Minutes: NASS Business Services Committee Meeting
9:00 AM - 10:30 AM
July 16th, 2016
Nashville, TN

Participants:
Hon. Jeffrey Bullock, DE (Co-Chair)
Hon. Paul Pate, IA (Co-Chair)
Hon. John Merrill, AL
Hon. Mark Martin, AR
Hon. Wayne Williams, CO
Hon. Denise Merrill, CT
Hon. Brian Kemp, GA
Hon. Shan S. Tsutsui, HI
Hon. Lawerence Denney, ID
Hon. Kris Kobach, KS
Hon. Alison Lundergan-Grimes, KY (by proxy)
Hon. Tom Schedler, LA
Hon. John Wobensmith, MD
Hon. Matt Dunlap, ME
Hon. Steve Simon, MN
Hon. Jason Kander, MO (by proxy)
Hon. Bill Gardner, NH
Hon. Barbara Cegavske, NV
Hon. Elaine Marshall, NC
Hon. Al Jaeger, ND
Hon. John Husted, OH
Hon. Pedro Cortés, PA
Hon. Nellie Gorbea, RI
Hon. Mark Hammond, SC
Hon. Tre Hargett, TN
Hon. Carlos Cascos, TX
Hon. Jim Condos, VT
Hon. Natalie Tennant, WV

Secretary Bullock called meeting to order at 9:00AM and introduced Mr. Tim Moss, Chief Executive, Companies House, Government of the United Kingdom. Mr. Moss presented on the new UK registry of persons with significant control and how it was implemented. He noted that Companies House operates the registry of all corporations in the UK. He described how their purpose is not only to serve as the registration authority, but to support the economy and provide people with data in a transparent manner. He said Companies House has approximately 3.7 million companies in its registry and is growing rapidly. He said that Companies House recently decided to make the registry data available free

of charge, which has significantly increased usage of the site. He noted that since 2013 the UK has been working to adopt and implement a requirement that companies disclose the people who have significant control of the company (PSC). He said that as of April 2016, each company has to maintain a PSC registry, and as of June 30 2016 that information must be filed with Companies House. He said this applies to all new companies, and existing companies will have to provide the information as part of an annual filing.

He added that as part of UK efforts to increase the availability and of transparency of data, the PSC information is publicly available. He said that companies are required to take reasonable steps to determine the PSC, and the PSC is required to supply information. He noted that the data will allow people to look through the chain of corporate ownership and find the individual ultimately in control. He said that it can be difficult for people to understand the PSC concept, particularly small businesses with 1 or 2 shareholders who are themselves in control of the corporation. He noted the importance of educating people on the concept. He mentioned that some have expressed concern that a bad actor won't disclose accurate information, but said this can trigger criminal penalties and prosecution. He showed how an individual can search for the PCS information on the Company House website, and said that in the future they will be focusing on making it easier to search for the PSC information, along with compliance, enforcement, and analysis of the PSC data.

Secretary Pate announced that the Committee had two business items to consider. He said the first was consideration of the NASS Endorsement of the NPA Resolution Adopting Apostille Best Practices. He noted that the endorsement was set to expire this year, and NPA has requested that NASS reauthorize it.

Action Item

Secretary Merrill of Alabama moved that NASS reauthorize the Endorsement of the NPA Resolution Adopting Apostille Best Practices. The motion was seconded by Secretary Cegavske and passed unanimously.

