From: John Messing [jmessing@law-on-line.com]
Sent: Sunday, May 21, 2006 2:01 PM
To: EMarshall@sosnc.com
Cc: hmontgomery@sosnc.com; treiniger@nationalnotary.org;
Thomas.E.Wrosch@state.or.us
Subject: Comments of John Messing, Chair, eTrust Subcommittee, ABA to
proposed enotarization standards

Dear Chair of the National eNotarization Commission:

Congratulations on a first effort that notary administrators may find useful as an enotarization reference. I regret that I will not be able to be present for your Commission's deliberations in Washington, DC later this month. Your work is important and appreciated.

I chair the ABA Science and Technology Law Section's eTrust subcommittee, which produced a White Paper on eNotarization. I also am the Chair of LegalXML-OASIS, which is an XML standards body that develops technical standards for legal purposes, including eNotarization. The following comments are my own.

eTrust was a joint effort of representatives from several different professions, including mortgage banking, real estate, notary membership organizations, notary administrators, and lawyers, some of whom were technically proficient.

Opposing factions within the workgroup with conflicting agendas reached unanimous agreement that tamper-evident protections are necessary to prevent fraud.

Disagreement persisted on the appropriate means to introduce or implement such protections. One group, which was a minority, argued that political bodies such as notary administrators or legislatures should set technology standards for tamper-evident enotarizations. Another group, which constituted a majority of the workgroup membership, insisted that market forces should be allowed to determine naturally the most appropriate combination of technologies. The views appear to reflect differing visions of conventional notarization, consumer protection, and how best to prevent fraud when technology is involved, especially in light of existing legislation such as the federal Esign law which specifically limits state and federal power to promote one electronic signature technology over another.

Debates about enotarization are taking place against a backdrop of legislation and court rules at the federal and state levels that increasingly deprecate the role of notarized documents in favor of simple declarations under penalty of perjury which are not witnessed by commissioned notaries. Paradoxically at the same time, there a rising crime wave of identity theft both at home and abroad that in my view makes effective electronic notarization urgent.

Once notarization passes from purely paper-based to electronic media, there are a number of candidate technologies that could be employed to make the job of fraud prevention easier and better. Although the eTrust subcommittee did not expressly consider it, video is prevalent, inexpensive, and easy to use, and can be found even in many modern cellphones. Commissioned notaries could leverage such ubiquitous technologies for improved real-time records of signature events. With electronic notarization, one is no longer just tied to textual words within documents to authenticate signers and attest to signatures.

I encourage your commission to explore ways to balance the goals of promoting technology diversity in this incubatory period, while at the same time protecting consumers. I also recommend vigilance against returning to pre-eSign laws and rules that would require digital signatures within a Public Key Infrastructure as the only authorized technology for enotarization, contrary to modern State and federal laws. In this regard I draw your attention to proposed standard no. 9, which as posted states as follows:

"9. The notary public's official electronic seal is deemed to be reliable if the following requirements are met: a) it is unique to the notary public, b) it is capable of independent verification, c) it is retained under the notary public's sole control, d) it is attached to or logically associated with the electronic document and d) it is linked to the data in such a manner that any subsequent alterations to the underlying document or electronic notarial certificate are detectable and may invalidate the electronic notarial act."

I request you to examine and seek legal opinion whether this language so closely follows language of digital signatures laws that have been federally pre-empted or withdrawn from the books that it could be deemed to require a Public Key Infrastructure ("PKI") and thus violate UETA and eSign by impermissibly prescribing a single technology for enotarization. (PKI is the technology being used in the Pennsylvania pilot of the NNA, to my understanding.)

Some logistical comments about mistakes in the NNA web page that is maintained for the commission have been sent to Mssrs. Reiniger and Hansberger of the NNA for correction.

Please do not hesitate to contact me if I may be of further assistance to the Commission.

Thank you for the opportunity to comment, and best regards.

