on the important fraud-fighting role of the notary public, both in the paper-based world and the emerging electronic realm. The NNA also devotes resources to helping legislators draft effective notarial statutes.

Indeed, the NNA's Model Notary Act serves as comprehensive prototype legislation. First drafted in 1973 in collaboration with Yale Law School and updated in 1984 and 2002 by a panel of secretaries of state, legislators, attorneys and notaries, the Act is regularly used by state legislatures in revising their notarial laws. The 2002 Act is a complete model statute covering every phase of commissioning and regulating notaries who perform both paper-based and electronic notarizations. In developing *The Notary Public Code of Professional Responsibility*, the Association has provided an ethical guide of best practices for notaries to consult when statutes, regulations and official directives fall short of providing full guidance for appropriate conduct.

National Notary Association
Chatsworth, California
www.NationalNotary.org

Published as a public service by the National Notary Association, a non-profit professional organization. January, 2006.
The author hereby acknowledges and thanks the editors of the National Notary Association for their invaluable assistance with the preparation of this paper and provision of End Notes content.