Secretary Pate said the next resolution up for consideration was the NASS Resolution Reaffirming Support for the National Electronic Notarization Standards. He said the resolution was set to expire this year unless reauthorized. He noted that NPA has offered several amendments to the standards which have been distributed to the members over the last few months, and any feedback has been incorporated into the document. He said NPA has offered to prepare an implementation guide for the document. He also noted that the requirement for physical presence is still in the standards and has not been changed at all. Secretary Grimes' staff representative reported on behalf of Secretary Grimes, who is co-chair of the NASS Task Force on Remote Notarization, that she is concerned about taking action on the e-notarization standards before the Task Force has had a chance to fully consider and discuss the relevant issues. Secretary Schedler said he has spoken with Secretary Grimes and understands the arguments on different sides of the issue, but he said there are still a lot of unanswered questions and he had concerns about moving away from a personal presence requirement. NASS Executive Director, Leslie Reynolds, provided additional background information and clarification. She noted that NPA met

last fall to review the e-notarization standards, and there was debate about whether the personal presence requirement limited the progress and efficiency of e-notarization. She noted that as a result of that conversation NASS formed a Task Force on remote notarization to better understand that process and the potential implications. She noted that the NPA changes streamlined and clarified the current e-notarization standards but did not change the substance of the document. She noted that the Committee could take several approaches with the standards, including allowing them to sunset and revisiting at a later time (which could impact those states that are working to implement the standards or already have implemented them), postponing action on the standards until the remote notarization Task Force completes its work (which would leave the personal appearance requirement in place), or reauthorizing the standards now with the NPA changes (which leaves personal appearance but streamlines and updates for implementation), and consider amending later with language on remote notarization, if desired once the Task Force is complete. Secretary Pate suggested that the Committee move forward with the last option.

Action Item

Secretary Jaeger moved that NASS reauthorize the NASS Resolution Reaffirming Support for the National Electronic Notarization Standards with the suggested amendments from NPA. The motion was seconded by Secretary Marshall and passed unanimously.

Secretary Bullock provided an update on federal legislative activity concerning proposals for the collection of beneficial ownership information. He noted that NASS has argued for several years that it supports law enforcement efforts to prevent money laundering and other financial crimes, but does not believe requiring 50 different state systems to collect beneficial ownership information is the right approach, particularly since the information is already collected by the IRS. He said his office has been working with the Senators from Delaware to draft a legislative proposal that was consistent with the NASS position on having the IRS make responsible party information from the Employer Identification Number (EIN) SS4 form available to law enforcement. Rick Geisenberger noted that federal legislation, S.3268 The Closing Loopholes Against Money-Laundering Practices Act was introduced by Senators Carper (D) and Coons (D) from Delaware and cosponsored by Senator Heller (R-NV) (former NV Secretary of State) making it a bipartisan bill. He outlined the key provisions of the bill, noting that it would require all entities to obtain an EIN using the SS4. He said most entities are already required to obtain an EIN but the bill would close loopholes for certain entities. He added that it provides limited discretion for the Secretary of the Treasury to disclose responsible party info from the SS4 to federal law enforcement for investigations into terrorist and money laundering financial crimes. He noted that this approach would avoid the complications of having 50 different states collect the information. Secretary Bullock noted that the legislation doesn't answer all of the questions, but is consistent with NASS position and he encouraged members to support the bill. Secretary Gardner said the bill does appear consistent with the NASS position, and he made a motion that NASS go on the record endorsing the legislation. Secretary Cegavske seconded the motion. Secretary Jaeger said he would like for NASS to be able to have a specific bill to support that reflects the consensus of the Association in a bipartisan manner, and said he supported the motion.

Secretary Kobach said that the bill would require sole proprietorships to obtain an EIN, and expressed concern that this places an unnecessary burden on these individuals who may lack business expertise and knowledge of regulations. He added that the bill would impose large financial penalties on these individuals if they failed to obtain an EIN. Mr. Geisenberger noted that this provision addresses concerns about existing loopholes, and said it includes an exception if a person demonstrates reasonable cause. Secretary Kobach expressed doubt that lack of awareness of the requirement would qualify as reasonable cause. Mr. Geisenberger noted that it would be important to inform and educate people about the requirement, and added that the form can be filled out quickly online. Several members indicated that they shared Secretary Kobach's concerns about the impact of the EIN requirement. Secretary Martin added that he also has concerns about the potential impact on someone's due process rights. Other members noted that federal authorities are unlikely to pursue penalties against someone who made an honest mistake or oversight, and expressed support for having a specific bill to support that is consistent with the NASS position and provides law enforcement with the information they need.