John Messing
5151 E. Broadway Blvd., Suite 1600
Tucson, AZ 85711
(520) 512-5432 (o)
(520) 512-5401 (f)
(520) 270-1953 (c)

blog: formofthequestion.blogspot.com

----Original Message-----
From: John Messing [mailto:jmessing@law-on-line.com]
Sent: Thursday, June 01, 2006 8:14 AM
To: EMarshall@sosnc.com
Cc: hmontgomery@sosnc.com
Subject: Supplementary Comments of John Messing on enotarization standards

Dear Chair and Commission Members:

Following submission of my personal comments on the proposed standards as of May 21, 2006, it was reported to me that at the May 27, 2006 public session of the Enotarization Commission, reference was made to my email submission (attached) with the observation that I was a provider of a technology for enotarization.

In the interests of full disclosure and complete transparency to and by everyone, please be advised of the following.

Law-on-Line, (http://www.lawonline.biz), is a company I helped to found. It developed a prototype of an enotarization program for immediate use today which also is adaptable to atomic or quantum computing. That makes it unique. I intend for it to benefit the entire legal community, including its need for notarized documents.

To understand the importance of atomic computing, please visit, for example, http://en.wikipedia.org/wiki/Quantum_computer, http://www.qubit.org/library/intros/comp/comp.html, and http://www.techreview.com/read_article.aspx?id=16505&ch=infotech.

Atomic (quantum) computing is currently beyond the pure laboratory testing stage and is in limited operational use. Though in its infancy, it threatens to undo the security of conventional digital signatures and digital certificates through the ability of the atomic computer to break the encryption codes and instantly create flawless and indetectable forgeries, even as to digital signatures that may have been created before the atomic computers were invented. The Law-on-Line technology is immune to this impending virtual world-rocking event.

The Law-on-Line prototype that was developed also postulates a repository of cryptographic artifacts which can be accessed to verify electronic signatures; a secure method of authenticating authorized notaries using web services and service oriented architecture, and optionally supports the use of biometric extensions in digital certificates for enhanced security where necessary as determined by the needs of relying parties.

The prototype was developed pursuant to marketing arrangements between Law-on-Line and the National Notary Association.

By way of correction, please note that my remarks are intended to refer equally to Section 7 as well as Section 9 of the proposed standards.

Thank you for your service to the community of those of us who are notaries, service notaries, or advise them legally.

May 25, 2006

BY ELECTRONIC MAIL

The Honorable Elaine F. Marshall
Secretary of State of North Carolina
The National Association of Secretaries of State
{Address}

RE: National Association of Secretaries of State ("NASS") Recommended Uniform Legal Standards for Enabling E-Notarization in a Secure and Accountable Manner

Dear Honorable Marshall:

Wachovia Corporation ("Wachovia") appreciates the opportunity to comment in response to the NASS Notice of Recommended Uniform Legal Standards for Enabling E-Notarization in a Secure and Accountable Manner.

Wachovia is a national bank engaged in the business of offering a wide variety of financial services to its customers. These financial services include but are not limited to securities, commercial, consumer, trust and deposit products, primarily offered on the East Coast, but recently expanded to customers on the West Coast. Many of the financial transactions completed across the organization involve documents that must be notarized. The issue of uniform notary standards, including notary standards for electronic transactions will have a significant impact on Wachovia's business. We appreciate the efforts of the NASS to reach a consensus as to standards that will assure the safety and security of the electronic notarization process.

Physical Appearance Requirement. Wachovia agrees with the uniform standard that requires the physical appearance of a person before a notary. However, we are aware the technology may be developing so quickly that video-conference transactions may be a potential option. This would enable a virtual closing in which the notary could still assess the signors identity , willingness to sign and awareness/ capacity of the signor. . The requirement for a "physical appearance" would ideally allow for some flexibility based on developing technology to satisfy these needs. Wachovia supports the continued use of identification verification standards that exists in the paper-based environment again, within the context of developing technology. For example, we envision a time when biometrics may be a more reliable method of identification verification than a driver's license.

