



Notarization Task Force on Best Practices & Verification Standards to Implement Electronic Notarization

Report to the Governor and General
Assembly

December 2019

The contents of this report are based upon the findings of the Notarization Task Force on Best Practices and Verification Standards to Implement Electronic Notarization, pursuant to Public Act 100-0440.

To the Governor and the Members of the Illinois General Assembly,

Traditional notaries public are charged with three basic duties when serving the public as an impartial witness related to the signing of documents – to verify the identity of the signer, to confirm that the person is signing of their own free will and to witness the signing of the document. Since its inception, this function has always been performed in-person.

Consumers and businesses may struggle to access and utilize these services for a variety of reasons including time constraints, the inability to travel, living in an underserved area or the modern-day development of shifting documents from paper-based to electronic-based.

Due to technological advances, the ability to witness and sign documents electronically now exists. To better serve those in need of notary services, several states across the country have begun exploring and implementing electronic notarization and/or Remote Online Notarization (RON) as a convenience.

Electronic notarization may occur either remotely or in-person, but the documents, signature, seal and certification will all be transacted digitally in either case. A remote transaction will occur online with the signer appearing before the notary public via online audio-video technology, while an in-person appearance may occur when processing a digital document.

The Notarization Task Force on Best Practices and Verification Standards to Implement Electronic Notarization, or E-Notary Task Force for short, held meetings between September 2018 and December 2019. Discussions focused on the legislative landscape throughout the country and the task force sought testimony of industry experts, vendors and other stakeholders alike, in order to make a sound assessment on the feasibility of implementing electronic notarization in Illinois and to reasonably anticipate its impact on commerce, government and consumers.

Pursuant to Public Act 100-0440, the task force is pleased to present you with the report and recommendations based on its findings.

Sincerely,

A handwritten signature in black ink, appearing to read "David Weisbaum". The signature is fluid and cursive, with a long horizontal stroke at the end.

Members of the E-Notary Task Force
David Weisbaum, Chairman

Table of Contents

- Member List..... 5
- Purpose of the Task Force..... 7
- Overview of Meetings..... 7
- Testimony from Interested Parties
 - Financial Industry..... 10
 - Cook County Recorder of Deeds – Deputy Recorder John Mirkovic 11
 - Housing and Urban Development, Office of Inspector General – Brad Geary..... 11
 - Pennsylvania Association of Notaries - Marc Aronson..... 12
 - American Society of Notaries - Kathleen Butler..... 13
 - National Notary Association - Bill Anderson..... 15
- Vendor Presentations..... 16
- National Standards
 - Revised Uniform Law on Notarial Acts (RULONA) 2018..... 16
 - Mortgage Industry Standards Maintenance Organization (MISMO)
 - Remote Online Notarization Standards..... 17
 - National Association of Secretaries of State..... 17
- States with Best Practices
 - Nevada, Indiana and Texas..... 18
- Basic Assessment and Recommendations
 - Standards for an electronic signature and seal..... 19
 - Application process for electronic notarial commission..... 20
 - Training and best practices..... 20
 - Fees..... 21
 - Document acceptance..... 21
 - Security measures..... 21
 - Revocation..... 22
- Final Recommendation..... 23

Attachments

Pennsylvania Association of Notaries - Marc Aronson.....	Appendix A
American Society of Notaries - Kathleen Butler.....	Appendix B
National Notary Association - Bill Anderson.....	Appendix C
Revised Uniform Law on Notarial Acts 2018 (RULONA 2018)	
Section 14A.....	Appendix D
Subsection 20 (c).....	Appendix E
Subsection 4 (c).....	Appendix F
Mortgage Industry Standards Maintenance Organization (MISMO)	
Remote Online Notarization Standards.....	Appendix G
National Association of Secretaries of State.....	Appendix H

Task Force Membership

David Weisbaum Director, Department of Index, Secretary of State (Appointed by Secretary of State Jesse White)	Chairman
Senator Linda Holmes 42 nd Senate District (Appointed by Senate President John Cullerton)	Member
Representative Stephanie Kifowit 84 th Legislative District (Appointed by Speaker Michael J. Madigan)	Member
Senator John F. Curran 41 st Senate District (Appointed by Senate Minority Leader Bill Brady)	Member
Paul Hinds DuPage County Clerk (Appointed by House Minority Leader Jim Durkin) <i>Clerk Hinds resigned in January and vacancy was not filled</i>	Member
Mike Standley Chief Deputy Director, Information Technology, Secretary of State	Member
<i>Tiffani Baum</i> <i>Information Technology, Secretary of State</i> <i>(Appointed by Secretary of State Jesse White)</i>	<i>Designee</i>
Andrew Dougherty Consumer Fraud Bureau, Attorney General's Office (Appointed by the Attorney General's Office)	Member
Kenneth Matuszewski (Appointed by the Illinois State Bar Association)	Member
Meredith Mays Espino Corporate Counsel, Accuity (Appointed by the Chicago Bar Association)	Member

Kraig Lounsberry President, Community Bankers Association of Illinois	Member
<i>Megan Peck</i> <i>Vice President, Govt. Relations, Community Bankers Association of Illinois</i> <i>(Appointed by the Community Bankers Association)</i>	<i>Designee</i>
Dan McLean Vice President of Real Estate Operations, Credit Union 1 (Appointed by the Illinois Credit Union League) <i>Kristie James previously served as member</i>	Member
Susan D. Snyder Associate General Counsel, Northern Trust Company	Member
<i>Annette Hurley</i> <i>Senior Legal Counsel, Northern Trust Company</i> <i>(Appointed by the Corporate Fiduciaries Association of Illinois)</i>	<i>Designee</i>
Matthew Farrell Urban Real Estate (Appointed by the Chicago Association of Realtors)	Member
Piero Orsi Precision Title Company (Appointed by the Illinois Association of Realtors) <i>Justin Letheby previously served as member</i>	Member
Amy DeLaney DeLaney DeLaney & Voorn, LTD (Appointed by the National Academy of Elder Law Attorneys, IL Chapter)	Member
VACANT (Appointment by Illinois Bankers Association) <i>Ben Jackson regularly attended for the Illinois Bankers Association</i>	Member
VACANT (Appointment by the Illinois States Attorneys Appellate Prosecutor)	Member

Purpose of the Task Force

As citizens throughout Illinois become more reliant upon electronic devices, they also increasingly rely upon electronic documentation. The use of electronic records has increased substantially since Illinois' adoption of the Electronic Commerce Security Act (1999), the Uniform Real Property Electronic Recordings Act (2004) and the federal adoption of the Electronic Signatures in Global and National Commerce Act (E-Sign Act, 2000).