Secretary Pate asked for a vote on the motion from Secretary Gardner to endorse the federal legislation requiring the IRS to share EIN information with law enforcement. After the voice vote Secretary Pate called for a division. A roll call vote was taken with 15 members opposing the motion, 12 in support, and 1 abstention. As a result the motion failed.

Several members suggested exploring potential changes to the bill that would address the specific concerns raised. Secretary Bullock indicated that this was an option, and said it was important that NASS find a way to move forward at some point. Secretary Simon said it was important to clarify that while the motion to endorse the bill failed, that was not an expression of opposition to the bill, and the Committee agreed. Secretary Pate encouraged members to provide Secretary Bullock with any suggested improvements to the legislation, and said NASS could reconsider the issue at a later date.

Secretary Hargett gave a presentation on efforts in Tennessee to combat scams impacting individuals and businesses in the state. He noted that Tennessee has taken action to prevent companies posing as the business services division through mailings by requiring a disclosure notice on those mailings. He said the Office works with the Tennessee Department of Labor to highlight scams that send solicitations to purchase workplace posters that are available for free. He also noted instances where individuals have filed false UCC statements against someone, and he noted that the filing of fraudulent UCC liens is a Class E felony Tennessee.

The meeting adjourned at 10:30 AM.

Note: the NASS Task Force on Business Identity Theft met on July 16th. The Task Force co-chairs Secretary Pate and Secretary Marshall discussed the results of a Task Force survey on business identity theft, and noted that the survey indicates that states are interested in learning more about the issue and how it affects business and state databases. They encouraged states that have not completed the survey to do so. They noted the importance of staying ahead of business identity fraud and scams, and the

importance of providing victims of these scams with information, resources, and assistance. They also noted the importance of working with other state agencies, particularly the state Attorney General. They encouraged states to continue working to implement the recommendations of the NASS White Paper on Developing State Solutions to Business Identity Theft. They also noted that it was important to continue the discussion on ways to combat business identity theft.

NASS Endorsement of Notary Public Administrators' Resolution to Implement a Series of Best Practices Designed to Achieve Uniformity in Apostilles

Adopted July 13th, 2011

The Notary Public Administration (NPA) Section of NASS is a collection of state government representatives, most of whom work for the Secretary of State, who are experts in the field of notary law and practices. In an effort to further goals of the NPA Resolution to achieve uniformity, to the greatest extent possible, of the characteristics of an apostille, the members of the National Association of Secretaries of State endorse their resolution .

Resolution of the Notary Public Administrators

A Section of the National Association of Secretaries of State
July 20, 2010
Resolution

Recognizing that under the Hague Apostille Convention of 1961 each Competent Authority retains the discretion to issue Apostilles in a form consistent with the basic requirements of the Convention;

And further recognizing that this affords the possibility of a variety of forms;

And further recognizing that the variety of forms issued by US state Competent Authorities has led to confusion among and rejections by intended recipients of US state-issued Apostilles;

And further recognizing that a higher degree of uniformity among US state-issued Apostilles would alleviate confusion and minimize rejections;

The Notary Public Administrators, in order to implement a series of best practices with the goal of achieving uniformity to the greatest extent possible, and in conformity with the Conclusions & Recommendations adopted in 2003 and 2009 by the Special Commission on the practical operation of the Hague Apostille Convention;

Resolve to adopt the following best practices:

- The Apostille shall conform to the model certificate annexed to the Hague Apostille Convention in the form of a bordered square with sides at least 9 centimeters long on an *allonge* that is 8.5 x 11 inches.
- The type of paper to be used for the certificate is at the discretion of the Competent Authorities.
- When affixing an Apostille, Competent Authorities should use the following procedures:
    - Offset the *allonge*
    - Affix the *allonge* to the front of the page that contains the signature and seal that is certified
    - Apply a stamp that overlaps the *allonge* and the underlying public document
    - Where feasible, the *allonge* should be affixed on the left side of the public document; otherwise the allonge may be attached as appropriate. The readability of the Apostille and the public

document should be the primary consideration in making this determination.