Registration Requirement. Wachovia agrees with the need for registration of a Notary to perform duties electronically with a commissioning official within the applicable jurisdiction. Since Wachovia relies on the validity of notarizations contained on documents it receives in each state, we are deeply concerned about the need for state commissioning officials to monitor the registration and training of individuals who perform all types of notarizations. Our experience indicates a wide variety of requirements for training in general across the states. The complexity of electronic functionality is so new to the general public and to notaries that we believe it is necessary to require a training component to the uniform standards. It is important to the enforcement of documents that electronic notarizations be honored across state lines. Wachovia believes that an additional component of monitoring and training will increase the trust in the electronic certification structure with respect to business conducted on a national level.

Form and Manner of Performing the Electronic Notarial Act.
Section 9 which addresses what will be deemed to be a reliable notary seal must be tied to a national electronic security standard. While Wachovia believes this standard should include a requirement for document level security that indicates the document has not been altered since it was first rendered in its final form, Wachovia believes that the specifics of such security are better left to the market forces driven by the companies and individuals who utilize these documents rather than governmental action. Additionally, Wachovia has concerns which it believes would be best solved by the parties that have a vested interest in the transaction as to whether such security should be on a document-by-document basis or part of an overall system or process just as it is in the paper world today.

Wachovia appreciates the opportunity to review and comment on the proposed standards. We look forward to further discussion of these issues. Please contact me if you have any questions about our comments.

Sincerely,

Sybille Nelson
Senior Vice- President
eCredit Program Manager
540/ 563-6047

From: McGinnis, Joe [mailto:JJMcGinnis@ugtic.com]
Sent: Friday, June 02, 2006 11:44 AM
To: nationalcommission@nationalnotary.org
Subject: - e-notary commission comments- ELECTRONIC LOGBOOK FOR THE NOTARY-
PREVENTION OF FRAUD

THE "NATIONAL" E-NOTARY SHOULD BE REQURIED TO MAINTAIN AN ELECTRONIC LOGBOOK AND HAVE AN ELECTRONIC FINGERPRINT RECORDING DEVICE (SIMILAR TO OBTAINING A THUMBPRINT FOR DOCUMENTS IN CALIFORNIA AND AS SUGGESTED IN OTHER STATES) AS AN AUTHENTICATION DEVICE .

The logbook should have printable pages kept chronologically with an electronic copy of the document or at least the face and signature pages kept on file with the Notary.

Concern is to control possible fraud perpetrated through use or improper use of e-notary.

June 8, 2006

Comments by the Pennsylvania Association of Notaries and
the United States Notary Association concerning the
National E-Notarization Commission Proposed Standards

Definitions

1. Authentication—A notary does not "authenticate" an individual's identity, although he or she may "verify" it with appropriate credentials. To authenticate an individual's identity would require validating the credentials. In fact, the Commission itself uses "verify" instead of "authenticate" elsewhere in the Standards.
We recommend replacing "authenticate" with "verify" with regards to the notary identifying an individual.

2. No comment.
3. No comment.
4. Electronic notarial act—The Associations' premise is that a notary is a notary, whether they are using a wet signature on paper or an electronic sound, symbol or process with an electronic document. To make a distinction between these two methods implies that there are separate notarial acts depending on the method.
We recommend that this definition be eliminated.

5. Electronic notary public and electronic notary—In a recent survey conducted by the Notary Public Administrators section of the National Association of Secretaries of State, the vast majority of respondents stated that a new, separate term was not needed for notaries who notarized electronically. As discussed in Definition 4 regarding notarial acts performed electronically versus other methods, the Associations' premise is that a notary is a notary, no matter what tool is used to perform a notarial act. It is a burdensome process to require a commissioned notary public to go through another commissioning to be able to notarize electronically, when a simple registration of an electronic signature would accommodate the issuance of notarial authentications and apostilles. In addition, making a distinction between "notary public" and "electronic notary public" implies that an individual can be one without the other, but at this time a notary may not be an "electronic" notary without first becoming a "paper" notary.
6. Electronic notary seal and official electronic seal—The term "electronic notary seal" cannot be used since one vendor is already using the term Electronic Notary Seal (ENS™) for its product. There is no reason to believe that this product (a digital signature and certificate) will be the one-and-only-and-forever means to notarize electronically, nor is there reason to believe that the Commission has to limit itself in such a manner in promoting electronic commerce. We believe this would be in direct contradiction to the intent of federal and state electronic transactions acts.