The Notarization Task Force on Best Practices and Verification Standards to Implement Electronic Notarization, created by Senate Bill 1459 (Senator Linda Holmes/Representative Stephanie Kifowit), was tasked with reviewing and reporting on national standards for best practices in relation to electronic notarization, including security concerns and fraud prevention.

The goal of the task force is to investigate and provide recommendations on national and state initiatives to implement electronic notarization in such a manner that increases the availability to notary public services, protects consumers, and maintains the integrity of the notarization seal and signature.

In order to meet the growing demand for electronic commerce that is both convenient and secure, by statute, the task force was mandated to meet no less than five (5) times between the effective date (August 25, 2017) and December 31, 2019 and a report of findings and recommendations is to be submitted to the Governor and the General Assembly by June 30, 2020.

Overview of Meetings

The E-Notary Task Force met eight (8) times between September 2018 and December 2019. A brief description of each meeting will follow below and the agendas and minutes from those meetings can be located at the following website:

https://www.cyberdriveillinois.com/services/open_meetings_act/notarization/home.html

- ***September 5, 2018***

The appointed members of the task force met for an organizational meeting. The requirements of Public Act 100-0440 were outlined and Senator Linda Holmes and Representative Stephanie Kifowit briefed the members on the genesis for their legislation. Discussions centered around the current requirements of notaries public in Illinois, the states who are implementing electronic notarization, and the work of the Uniform Law Commission through Revised Uniform Law on Notarial Acts (RULONA) 2018 to try and address electronic notarization. The members decided to hear from financial institutions at the next meeting.

- ***January 17, 2019***

Representatives from the financial industry were slated for testimony. The Community Bankers Association of Illinois (CBAI) indicated that they were remaining neutral, however were interested in potential legislation and suggested consideration to electronic notarization being permissive, that an electronic notary must first be a traditional notary, that the two types of notary be a separate commission (and bond), that the certificate for an electronic notary indicate that it was accomplished using audio-video communication and that the record be kept for five (5) years. The Illinois Credit Union League (ICUL) remained neutral as well, but indicated that there was significant interest in the convenience of electronic notarization with specific concerns to the security of the transaction and that the act be optional and not mandatory.

John Mirkovic, Deputy Recorder for the Cook County Recorder of Deeds offered testimony in support of electronic notarization, noting that it was a specific suggestion that stemmed from his work on the Illinois Blockchain Task Force. The task force discussed states throughout the country that had implemented electronic notarization and indicated specific interest in Indiana, Nevada and Texas. The members decided to hear from the Department of Housing and Urban Development regarding fraud related schemes and to further scrutinize the statutes for Indiana, Nevada and Texas at the next meeting.

- ***February 22, 2019***

A representative from the Department of Housing and Urban Development Office of the Inspector General (HUD OIG) offered testimony on fraudulent schemes, specifically relating to insurance fraud with the Federal Housing Authority (FHA). He indicated that many of these schemes started out with the fraudulent notarization of deeds and the subsequent transferring of property out of a person's possession.

The task force engaged in a robust conversation about the specific legislation that created electronic notarization in Indiana, Nevada and Texas. The aspects that members liked included an approved vendor list, a roster of individuals who were commissioned to do electronic notarization with particular note if a notary's status was revoked, and various training requirements.

Amy DeLaney, representing the National Academy of Elder Law Attorneys, expressed concerns about the electronic notarization of transfer documents when involving senior citizens, noting that one (1) out of ten (10) seniors are financially exploited. The members decided to issue a Request for Information (RFI) to hear from vendors who currently offer electronic notarization services at the next meeting.

- ***April 17, 2019***

Four (4) vendors responded to the RFI and two (2) were on hand to offer demonstrations of the remote online notary services that they offer. One vendor, Notarize Inc., offered services for approximately four (4) years and they have done tens of thousands of transactions in numerous states. The other vendor, Pavaso, has been offering remote notary services for approximately one (1) year, primarily for mortgage closings. After an in-depth question and answer period, the members agreed to hear from notary associations at the next meeting.

- ***June 19, 2019***

Marc Aronson, President of the Pennsylvania Association of Notaries; Kathleen Butler, Executive Director of the American Society of Notaries; and Bill Anderson, Vice President of Government Affairs for the National Notary Association were all on hand to offer perspectives on the current atmosphere of electronic notarization throughout the country. The discussion focused upon:

- The benefits of a single commission versus a separate commission for electronic notarization
- Fee structures
- Bond requirements
- Education and testing standards
- Regulation of notaries' electronic signatures and seals
- Protection of consumer information
- Benefits of RULONA and the Uniform Electronic Transactions Act (UETA)

The members acknowledged that there is a high reliance upon the competence of the vendor and the technology that they are using, but then discussed legislative options if Illinois were to move forward with electronic notarization. States that are currently using the technology have either (1) adopted RULONA with the 2018 amendments authorizing remote notarization, (2) drafted their own legislation with administrative rules that govern the implementation or (3) accomplished all of the requirements in legislation with no administrative rules. The members decided to meet again to discuss the issue of recommendations from the task force.

- ***July 18, 2019***

The members reviewed suggested requirements for electronic notarization in Illinois based upon the input of the Secretary of State's Index Department, the legislative models in Indiana, Nevada and Texas, and the input from task force members who represent their respective organizations along with the interested parties who have participated in the meetings. The members decided to meet again to discuss the industry impact.

- ***October 17, 2019***

The members met to discuss the impact of electronic notarization on the title and real estate, banking and loans and legal industries. They also reviewed a draft version of the report to the Governor and General Assembly, made recommendations and suggested sharing it with interested parties. The members agreed to meet one more time in December to vote on the report.

- ***December 12, 2019***

The members met to vote on the report to the Governor and General Assembly.