- Competent Authorities shall use tamper-evident methods of affixation. The Notary Public Administrators recommend the use of grommets as a uniform standard.
- The following language should be used outside the bordered square:

  "This Apostille only certifies the authenticity of the signature and the capacity of the person who has signed the public document, and, where appropriate, the identity of the seal or stamp which the public document bears.
  This Apostille does not certify the content of the document for which it was issued.
  This Apostille is not valid for use anywhere within the United States of America, its territories or possessions.
  [To verify the issuance of this Apostille: [www.e-Register of issuing state]]"

And the Notary Public Administrators further resolve to encourage the active consideration of issuing electronic Apostilles (e-Apostilles) and operating electronic registers (e-Registers) of Apostilles as suggested by the electronicApostille Pilot Program (e-APP).

Adopted the 13th day of July 2011
in Daniels, WV

EXPIRES: Summer 2016

NASS Resolution Reaffirming Support for the National Electronic Notarization Standards

Adopted on July 12, 2006
Reaffirmed on July 13, 2011

Mission Statement

It is the goal of the National Association of Secretaries of State (NASS) to endorse and promote these technology neutral standards, developed originally by the National E-Notarization Commission,* for secure and feasible implementation of electronic notarization. In the event of ambiguity of a term or standard, it should be interpreted in favor of technology neutrality.

FOREWORD

The National E-Notarization Commission, whose formation was endorsed and sanctioned by NASS at our 2006 Winter Conference and chaired by North Carolina Secretary of State Elaine Marshall and North Dakota Secretary of State Al Jaeger, developed these e-notarization Standards. The Commission worked via conference call in the spring of 2006 and held a public meeting in May 2006 to hear comments on proposed standards. The final Standards were presented to the NASS members for consideration at our 2006 Summer Conference. The NASS members voted unanimously to adopt these Standards, which were reaffirmed in 2011. These Standards will sunset in 2016 unless reaffirmed.

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, nor do they limit the utilization of electronic signatures outside the electronic notarization process.

Definitions

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

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

3. "Electronic notarial act" means an official act by a notary public on or involving an electronic document and using electronic means authorized by the [commissioning official] or the laws of the jurisdiction of appointment.[1]

4. ~~7.~~ "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

[1] These Definitions and Standards use the terms "commission," "commissioning" and "appointment" interchangeably, to refer to a state's authorization of an individual to perform notarial acts.

public in a particular electronic notarization.[2]

5. "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.[3]

6. "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.

7. ~~4.~~ "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~~ these Standards.

8. "Non-repudiation" means the inability of the signer of an electronic document to deny their electronic signature without factual basis.[4]

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. "Notary public" means an individual commissioned or appointed to perform a notarial act by the [commissioning/appointing officer or agency] of this State.[5]

~~10.~~ 11. "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 ~~documents~~ identification credentials to each other without reliance on electronic devices such as telephones, computers, video cameras or facsimile machines.

12. "Registration" and "register" mean a separate commission to perform electronic notarial acts under the laws of this State, or registration with the commissioning official in compliance with these Standards.[6]

---

[2] Although the definitions for "electronic notarial certificate" and "electronic notary seal" 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.

[3] See footnote 2.

[4] The concept of "non-repudiation" is intended to create a presumption of regularity and reliability of electronically executed documents, so that they may be relied upon by third parties. ~~This concept does not limit the ability of a person to assert a denial of an electronic signature, but serves to shift the burden of proof to the party seeking repudiation.~~ This presumption is foundational to commissioning authorities' ability to authenticate notarial acts.