Neither “electronic seal” term in Definition 6 is acceptable to, for example, Pennsylvania’s Notary Public Law, which states that “… a notary public is not required to use an electronic seal [emphasis added] for the notarization, acknowledgment or verification of electronic records and electronic signatures …” provided that notarial information is attached to or logically associated with the record or signature [57 P.S. §158(f)]. There may be other states with laws or regulations that also address the non-requirement of an electronic seal.

We recommend that another term be found.

7. No comment.
8. Electronic notarial certificate—A notary’s certificate used to notarize electronically is the same certificate now used by a paper notary, except that it will be in an electronic format as part of an electronic document. As with “notarial act” and “notary,” we do not see the need to redefine what is already well established.
9. No comment.
10. Physical appearance and appears before the notary—The phrase “give identification documents to each other” in this definition implies that the notary must identify him/herself to the customer, which is not the case at this time. There currently is no national database of “paper” notaries nor any requirement for "paper" notaries to identify themselves to their customers. One of the basic tenets of the laws that give us guidance in the electronic world is that requirements should not be more onerous in the electronic world than in the "paper" world.
Also, it is currently very easy to order a fraudulent notary seal for any state from an rubber stamp company and use it for fraudulent acts. Cable News Network (CNN) recently revealed a scam in Texas whereby an individual opened a brokerage account in the name of an existing company with an application he notarized himself with a fake rubber stamp seal. He used the account to deposit corporate checks stolen by a company employee and then withdrew the funds—$12 million worth. CNN followed up by purchasing a rubber stamp seal in the name of “I.D. Thief” and received it without question. It was suggested in the CNN program that notary customers check with the state to make sure a notary stamp is valid, which is a burden to the public and not readily accomplished in our experience. We are told to identify utility company employees wanting access to our houses by their badges, uniforms and trucks, and still imposters figure out new ways to gain access for criminal acts. There is no guarantee that any electronic means of verifying (or authenticating) a notary’s credentials could not also be overcome by technologically savvy criminals.

We recommend that the phrase be rewritten.

Physical Appearance Requirement

We question whether either paragraph 1 or 2 is needed. Current notary law addresses the personal appearance requirement and identifying signers for a notary, without distinction to a “paper” notary or an “electronic” notary. In addition, Definition 10 adequately defines personal appearance.

1. If paragraph 1 remains, we recommend that it be reworded so that appearing “before” a notary means “in the personal presence of” a notary, as opposed to “before” a notary on a TV or computer screen. It would help remove any perceived loopholes in this requirement.

Registration Requirement

We strongly disagree with the registration requirement. It is based on a business model for vendors and should not be forced upon the notary population of this country. We recommend that notaries in good standing with their state commissioning officials should be permitted to use their choice of electronic sound, symbol or process, along with their ink pens, to continue performing their functions as notaries public.

In addition, the requirement does not stipulate that any issues addressed by the Commission or authorized by the states must be technology-neutral.

Form and Manner of Performing the Electronic Notarial Act

5. We recommend that this paragraph end with the words “… with the electronic document[.]” and that the words “… such that removal or alteration of such electronic signature is detectable and will render evidence of alteration of the document containing the notary certificate which may invalidate the electronic notarial act” be removed. If the notary signature (or seal) is removed after the act has taken place, it does not mean that the act never occurred. If the document is changed after the notarial act, it does not mean that the act itself never occurred or is invalidated. If the signature alteration is what is detectable, that does not mean document alteration is detectable. One has no way of knowing what changes were made. Changes to a document do not necessarily invalidate the notarial act. Automatically overturning the act, much less the entire document, is a serious liability issue in electronic commerce and is best left to the parties and the courts. Another issue is with use of the word “evidence” as both a verb and a noun in the

same sentence. We recommend rewording to avoid confusion.

6. As stated in paragraph 5, please consider that automatically overturning the notarial act, much less the entire document, is a serious liability issue in electronic commerce and is best left to the parties and the courts.