Testimony from Interested Parties

- ***Financial Industry***

1-17-19

Community Bankers Association of Illinois
Megan Peck, Vice President, Government Relations

Megan Peck recognized the need for innovative uses of technology to make the notary process more efficient and available to the public, while also increasing productivity and customer satisfaction. She stressed the need for a cautious and deliberate approach and encouraged the task force to look at the recently enacted laws in both Texas and Indiana, noting that the financial services industry weighed in heavily in drafting legislation to implement electronic and remote notarization there.

A few key provisions that CBAI and its member banks suggested for possible legislation include:

- Electronic and/or remote notarization should be permissive.
- Should require a notary who performs remote notarization to be a regular notary public of the state first.
- Should require a separate commission (and bond) for notaries to perform electronically and remotely.
- Should require the certificate for an electronic/remote notarial act to indicate that the appearance was accomplished using audio-video communication.
- Should require notaries to keep a record of at least five (5) years of each online notarization, which includes a recording of the audio-video communication session.

1-17-19

Illinois Credit Union League

Dan McLean, Vice President of Real Estate Operations, Credit Union 1

Dan McLean testified that having been in constant communication with Illinois credit unions and the Credit Mortgage Association, he is aware that there is significant interest from their members in the ability to close mortgage loans from the convenience of their homes. He also said that Credit Union 1 has presence in Indiana and Nevada, where they have adopted electronic notary language and they are closely monitoring its impact.

Mr. McLean stressed the importance of the security of the technology, while making electronic notary transactions optional and not mandatory. He recognized that there is a significant liability involved in these transactions and expressed concern that the liability would not fall upon the vendor.

- ***Cook County Recorder of Deeds***

1-17-19

Cook County Recorder of Deeds

John Mirkovic, Deputy Recorder

John Mirkovic, Deputy Recorder for the Cook County Recorder of Deeds offered testimony in support of electronic notarization. He noted that at the Recorder's office they have seen demonstrations of the technology and have been impressed with it. They also will accept electronically notarized documents from a state like Virginia that has authorized electronic notarization.

Mr. Mirkovic stated that electronic notarization was a specific suggestion that stemmed from his work on the Illinois Blockchain and Distributed Ledger Task Force. In a report issued on January 31, 2018, that task force recommended that electronic notarization would "help modernize Illinois law in a clear direction towards electronic commerce and away from the ease of fraud that can be committed by paper-and-stamp methods." The report also noted that, "a holistic look at state notary laws should include an analysis of remote video notarization enablement, biometric based notarization as well as other technology enabled methods which would be a move that would better facilitate electronic transactions."

- ***U.S. Department of Housing and Urban Development
Office of the Inspector General***

2-22-19

HUD OIG

Brad Geary, Special Agent in Charge

Brad Geary explained that his office is responsible for investigating numerous frauds, one of the most notable being related to insurance with the Federal Housing Authority (FHA). He said that when a FHA loan is insured, and in the event it goes into default, the property will often go back to HUD and be resold at a loss.

Mr. Geary outlined the following schemes that his office has witnessed in the Midwest:

- Theft of loan officer identities and appraiser identities in order to make sure that loans go through that otherwise would not have. This is exacerbated in the electronic age.
- Sovereign citizens who trade deeds back and forth, collect security deposits and rent, yet avoid any legal record of transactions.
- Reverse mortgages with poor appraisals that inflate the amount of equity available in a property. He indicated that this scheme often involves senior citizens, taken advantage of by a contractor who offers to perform work, but ends up taking the money with little to no work performed. In other cases, a contractor will file a false lien for work that was never performed to obtain a portion of the sales proceeds.
- Falsification of property deeds due to the physical theft of the notary public stamp. He indicated a notorious case in the early 2000's in Cook County where vacant houses on the Southside of Chicago were being deeded out of peoples' names without their knowledge. The properties were then being resold fraudulently with FHA insurance and people were losing hundreds of thousands of dollars.

Mr. Geary said that when considering potential legislation for electronic notarization, the biggest consideration would be that people clearly understand what they are signing and that internal controls are strong enough to withstand hacking attempts. He indicated that title closings are subject to hacking in an attempt to wire transfer funds to a different destination. He also said that training and communication are vital so that people understand the rules and are trained on how to perform transactions.

- ***Pennsylvania Association of Notaries***

6-19-19

Pennsylvania Association of Notaries

Marc Aronson, President

Marc Aronson said that his comments are his personal thoughts, based upon his 48 years of experience in the industry and do not reflect a position from the Pennsylvania Association of Notaries. He then gave a briefing on trends in electronic notarization across the county, which can be found in **Appendix A**.

Mr. Aronson supported registration and education for electronic notaries; however, did not see the need for two separate commissions as technology simply allows a new tool to perform the same function as a traditional notary. He said that a few states allow enhanced fees for face-to-face electronic notarization, while remote online notarization (RON) incurs additional fees to be split between the notary and the vendor.

For bond requirements, Mr. Aronson said that a few states have increased requirements for RON only, but bond underwriters have indicated that unless a state statute requires a bond specifically for RON, the bond for paper-based or face-to-face electronic notarial acts should also respond to claims for acts performed remotely.

Regarding increased training, he supported mandatory education for all notaries, traditional or electronic. He noted that the process of applying for commission and getting education can be made more efficient and cost-effective if it is performed entirely online. However, in Pennsylvania, notaries receiving in-person education have a higher passing rate on testing than notaries receiving online education.

When asked about statistics on fraud related to electronic notarizations, Mr. Aronson said that it would be awhile before they see any statistics since the technology is so new. When asked what would happen to electronic journals of transactions if a vendor were to go out of business, Mr. Aronson said that there would typically be provisions where the journals must be kept by someone and cannot be sold as an asset.

On the topic of the regulation of electronic signatures and electronic seals, Mr. Aronson described some of the practices in California, North Carolina and Montana, which can be found in **Appendix A**. He noted that states with the Uniform Electronic Transactions Act (UETA) have not specified details, but are waiting for UETA to define them.

Illinois has not adopted UETA, due to the fact that similar legislation, the Electronic Commerce Security Act (ECSA), was previously enacted. (ECSA governs electronic signatures and records, but does not detail which technologies or platforms are to be used. Rather, ECSA states that parties may establish reasonable requirements as to the type of symbol or security procedure that they will accept as a signature.)