[5] The Revised Uniform Law on Notarial Acts differentiates "notary public" from "notarial officer," which is a notary public OR other individual—for example, judges, clerks, etc.—authorized to perform a notarial act. These Standards contemplate only notaries public.

[6] This new Definition recognizes that some states that have authorized electronic notarization require only a single notary commission for performance of paper-based and electronic notarial acts, while other states require a separate commission for each medium. As such, "registration" and "register" apply to either commissioning or appointment approach.

DRAFT

13. "State" means a state of the United States, the District of Columbia, Puerto Rico, the United States Virgin Islands, or any territory or insular possession subject to the jurisdiction of the United States.

14. "Tamper-evident" means that any changes to an electronic document shall display evidence of the change.

~~11.~~ 15. "Unique to the Notary Public" and "under the sole control" mean with respect to an electronic notarization that the signing device used to affix the electronic signature of the Notary Public and to render the official electronic seal information tamper-evident must be accessible by and attributable solely to the Notary Public to the exclusion of all other persons and entities for the necessary period of time that such device is engaged and operating to effectuate the authorized electronic notarization.[7]

~~*Comments:*~~

~~** The National E-Notarization Commission, whose formation was endorsed and sanctioned by NASS at our 2006 Winter Conference and chaired by NC Secretary of State Elaine Marshall and ND Secretary of State Al Jaeger, developed the e-notarization standards. The Commission worked via conference call in the spring of 2006 and held a public meeting in May 2006 to hear comments on proposed standards. The final standards were presented to the NASS members for consideration at our 2006 Summer Conference. The NASS members voted unanimously to adopt these standards.*~~ *(MOVED TO FOREWORD)*

~~*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.*~~ *(NOW IN FOOTNOTE 2)*

~~*The definitions of "unique to the Notary Public" and "under the sole control" are terms that do not require any particular currently existing technology or preclude any signature or seal technology that may emerge in the future for the purpose of electronic notarization that satisfy these standards.*~~ *(NOW IN FOOTNOTE 7)*

~~*The concept of "non repudiation" is intended to create a presumption of regularity and reliability of electronically executed documents, so that they may be relied upon by third parties. This concept does not limit the ability of a person to assert a denial of an electronic signature, but serves to shift the burden of proof to the party seeking repudiation.*~~ *(NOW IN FOOTNOTE 4)*

[7] The definitions of "unique to the notary public" and "under the sole control" are terms that do not require any particular currently existing technology or preclude any signature or seal technology that may emerge in the future for the purpose of electronic notarization that satisfy these standards.

DRAFT

Standards

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.[8]

~~*Comments:*~~

~~*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.*~~ *(NOW IN FOOTNOTE 8)*

Registration Requirement

3. The commissioning official shall require a notary public to register ~~Before performing any electronic notarial act, a notary public shall register~~ the capability to notarize electronically before performing any electronic notarial act. Such registration shall be with the [commissioning official]~~.~~ every time a notary public adopts a new or additional technology with which to perform electronic notarial acts.

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, d) an exemplar of the notary's electronic signature and of the notary's official electronic seal, and e) any necessary instructions or techniques that allow the notary's electronic signature and/or official electronic seal to be read.~~

The commissioning official shall require a notary public who registers the capability of performing electronic notarial acts to provide the following information: a) the electronic technology or technologies to be used in attaching or logically associating an electronic notarial signature, seal and certificate to an electronic document; b) an exemplar of the notary's electronic signature and official electronic seal, and c) any necessary instructions or techniques supplied by the vendor that allow the notary's electronic signature and official electronic seal to be read.[9]

---

[8] 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.

[9] 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. 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. Although Uniform Electronic Transactions Act (UETA) , and Uniform Real Property Electronic Recording Act (URPERA) and the federal E-Sign Act 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 –

DRAFT

~~*Comments:*~~

~~*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. 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.*~~
(NOW IN FOOTNOTE 9)

Form and Manner of Performing the Electronic Notarial Act

5. ~~When performing an electronic notarization, a notary public shall apply 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.~~

When performing an electronic notarization, a notary public shall complete an electronic notarial certificate and attach or logically associate the notary's electronic signature and seal to that certificate in a tamper-evident manner. Evidence of tampering pursuant to this standard may be used to determine whether the notarial act is valid or invalid.