This section also speaks to the notary as providing document integrity, which is not required under current notary law.

7. This paragraph appears to be a sub-set of paragraph 5 and should be included with it to avoid confusion.
Also please note that the term “verification” is not defined under Definitions in the Standards. Stating that the electronic signature must be “capable of independent verification” begs the question, verified by whom?

As stated in paragraphs 5 and 6, please consider that automatically overturning the notarial act, much less the entire document, is a serious liability issue in electronic commerce and is best left to the parties and the courts.

This section also speaks to the notary as providing document integrity, which is not required under current notary law.

We also recommend establishing one set of security requirements for both the signature and the seal, not each separately.

8. As stated in paragraphs 5, 6 and 7, please consider that automatically overturning the notarial act, much less the entire document, is a serious liability issue in electronic commerce and is best left to the parties and the courts.
This section also speaks to the notary as providing document integrity, which is not required under current notary law.

We also have continued concerns about the expression “electronic seal” as stated in Definition 6.

9. This paragraph appears to be a sub-set of paragraph 8 and should be included with it to avoid confusion.
As stated in paragraphs 5, 6, 7 and 8, please consider that automatically overturning the notarial act, much less the entire document, is a serious liability issue in electronic commerce and is best left to the parties and the courts.

This section also speaks to the notary as providing document integrity, which is not required under current notary law.

We also have continued concerns about the expression “electronic seal” as mentioned in Definition 6 and with the term “verification” which is not defined under Definitions in the Standards. Also, as stated in paragraph 7, we question who would be qualified to verify the “seal.”

Please note a typo in this paragraph with two d) items instead of a d) and an e).

We encourage the Commission to consider all currently known technology to ensure neutrality as mandated by law. We encourage the Commission to consult with experts about what the future may bring for electronic signatures to ensure that the Commission’s work has a long, useful and relevant life.

10. Please clarify if a notary may use an electronic signature (without the “seal”) as a private individual for non-notarial acts.
11. What recourse does a notary have for some technological mistake that may be beyond his or her control? Not applying a signature to a paper document is one thing, applying an electronic signature that arrives at the document’s destination a garbled mess is another.
Comment below 11. We request clarification on the statutory requirements for “federal and state rules of evidence.” We recommend that the Commission consult with legal experts on this point. If operable law calls for notarizations to be performed according to state law, and if no seal is required by said state, it is hard to believe that there is a loss of evidentiary value if information that would normally be on a seal is not included on the electronic notarization of an electronic document.

Also, using “evidence” as a noun here and a verb in the header before paragraph 13, as well as in paragraph 13, could confuse many individuals.

We appreciate the Commission’s mention of technology neutrality in the last paragraph. We are concerned about whether or not the Commission consulted with the legal and technology experts to consider whether all signature profiles would qualify. It has been brought to our attention that some may not. In fact, there appears to be just one technology that qualifies based on the language in these standards.

Security Requirements

12. We ask for clarification on what information may not be shared. We do not wish to assume that the Commission means name or address or other general information used during the registration process in Pennsylvania. We also recommend that a “reasonable precaution” be defined.
We strongly disagree with the registration requirement. It is based on a business model for vendors and should not be forced upon the notary population of this country. We recommend that notaries in good standing with their state commissioning officials should be permitted to use their choice of electronic sound, symbol or process, along with their ink pens, to continue performing their functions as notaries public.

In addition, the requirement does not stipulate that any technology issues addressed by the Commission or the states must be vendor-neutral.

Comments after 12. Perhaps it would be more useful to note those security aspects that can be shared, as opposed to using a “such as but not limited to” generalization.
As written, this comment provides neither guidance nor protection for the notary.

Requirements for Evidencing the Notarial Act

13. We have a concern about the word “non-repudiation,” which is not included in Definitions. “Non-repudiation” in the technology world is a reference to proving the

relationship between a public and private key. It does not mean that an individual could not repudiate an electronic signature, even a secure one. It also refers to one type of technology, digital signatures. Elsewhere in the Commission's work, there has been mention of technology neutrality. There are, and will be, many methods of complying with the concept of a sound, symbol or process in the electronic environment other than digital signatures, and we recommend that the Commission use technology-neutral language in this paragraph.