- ***American Society of Notaries***

6-19-19

American Society of Notaries
Kathleen Butler, Executive Director

Kathleen Butler gave a briefing on trends in electronic notarization across the county, which can be found in **Appendix B**. Ms. Butler was asked if there are specific security standards imposed upon electronic notaries to protect data in the transaction and personally identifiable

information. She said that for in-person electronic transactions, the security measures would be the same for a traditional notary:

- Personal knowledge, a tangible information credential or the oath or affirmation of a credible witness.
- The Notary must not allow any person other than the credential holder to view or handle the credential.

For a remote online notarization, Ms. Butler referred to standards offered by the National Association of Secretaries of State, noting that the technology provider bears the burden:

- The technology must provide a means of authenticating transaction participants to reasonably ensure that only the proper parties have accessed the audio-video communication session.
- The technology must provide reasonable security measures to prevent unauthorized access to the live transmission of the audio-video communication session; the recording of the audio-video communications session; the verification methods and credentials used to verify the signer's identity; and the electronic documents presented for electronic notarization.

Next, Ms. Butler was asked about current trends in mandating the use and retention of notary journals, the type of journal allowed or specified, and related standards. She indicated that twenty-seven (27) states mandate journaling and the notary has a duty to maintain custody and control of the journal, which typically includes:

- The signer's name and address
- The method used to identify the signer (be it personal knowledge or satisfactory evidence of identification, or a technology used in performance of a remote online notarization)
- An indication of the notarial act performed
- Nominal descriptive information about the document presented for notarization
- The date of the notarization

Ms. Butler also said that eleven (11) states require a notary to obtain the signer's signature in the journal, while one state requires the signer's thumbprint in the journal. States that have authorized remote online notarization require the online notary to retain a recording of the audio-video communications session.

Finally, she was asked how customers can be assured that their documents and identity information are safeguarded and what other states are doing toward this effort. She said that Illinois has one of the country's most robust state laws governing data privacy and rather than viewing electronic notarial acts as inherently less secure, she proposes that the technologies

that address transactional integrity and security will make electronic notarial acts inherently more secure.

- ***National Notary Association***

6-19-19

National Notary Association

Bill Anderson, Vice President of Government Affairs

Bill Anderson gave a briefing on trends in electronic notarization across the country, which can be found in **Appendix C**. He indicated three pillars of sound electronic and remote online notarization laws for implementation:

Technology Neutral

- The Revised Uniform Law on Notarial Acts (RULONA) 2018 and the Uniform Electronic Transactions Act (UETA) avoid naming individual technologies, which give the statute a longer shelf life.
- Definitions like “communication technology” and “identity proofing” play to a particular technology, the Internet. Words like “remotely located individual” are also more desirable than an “online notarization.” RULONA also chose to use a more performance-based word, “tamper-evident”, to describe the type of technology a Notary must use instead of a particular technology.

Uniformity Across Jurisdictions

- Large corporate clients who employ dozens to hundreds of Notaries across multiple states are asking for uniformity in Notary statutes so that they can standardize their operations from state to state.
- Many of the statutes of the twenty-two (22) states that have enacted remote notarization are substantially similar.
- Virtually every state has a statute which says that a document notarized by a Notary or notarial officer of another state will be recognized in their state.

Consistency

- When prescribing the informational elements that go into a Notary’s electronic seal or official stamp, make sure that they match the elements of the Notary’s physical stamp.
- Use of the word “Notary Public” to refer to who performs paper, electronic and remote notarizations, which RULONA does.
- Journaling requirements should apply equally for all types of notarizations.
- Education and training should also apply equally for all types of notarizations.

Vendor Presentations

The members expressed an interest in hearing from technology vendors who currently offer electronic notarization or remote online notarization technologies in other states. In observance of the Illinois Procurement Code, the Secretary of State's Office issued a Request for Information (RFI) on March 5, 2019 with a response deadline of March 26, 2019. The following companies responded to the RFI.

- Notarize Inc.
- Carahsoft Technology Corp.
- PCC Technology Inc.
- Pavaso

Notarize and Pavaso were both scheduled for presentations, on April 19, 2019, to demonstrate their technology for the members. A description of their demonstrations and the member discussions can be located in the minutes to that meeting at the following website:

https://www.cyberdriveillinois.com/services/open_meetings_act/notarization/notarization0419minutes.pdf

National Standards

- ***Revised Uniform Law on Notarial Acts (RULONA) 2018***

The Revised Uniform Law on Notarial Acts (RULONA) is a comprehensive act that addresses every area of notarial law and has been enacted in twelve (12) states: Colorado, Idaho, Iowa, Minnesota, Montana, North Dakota, Oregon, Pennsylvania, Rhode Island, Vermont, Washington and West Virginia. Due to the increased use of electronic records, amendments to RULONA were approved by the Uniform Law Commission in 2018.

RULONA 2018 was prepared to help address the acceptance of electronic records coupled with the rapidly emerging trend among states to authorize the performance of notarial acts by means of audio-visual technology. States who enact RULONA 2018 will authorize notary publics to perform notarial acts in the state in which they are commissioned for remotely located individuals using audio-visual communication technology regardless of where the individual may be located.

RULONA 2018 includes provisions to provide a stable infrastructure for the performance of notarial acts with respect to electronic records and signatures. Amendments to RULONA 2018 include:

- Section 14A to address remote notarization.
- Subsection 20 (c) to allow a notarial officer to certify that a tangible or paper copy of an electronic record is an accurate copy.

- Subsection 4 (c) to authorize the recorder to accept that certified copy for recording.

These three sections can be found in **Appendix D, Appendix E and Appendix F.**

- ***Mortgage Industry Standards Maintenance Organization (MISMO) - Remote Online Notarization Standards***

The Mortgage Industry Standards Maintenance Organization (MISMO) created standards for remote online notarization in an effort to promote consistency for the mortgage industry and state regulations and in the interest of further adopting remote online notarization.

Their standards took into account input from the Mortgage Bankers Association (MBA) and the American Land Title Association (ALTA). The full document can be found in **Appendix G.**

- ***National Association of Secretaries of State Revised E-Notarization Standards***

In 2006, the National Association of Secretaries of State (NASS) formed the National E-Notarization Commission to develop in-person electronic notarization standards, which were unanimously adopted by NASS members. Ten (10) years later, NASS formed the Remote Notarization Task Force to develop standards for remote notarization with a focus on credibility of the process, identity fraud prevention and accountability to the public. The work of this task force resulted in an addendum to the in-person electronic notarization standards to accommodate remote notarization, which were adopted by NASS members in 2018.