DRAFT

contained in the notary public's holographic signature and traditional inking and embossing notary seals – also be elements of a notarized electronic document.

~~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.~~ (INCORPORATED INTO STANDARD 5)

~~7~~6. 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, and d) it is attached to or logically associated with the electronic document~~,~~ in a tamper-evident manner. Evidence of tampering pursuant to this standard may be used to determine whether the notarial act is valid or invalid.~~and c) 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 apply an 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.~~ (INCORPORATED INTO STANDARD 5)

~~9~~7. 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, and d) it is attached to or logically associated with the electronic document in a tamper-evident manner. Evidence of tampering pursuant to this standard may be used to determine whether the notarial act is valid or invalid.~~and c) 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~~8. 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.~~9 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.

~~*Comments:*~~

~~*Although Uniform Electronic Transactions Act (UETA), and Uniform Real Property Electronic Recording Act (URPERA) and the federal E-Sign Act 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.*~~ *(NOW IN FOOTNOTE 9)*

~~*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, nor do they limit the utilization of electronic signatures outside the electronic notarization process.*~~ *(NOW IN FOREWARD)*

Security Requirements

~~12~~10. The notary public shall not disclose any access ~~share the information~~ used to affix the electronic notary's signature and seal ~~in registering with the [commissioning official]~~ except when requested by law enforcement, the courts, and with reasonable precautions, electronic document preparation and transmission vendors.[10]

[10] 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.

DRAFT

~~*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.*~~ *(NOW IN FOOTNOTE 10)*

Requirements for Authenticating the Notarial Act

~~13~~11. 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 will be rendered ineligible for authentication by the [commissioning official] 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.[11]

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

~~14~~12. 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.[12]

~~15~~13. Electronic ~~C~~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.[13]

~~*Comments:*~~

---

[11] "Authentication" in this context is "a certification of the genuineness of the official character, i.e., signature and seal, or position of a foreign official. It is an act done with the intention of causing a document which has been executed or issued in one jurisdiction to be recognized in another jurisdiction. Documents which may require authentication include legal instruments notarized by foreign notaries or other officials, and copies of public records, such as birth, death, and marriage certificates, issued by foreign record keepers." (22 CFR 92.36)

[12] 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, authentication and non-repudiation. The term "public document" is used as defined in Article 1 of the Hague Conference on Private international Law's Convention Abolishing the Requirement of Legalisation for Foreign Public Documents.

[13] 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, authentication and non-repudiation. The term "public document" is used as defined in Article 1 of the Hague Conference on Private international Law's Convention Abolishing the Requirement of Legalisation for Foreign Public Documents.

DRAFT

~~*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, authentication and non-repudiation. 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, authentication and non-repudiation.*~~ *(NOW IN FOOTNOTE 12)*

-

~~*"Authentication" in this context is "a certification of the genuineness of the official character, i.e., signature and seal, or position of a foreign official. It is an act done with the intention of causing a document which has been executed or issued in one jurisdiction to be recognized in another jurisdiction. Documents which may require authentication include legal instruments notarized by foreign notaries or other officials, and copies of public records, such as birth, death, and marriage certificates, issued by foreign record keepers." (22 CFR 92.36)*~~ *(NOW IN FOOTNOTE 11)*

-

DRAFT

~~*The term "public document" is used as defined in Article 1 of the Hague Conference on Private international Law's Convention Abolishing the Requirement of Legalisation for Foreign Public Documents.*~~ *(NOW IN FOOTNOTES 12, 13)*

Adopted the __th day of July 20__
in _____, ____

EXPIRES: Summer 20__