Our next concern is with the phrases "improperly modified" and "unauthorized alteration." We question what technology or individual will determine the difference between proper and improper modifications or authorized and unauthorized alterations. We also question if the document will contain an indication of either a modification or alteration, such as indicated in paragraphs 5, 6, 7 and 8 regarding the notary's signature and seal.

And last, we are concerned that validating the integrity of the document has been confused with the commissioning official's ability to authenticate a notary. The idea that a document or a notarial act can be invalidated because of a problem with the technology is new and unfounded.

Requirements for Issuance of Electronic Apostille and Certificate of Authentication (Appointment)

14. Please see our concerns about the phrase "non-repudiation" as stated in paragraph 13.
Also, we request clarification of the phrase "… a person attempts to remove the Apostille from the public document." First of all, we question why only "public" documents are mentioned. Second, through the Notary Public Administrators section of the National Association of Secretaries of State, we have often heard speakers from the United States Department of State and state notary public administrators relate stories of fraudulent apostilles being attached to documents, not removing valid apostilles from them. Perhaps both occurrences are common.

15: Please see our concerns about modification and non-repudiation as stated in paragraph 13.
Comments after 15. We recommend rewording of the sentence, "Therefore, any separation legally invalidates the Apostille." We understand the intent of this language, but we can see in the paper age that the apostille and document could be separated, for example, to facilitate the scanning or other processing of the documents. "Legally joined" has a different connotation than "any separation legally invalidates" indicates.

NATIONAL E-NOTARIZATION COMMISSON
PROPOSED STANDARDS
Secretary of State Elaine Marshall, Chair
May 16, 2006

Definitions

1. "Authentication" means the process of identifying an individual, either in connection with the creation of a relationship or in connection with the individual's participation in a transaction.

2. "Electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

3. "Electronic document" means information that is created, generated, sent, communicated, received, or stored by electronic means.

4. "Electronic notarial act" means an official act by a notary public on or involving an electronic document and using means authorized by the [commissioning official] or the laws of the jurisdiction of appointment.

5. "Electronically enabled notary public" means a notary public who has registered with the [commissioning official] the capability of performing electronic notarial acts in conformance with this Article

6. "Electronic notary seal" and "official electronic seal" mean information within a notarized electronic document that includes the notary public's name, jurisdiction of appointment, commission number, and commission expiration date, and generally corresponds to data in notary public seals used on paper documents.

7. "Electronic signature" means an electronic sound, symbol, or process attached to or logically associated with an electronic document and executed or adopted by a person with the intent to sign the electronic document or record.

8. "Electronic notarial certificate" means the portion of a notarized electronic document that is completed by the notary public, bears the notary public's electronic signature and/or official electronic seal, official title, commission number, commission expiration date, any required information concerning the date and place of the electronic notarization, and states the facts attested to or certified by the notary public in a particular electronic notarization.

9. "Notary electronic signature" means those forms of electronic signature which have been approved by the commissioning official as an acceptable means for an electronic notary to affix the notary's official signature to an electronic record that is being notarized.

10. "Physical appearance" and "appears before the notary" mean that the principal and the notary public are physically close enough to see, hear, communicate with, and give identification documents to each other.

Comment

The term "authentication" is used in the broad context of verifying identity and should not be confused with other specific types of authentication, such as document authentication performed by a notary public to help ensure that documents can be trusted in government or commercial dealings, certificates of authentication issued by commissioning officials to prove a notarial act, or the authentication procedure used in litigation for the purposes of admitting certain records into evidence.

Although the definitions for "Electronic notary seal" and "Electronic notarial certificate" have references to "Commission number", "Commission expiration" and "Notary seal", it is recognized that some jurisdictions do not issue commission numbers, or require notary seals. Other jurisdictions that issue life long notary commissions do not have expiration dates.

Physical Appearance Requirement

1. A notary public shall not perform an electronic notarization if the document signer does not appear in person before the notary public at the time of notarization.