The full document can be found in **Appendix H.** The addendum addressed the following standards:

- Personal Appearance Requirement
- Registration Requirement
- Form and Manner of Performing the Electronic Notarial Act
- Security Requirements
- Requirements for Authenticating the Notarial Act
- Requirements for Issuance of Electronic Apostilles and Certificates of Authentication (Appointment)
- Authority to Perform Electronic Notarizations Using Audio-Video Communication
- Requirements for Remote Electronic Notarization Systems

States with Best Practices

- ***Indiana, Nevada, and Texas***

The task force reviewed electronic notary legislation from other states and determined that the statutes in effect in Indiana, Nevada, and Texas represented the best practices in use at this time. Each of these states' statutes is consistent in most regards. For example, all states include explicit definitions of the terms used in electronic notarizations; establish fees electronic notaries are entitled to charge consumers; establish technological standards that electronic notary vendors and participants must adhere to when performing electronic notarizations; and require audio-video communication that enables the notary and the consumer to communicate in real time.

The substantive differences between these statutes are few. For example, Nevada and Indiana require an applicant for an electronic notary commission to complete a required course of study prior to being commissioned. Texas does not require a course of study nor continuing education. The task force considered this substantive difference and recommended that legislation introduced in Illinois should include a requirement for a course of study to protect the integrity of the notarial process, as well as to protect the notary from inadequate information or a misunderstanding of technological standards.

Likewise, each of the states requires an electronic notary to record and retain the transaction; however, they differ in the length of time for which that record must be retained. Nevada requires that the recording be maintained for not less than seven (7) years whether the notarization was completed or not. Indiana requires the same recording and electronic journal of the notary to be maintained for ten (10) years and Texas requires the recording to be maintained for five (5) years.

Texas does not require an electronic notary to maintain an electronic journal; however, both Nevada and Indiana do. The task force recommends requiring a journal for all notaries as further evidence of the act, as well as the verification of the signer's identity.

The most important difference to the task force is the state's role in regulating the technology used by electronic notaries. For example, each state requires "tamper evident" technology in order to protect the personally identifying information of the signers, as well as the integrity of the notarization. They differ, though, in what level of regulation the Secretary of State has in determining appropriate technology standards. For example, Texas requires that the Secretary of State adopt rules that provide standards for credential analysis and identity proofing, and to further regulate the security of the technology used in online notarization. The task force recommends that the Secretary of State set base technological standards by adopting existing standards (i.e. ISO) and that the requirements to maintain those standards fall upon the vendor platform chosen by the notary. This process will allow the Secretary of State to maintain consistency and verify the security of online information shared by Illinois residents, as well as

to allow for the ever changing and improving technology that develops rapidly without the necessity of amending the legislation to allow for eventual changes.

Basic Assessment and Recommendations

The task force was required to discuss and provide recommendations regarding standards for an electronic signature, including encryption and decryption; the application process for electronic notarial commission; and the training of notaries on electronic notarization standards and best practices prior to the commission of an electronic notary's electronic signature. The task force was further required to evaluate and make recommendations on fees for notary application and commission, on which documents and acts can be attested to by electronic notaries, and on security measures that will protect the integrity of the electronic notary's electronic signature, as well as standards that the Secretary of State may rely upon for revoking an electronic notarization.

Finally, the task force was required to make a recommendation on whether and to what extent the Illinois Notary Public Act (5 ILCS 312) should be expanded and updated. The foregoing subjects are discussed in detail below.

- ***Standards for an Electronic Signature and Seal***

The task force recommends that the electronic seal and signature must be logically attached to the document being notarized. To protect the integrity of the notarial process, an electronic notarization must be performed using audio-video communication and the notarial certificate must include language verifying that the audio-video communication was used in the notarization. Further, the electronic seal, signature, and the notarized document must be capable of independent verification and tamper-evident so that any subsequent change or modification will be evident.

The task force recommends that an electronic notary have an affirmative duty to keep the electronic signature and seal in his or her exclusive control, prohibit any access by a third party, and when not in use that the signature and seal be kept secure and protected by use of a password. Further, the electronic notary should be statutorily prohibited from providing access or disclosing information necessary to use or affix the signature and seal except when ordered by law enforcement or a court order. The electronic notary should also be statutorily prohibited from selling or transferring personal information, except when required by law, legal process and/or government authorities. In the event that the electronic signature or seal is compromised, stolen, or vandalized, it is the duty of the notary public to advise law enforcement, the vendor providing the electronic notarization platform, and the Secretary of State immediately, but in no event more than ten (10) days from the date that the notary official discovers or suspects that they are no longer in possession of the electronic seal or signature or that the security of the electronic seal or signature has been compromised.

- ***Application Process for Electronic Notarial Commission***

The task force recommends that applicants for electronic notarial commissions hold a four (4) year commission to run concurrently with any traditional notary public commission he or she may also hold. If either the electronic commission or the traditional commission is terminated by the Secretary of State, the other shall also be terminated. The task force recommends that the application process for an electronic notarial commission mirror the process for traditional notarial commissions already set forth in the Illinois Notary Public Act with the following exceptions:

- The applicant must provide an email address and inform the Secretary of State if that email address changes immediately, but not longer than ten (10) days.
- The applicant must complete a course of study on electronic notarization and pass a qualifying examination.
- The applicant must provide a description of the technology or the name of the vendor that the applicant intends to use to create his or her electronic signature in performing electronic acts. It shall be the duty of the Secretary of State to approve qualified vendors acceptable to the Department of Index.
- The applicant must provide an electronic signature so that the Secretary of State may approve the signature to ensure that it meets the requirements of the Notary Public Act and ensure that the it is unique to the commissioned notary.

- ***Training and Best Practices***

When considering the training of notaries on electronic notarization standards and best practices prior to the commission of an electronic notary's electronic signature, the task force reviewed legislation from other states that have already implemented electronic notarization. The statutes clearly indicated that training and a course of study prior to the commission is a best practice recognized by the industry. The task force recommends that the applicants for electronic notarial commissions be required to complete a course of study and pass an examination before being commissioned. The task force specifically recommends that the course of study include at least the following requirements:

- The course must be taken online in order for the applicant to demonstrate a basic online aptitude.
- The course must be no less than one and one half (1.5) hours but no more than three (3) hours in duration.
- The course must provide instruction in electronic notarization, including the law, ethics, technology and procedures.
- The course must be preapproved by the Secretary of State.

- ***Fees***

The task force considered the fees provided for in the Illinois Notary Public Act and the fees charged by other states for commission as an electronic notary public. The average fee charged for electronic notarial commissions, according to industry experts questioned by the task force, is \$25.00. The task force recommends using the national average and assessing a fee of \$25.00 for electronic notary applications.

The task force further considered raising the fee that a notary is allowed to charge, recognizing that electronic notaries will have additional expenses in procuring an electronic notary platform and whether to allow an electronic notary to charge for his or her required travel as allowed in some states. The task force determined that an electronic notary should be authorized to charge up to \$25.00 per electronic notarization, recognizing that some of this fee will necessarily be paid to the vendor the notary chooses. The task force recommends that no additional fees be authorized for electronic notarizations, including any fees associated with required travel. The electronic notary remains able to reject a request to provide notarization if the travel would be burdensome and not cost effective. Further, electronic notarization should eliminate much of the travel requested for a notarization.

- ***Document Acceptance***

The task force considered which documents and acts an electronic notary should be able to attest to. It is the recommendation of the task force that any notarial acts that are authorized by the Illinois Notary Public Act be capable of electronic notarization.

- ***Security Measures***

The task force spent a great deal of its efforts discussing security measures that will best protect the integrity of the electronic notary's electronic signature. In doing so, it offers the following recommendations:

- The applicant must register the technology chosen for electronic notarizations with the Secretary of State.
- The Secretary of State pre-approve vendors to ensure that the vendors meet minimum standards necessary to protect the integrity of the notarial process.
- The vendors be required to follow International Organization for Standardization (ISO) 27000 family of standards or National Institute of Science and Technology (NIST) standards and guidelines appropriate for the technology being used. The Task Force determined ISO and NIST standards are recognized industry standards and are acceptable for the vendors.
- The electronic notary be required to advise the Secretary of State immediately, but in any event, not more than ten (10) days after changing technology or vendor

platforms, changing his or her email address or of a change to their electronic signature or seal.

- The applicant must register an example of his or her electronic signature and official electronic seal.
- Any electronic notarizations performed should be so performed using audio-video communication. This requirement will eliminate the risk that the electronic notary fails to procure the appropriate proof or verification of the signer's identity. The audio-video component must allow the notary and the principal to see one another and to communicate simultaneously, must be recorded, and must be securely maintained by the notary's vendor. The recording of the act is anticipated to prevent the common fraud often seen in traditional notarizations.
- Upon the death, termination or revocation of the notary or his or her commission, the notary or an authorized representative of his or her estate must destroy the disk, certificate, card, software or password that enables electronic affixation of the electronic seal or signature and send to the Secretary of State a written verification that same has been completed.
- The notary shall be required to keep an electronic journal of his or her notarizations and that the journal and any voice or video recordings be maintained for a minimum of five (5) but no more than ten (10) years following the act.

• ***Revocation***

The task force considered standards that the Secretary of State may rely upon for revoking an electronic notarization. In 2017, the General Assembly amended the Illinois Notary Public Act authorizing the Secretary of State to reprimand, suspend, or terminate a notarial commission upon a finding of wrongdoing. The statute further allows for the notary, who may be subject to discipline, to have the opportunity to contest the discipline in an administrative hearing with the Secretary of State. The task force recommends using the same standards and processes for suspending or revoking an electronic notary's commission, with the addition of the following prohibited acts. A notary may not:

- Knowingly create, manufacture, or distribute software or hardware for the purpose of allowing a person that is not commissioned as an electronic notary to notarize documents.
- Wrongfully obtain, conceal, damage or destroy the technology or device used to create the electronic signature of an electronic notary.
- Sell, rent, or otherwise make available to a third party the contents of the notary journal, video records, audio recordings, or any other record associated with any notarial act including personally identifiable information, except when required by law, legal process and/or government authorities.

Final Recommendation

The members of the E-Notary Task Force recognizes that electronic notarization is not only feasible in Illinois, but that it is already having an impact due to Illinois' acceptance of electronically notarized documents from other states. Due to the growing acceptance of electronic notarization, this technology will continue to play a larger role in the local and global landscape of e-commerce.

Electronic notarization offers unique fraud prevention aspects that do not exist under current law. On the frontend, multi-factor authentication will provide additional layers of security to verify that the signer is who they say they are. On the backend, audio-video communication will not only deter fraudulent acts by capturing a record of the transaction, but will serve as evidence against those who attempt fraudulent schemes.

In the interest of better serving businesses and consumers in Illinois, it is the recommendation of the task force that the Illinois General Assembly amend the Illinois Notary Public Act to authorize the Secretary of State to issue electronic notarial commissions to qualified applicants and that electronic notarizations be accepted and recognized statewide.

The Secretary of State's office continually looks for ways to streamline services for the citizens of Illinois and welcomes the opportunity to utilize this emerging technology as another tool for notaries public to more effectively perform their duties.

Illinois Notarization Task Force on Best Practices and Verification Standards to Implement Electronic Notarization

Chicago, IL

June 19, 2019

My name is Marc Aronson. I am the president and CEO of the Pennsylvania Association of Notaries. I am in my 48th year in the notary association business, and have been involved in the electronic signature and electronic notary space since the beginning of the electronic signature age in the year 2000.

Disclaimer: My comments today are my personal thoughts based on my experience and do not reflect the position of the Pennsylvania Association of Notaries or its support of any particular notarial process, technology, or vendor. The Association is, like you, learning about and evaluating new technologies that affect our members and the customers they serve.

I have been asked by the chairperson to comment on the following topics:

- Commissioning of electronic notaries
- Fees for electronic notarizations
- Bond requirements
- Education and testing
- Regulation of electronic signatures and seals

I am going to use these terms to reference different methods of notarization:

- Paper-based notarization
- Face-to-face electronic notarization
- Remote online notarization (RON)

Trends in Notary Public Registration

Are the states issuing a standard commission for paper notarization and a separate commission for electronic notaries?