2. The methods for identifying document signers for an electronic notarization shall be the same as the methods required for a paper-based notarization.

Comment

Under no circumstance shall a notary public base identification merely upon familiarity with a signer's electronic signature or an electronic verification process that authenticates the signer's electronic signature when the signer is not in the physical presence of the notary public.

Registration Requirement

3. Before performing any electronic notarial acts, a notary public shall register the capability to notarize electronically with the [commissioning official].

4. In registering the capability to perform electronic notarial acts, the notary public shall provide the following information to the [commissioning official]: a) the electronic technology or technologies to be used in attaching an electronic notarial certificate to an electronic document, b) the electronic technology or technologies to be used in attaching the notary's electronic signature to the electronic document, c) the electronic technology or technologies to be used in attaching the notary's official electronic seal to the electronic document, and d) any necessary instructions or techniques that allow the notary's electronic signature and/or official electronic seal to be read.

Comment

The technologies that a state may authorize for an electronic notarization will dictate how the attachment or logical association of the electronic notarial certificate, electronic signature, and official electronic seal to the document will be accomplished. Depending on the technology selected, it is possible that the electronic signature and seal may be combined in a single element, or that the seal may be a component of the signature or vice versa. The

important matter is that all of the notary public's identifying and commissioning information be made a part of, or a secure attachment to, the underlying notarized electronic document.

Form and Manner of Performing the Electronic Notarial Act

5. When performing an electronic notarization, a notary public shall evidence the notarial act with an electronic signature, which shall be attached to or logically associated with the electronic document such that removal or alteration of such electronic signature is detectable and will render evidence of alteration of the document containing the notary certificate which may invalidate the electronic notarial act.

6. When performing an electronic notarization, a notary public shall complete an electronic notarial certificate, which shall be attached to or logically associated with the electronic document such that removal or alteration of the electronic notarial certificate is detectable and will render evidence of alteration of the document containing the notary certificate which may invalidate the electronic notarial act.

7. The notary public's electronic signature is deemed to be reliable if the following requirements are met: a) it is unique to the notary public, b) it is capable of independent verification, c) it is retained under the notary public's sole control, d) it is attached to or logically associated with the electronic document, and e) it is linked to the data in such a manner that any subsequent alterations to the underlying document or electronic notarial certificate are detectable and may invalidate the electronic notarial act.

8. When performing an electronic notarization, a notary public shall evidence the notarial act with an official electronic seal, when required by law, which shall be attached to or logically associated with the electronic document such that removal or alteration of such official electronic seal is detectable and will render evidence of alteration of the document containing the notary certificate which may invalidate the electronic notarial act.

9. The notary public's official electronic seal is deemed to be reliable if the following requirements are met: a) it is unique to the notary public, b) it is capable of independent verification, c) it is retained under the notary public's sole control, d) it is attached to or logically associated with the electronic document and d) it is linked to the data in such a manner that any subsequent alterations to the underlying document or electronic notarial certificate are detectable and may invalidate the electronic notarial act.

10. The notary public's electronic signature in combination with the electronic notary seal shall be used only for the purpose of performing electronic notarial acts.

11. The liability, sanctions, and remedies for the improper performance of electronic notarial acts are the same as described and provided by law for the improper performance of non-electronic notarial acts.

Comment

Although UETA, and URPERA, and the federal ESign 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. What is important is that the basic identifying and commissioning information – contained in the notary public's holographic signature and traditional inking and embossing notary seals – also be elements of a notarized electronic document.

These standards do not in any way require the use of one specific technology, nor are they intended to privilege the use of one specific technology over another.

Security Requirements

12. The notary public shall not share the information used in registering with the [commissioning official] except when requested by law enforcement, the courts, and with reasonable precautions, electronic document preparation and transmission vendors.

Comments

Control of security aspects such as but not limited to passwords, token devices, biometrics, PINS, phrases, software on protected hardware shall remain only under the control of the commissioned individual.