Registration and education for electronic notarization are good ideas; however, we do not see the need for a separate electronic notary commission. Acting as an electronic notary is simply using a new tool to perform the traditional functions of a notary. The traditional commission as a paper notary public should cover the ability to act as an electronic notary. The state would incur additional expenses for issuing separate commissions. If a state decides to have a separate electronic notary commission, there would need to be a fee to cover the administrative cost.

Do the states allow for a sole electronic notary commission?

No state allows for an electronic notary commission without an existing paper notary commission.

Is there an enhanced fee for electronic notary commissions?

There are a few states who permit enhanced fees with *face-to-face* electronic notarization; *remote online notarization* incurs additional fees.

Twenty-two states have RON laws on the books. Fees range from \$4 to \$25 per notarization. Ten states permit the notary to charge \$25.

It should be noted that 75-80 percent of notaries public are employed and either do not charge a fee or turn the fee over to the employer by agreement.

A fee for RON transactions is split between the notary and the vendor.

Is there a higher bond requirement for electronic notary commissions?

For face-to-face electronic notarization, the bond requirements are the same as for paper-based notarization.

For remote online notarization, the bond requirements are the same with a few exceptions: Florida - \$25,000 in addition to \$7,500 paper-based; Utah - \$5,000 in addition to \$5,000 paper-based.

Note: Florida is the only state that requires \$25,000 errors and omissions (E&O) insurance.

Bond underwriters have told us that unless a state statute requires a bond specifically for remote online notarization, the bond for paper-based notarial acts or face-to-face electronic notarial acts should respond to claims for acts performed remotely.

Are education and testing standards established in other states? If so, does this occur with renewal of credentials?

Implementation of electronic notarization is a good time to consider mandatory education for all notaries public.

The three notary associations present today support and recommend education for all notaries public. The basic assurances of notarization are the same, whether paper or electronic.

In states where notary education is not required, getting education as an electronically-enabled notary might be the only education a notary gets.

Education and testing standards for face-to-face electronic notarization are established in Arkansas, Nebraska, Nevada, North Carolina.

For RON, Florida, Montana, Nebraska, Nevada, and Ohio required education.

There are approximately 18 states requiring some form of education and approximately 20 states requiring some form of exam.

State	Exam	Education
Alabama		Discretion of probate judge
Arkansas	Paper-based notaries Electronic notaries	Electronic notaries
California	New and renewing notaries	New notaries — 6 hours Renewing notaries — 3 hours
Colorado	New notaries only	New notaries or notaries who miss reappointment for more than 30 days must take an educational course
Connecticut	Open book, on commission application	
Delaware		Yes for electronic notaries, including continuing education
D.C.		Scheduled orientation session for new or not renewed for 12 months
Florida		3 hours live or interactive; new notaries only RON requires education
Guam	Yes	
Hawaii	Yes	
Idaho		Starting July 1, 2019
Indiana		Every two years
Louisiana	Yes (non-attorneys)	
Maine	Open book, on commission application	
Missouri		Yes: 3- hour education for new and renewing notaries; online or written course
Montana	Yes, new or expired for more than 30 days	RON requires education
Nebraska	Yes, open book, Paper-based Electronic notaries	Electronic notaries RON requires education
Nevada	Yes, for electronic notaries	4 hours: New and existing notaries who violate any provision of chapter 240, NRS, or lapsed more than one year; RON requires education

State	Exam	Education
New York	New notaries and notaries whose commissions have lapsed by more than 6 months; proctored exam	
N. Carolina	Yes (NC attorneys exempted)	New notaries: 6-hour course (NC attorneys exempted); education requirement for notaries wishing to perform electronic notarizations
Ohio	Yes: In most counties; type of exam varies by county	Not required by law, but offered in many counties as preparation for the examination RON requires education
Oregon	Open book, on commission application	3 hours for new commission applicants, or lapsed renewing
Pennsylvania	First time notaries or lapsed even one day	All notaries, 3 hours on commissioning, live or online
Puerto Rico	Yes (civil law tradition)	Educational requirement for attorneys
Utah	Yes	
Wisconsin	Tutorial exam	
Wyoming	Completion of at-home test is “encouraged, but not mandatory”	

Note: States not listed have no testing or education requirements for notaries.
Sources: American Society of Notaries; National Notary Association

Do any states combine online application with online education and testing?

The process of applying for commission and getting education can be made more efficient and cost-effective if it is performed entirely online. However, in Pennsylvania, we can say that notaries receiving in-person education have a higher passing rate on testing than notaries receiving online education.

How are electronic notaries’ electronic signatures and seals regulated in states? Do states keep a database of these identifiers?

States with UETA did not specify the form of electronic signatures and seals, relying on UETA to define them. Of course, Illinois does not have UETA; instead, you have the law that was the foundation for the drafting of UETA. Your Electronic Commerce Security Act (5 ILCS 175) became effective July 1, 1999.

As states become more prescriptive about electronic signatures and seals, notaries must ensure compliance, custody and control, security, etc.

For example, Arkansas no longer requires notaries who perform eNotarizations to obtain a digital certificate from the Secretary of State's office to create an electronic signature, but requires the notary's electronic signature to be (a) unique to the notary; (b) capable of independent verification; (c) retained under the notary's sole control; and (d) attached to or logically associated with the electronic document in a manner that produces evidence of any changes to the electronic document ("tamper-evidence").

California Government Code Section 8207:

The seal must:

- Be photographically reproducible when affixed to a document;
 - Contain the State Seal and the words "Notary Public";
 - Contain the name of the notary public as shown on the commission;
 - Contain the name of the county where the oath of office and notary public bond are on file;
 - Contain the expiration date of the notary public's commission;
 - Contain the sequential identification number (commission number) assigned to the notary public, as well as the identification number assigned to the seal manufacturer or vendor;
- and
- Be circular not over two inches in diameter, or be a rectangular form of not more than one inch in width by two and one-half inches in length, with a serrated or milled edged border.

North Carolina

"Electronic Notary Seal" and "Electronic Seal" mean information within a notarized electronic document that includes the notary's name, jurisdiction, and commission expiration date, and generally corresponds to data in notary seals used on paper documents.