Requirements for Evidencing the Notarial Act

13. Electronic notarial acts need to fulfill certain basic requirements to ensure non-repudiation and the capability of being authenticated by the [commissioning official] for purposes of issuing Apostilles and Certificates of Authentication. They are as follows: a) the fact of the notarial act, including the notary's identity, signature, and commission status, must be verifiable by the commissioning official and b) the notarized electronic document must be invalidated if it is improperly modified after the time of notarization, including any unauthorized alterations to the document content, the electronic notarial certificate, the notary public's electronic signature, and/or the notary public's official electronic seal.

Requirements for Issuance of Electronic Apostilles and Certificates of Authentication (Appointment)

14. Electronic Apostilles need to fulfill certain basic requirements to ensure non-repudiation: a) the fact of the issuance of the Apostille by the [commissioning official] must be independently verifiable and b) the Apostille must be invalidated if the underlying document is improperly modified as when, for example, a person attempts to remove the Apostille from the public document.

15. Certificates of Authentication (or Appointment) need to fulfill certain basic requirements to ensure non-repudiation: a) the fact of the issuance of the Certificate by the [commissioning official] must be independently verifiable and b) the Certificate must be invalidated if the underlying document is improperly modified as when, for example, a person attempts to remove the Certificate from the public document.

Comment

The Apostille and the underlying document are legally joined. Therefore, any separation legally invalidates the Apostille. To ensure a recipient the necessary degree of security and trust in deciding whether to accept, an electronic Apostille must, from the time of issuance, provide integrity (assurance that the Apostille and the document have not been altered), authentication (assurance as to where the Apostille and document come from) and non-repudiation (the commissioning official cannot deny having signed the Apostille). In the same way, the Certificate and the underlying document are legally joined, and any separation legally invalidates the Certificate. Therefore, to ensure a recipient the necessary degree of security and trust in deciding whether to accept, an electronic Certificate must, from the time of issuance, provide integrity (assurance that the Certificate and the document have not been altered), authentication (assurance as to where the Certificate and document come from) and non-repudiation (the commissioning official cannot deny having signed the Certificate).

OASIS LegalXML

Advancing Standards for Legal Data Exchange

LegalXML Member Section Steering Committee

Via First Class Mail, e-mail, and Facsimile

The Honorable Elaine Marshall
Chair, National eNotarization Commission
Secretary of State of North Carolina
P.O. Box 29622
Raleigh, NC 27626-0622

RE: National eNotarization Commission Proposed Standards

Dear Secretary Marshall:

This document contains comments regarding the proposed standard of the National eNotarization Commission of the National Association of Secretaries of State (the "eNotarization Commission") for electronic notarization (the "Proposed eNotarization Standard") that was discussed at a public meeting on May 27, 2006 in Washington, D.C. These comments have been endorsed by the OASIS LegalXML Member Section Steering Committee.

By way of background, I chair the OASIS LegalXML eNotarization Technical Committee, which deals with open standards for electronic notarization of electronic documents using technologies such as XML markup languages and electronic signature standards. I also represent the American Bar Association within OASIS, and I am the Vice-Chair of the Electronic Filing Committee in the Science and Technology Section of the American Bar Association. I have participated in the sessions of the ABA eTrust subcommittee, which operates under the ABA Electronic Filing Committee. I am a lawyer by training and a technologist by avocation. I am in private practice in a small firm in Charlotte, North Carolina that focuses on construction law. As for my involvement in legal technology matters, I also am a member of the North Carolina Bar Association's Technical Advisory Committee.

LegalXML is a member section of OASIS, the Organization for the Advancement of Structured Information Standards, and focuses on establishing world wide XML standards useful to the courts and the legal profession. OASIS itself is a non-profit international consortium of over 600 technology companies, governments, and technologists and it is responsible for many of the important open standards for e-commerce and e-government that are in use around the world today. For more information on OASIS, please visit www.oasis-open.org. For information on the OASIS LegalXML Member Section, please visit www.legalxml.org.

The OASIS LegalXML eNotarization Technical Committee has been studying electronic notarization for several years. The eNotarization Technical Committee is working with a set of technology-neutral, open standards to support electronic notarizations and apostilles. The OASIS LegalXML eNotarization Technical Committee is using as a first source a set of standard