§ 10B-37. Seal image.

(a) A notary shall affix the notary's official seal near the notary's official signature on the notarial certificate of a record.

(b) A notary's official seal shall include all of the following elements:

- (1) The notary's name exactly as commissioned.
- (2) The words "Notary Public".
- (3) The county of commissioning, including the word "County" or the abbreviation "Co.".
- (4) The words "North Carolina" or the abbreviation "N.C." or "NC".

(c) The notary seal may be either circular or rectangular in shape. Upon receiving a commission or a recommission on or after October 1, 2006, a notary shall not use a circular seal that is less than 1 1/2 inches, nor more than 2 inches in diameter. The rectangular seal shall not be over 1 inch high and 2 1/2 inches long. The perimeter of the seal shall contain a border that is visible when impressed.

(c1) Alterations to any information contained within the seal as embossed or stamped on the record are prohibited.

(d) A notarial seal, as it appears on a record, may contain the permanently imprinted, handwritten, or typed date the notary's commission expires

Montana

RULONA, 8) “Official stamp” means a physical image affixed to or embossed on a tangible record or an electronic image attached to or logically associated with an electronic record.

1-5-627. Database of notaries public. The secretary of state shall maintain an electronic database of notaries public:

(1) through which a person may verify the authority of a notary public to perform notarial acts; and

(2) that indicates whether a notary public has notified the secretary of state that the notary public will be performing notarial acts on electronic records.

California regulates the vendors of electronic notary seals.

There are four states where the state must approve the face-to-face electronic vendor: AR, NE, NC, PA.

There are five states where the state must approve the RON technology: IN, MI, MT, NV, OH.

There are four states where the state must approve the RON vendor: IN, MI, NE, NV.

North Carolina keeps a representation of the notary’s cursive digitized signature. This allows for authentication of the electronic notarization. Nevada, Texas and Montana also require a digitized cursive signature to be submitted to the state. The graphical scan of the traditional cursive signature may then be compared to the signature on file. The public, clerks and recorders expect the signature to look like a signature and the seal to look like a seal.

Thank you for the invitation to participate today. If I may be of further assistance, please let me know.

Marc L. Aronson
Pennsylvania Association of Notaries
800-944-8790, Ext. 113
maronson@notary.org



**AMERICAN SOCIETY OF
NOTARIES**

**Comments Before the Illinois Notarization Task Force on Best Practices and
Verification Standards to Implement Electronic Notarization
Wednesday, June 19, 2019 – Chicago, Illinois**

Kathleen Butler, Executive Director
American Society of Notaries
kathleen@asnnotary.org • 850-671-5164

American Society of Notaries is the original national, professional organization serving Notaries Public in the United States. ASN was incorporated in 1965 in the District of Columbia, later relocating to Florida and headquartering in the capital city of Tallahassee. ASN is a true non-profit, with no shareholders or for-profit subsidiaries. ASN is governed by a wholly voluntary Board of Directors. The Society offers notary education, supplies, membership services, technical support and legislative/regulatory information to Notaries throughout the United States. ASN is not a notary application processor or agent for the sale of surety bonds or errors and omissions insurance.

Butler’s comments (addressing a sub-set of Task Force questions posed to notary association representatives):

Since [the Task Force] requested our thoughts on trends, my comments on notary requirements are typical of most U.S. states... not Illinois-specific.

Q: Are there specific security standards imposed on eNotaries to protect customer identity information and access to eNotaries’ data?

The answer is yes, but I think it’s important to highlight the limited extent to which Notaries interact with sensitive customer identity data.

An electronic notarial act might be performed by an eNotary for a physically-present signer; or an electronic notarial act might be performed by an eNotary for a remotely-located signer.

For both forms of electronic notarization, **the eNotary interacts with customer identity information for two purposes:** to verify the signer’s identity; and to create and save a journal record.

Let’s look first at security related to a Notary verifying a signer’s identity.

When the electronic notarial act is for a physically-present signer, an eNotary verifies the signer’s identity using the same methods of identification required for notarization of a tangible record—personal knowledge, a tangible identification credential or the oath or affirmation of a credible witness. The main information security standard for handling and examining a tangible identification credential, physically exchanged back and forth between the Notary and the signer, is that the Notary must not allow any person other than the credential holder to view or handle the credential.

When the electronic notarial act is for a remotely-located signer who appears by means of audio-video communications technology, an eNotary uses certain technologies to help identify a signer who is not personally known. It’s here that we find specified security standards.

A useful example comes from the National Association of Secretaries of State Standards for Remote Online Notarization:

The technology must provide a means of authenticating transaction participants to reasonably ensure that only the proper parties have accessed the audio-video communication session.

The technology must provide reasonable security measures to prevent unauthorized access to the live transmission of the audio-video communication session; the recording of the audio-video communications session; the verification methods and credentials used to verify the signer’s identity; and the electronic documents presented for electronic notarization.

Notice that the duty to assure transactional security is placed on technology providers. They are, after all, experts on the technology.

While an eNotary might be required to take “reasonable steps” to ensure the integrity, security, and authenticity of remote online notarizations, such a reasonable step could be obtaining a technology provider’s assurance that its technology achieves those objectives. Or, IF the Notary’s state of commission evaluates and approves technology, a Notary’s reasonable step to ensure use of a remote notarization system that ticks all those boxes would be to choose one from the commissioning officer’s approved list.

[Additional commentary offered during Q&A – While a Notary may rely on technology to help complete formalities of a notarial act for a remotely-located signer, the Notary does not relinquish responsibility for any formality of the notarial act itself. The Notary still must be assured that the signer’s identity is known or satisfactorily established. The Notary must feel assured that the signer is acting with comprehension and intent. The Notary has the right and the responsibility to stop a notarization if he or she believes it cannot be completed compliantly.]

Next, let’s look at security requirements related to an eNotary’s journal record.

Whether required by law or administrative rule, or acting on a strongly recommended notarial best practice, a Notary Public has a duty to maintain custody and control of the notarial tool that contains customer information. That tool is the Notary’s journal.

Presently, around 27 states require journaling of notarial acts, with recent legislation and enactments demonstrating that journaling requirements are on the rise. Depending on the state, journaling may be required for notarization of any record whether it is tangible or electronic, or it may be required only for notarizations using audio/video communications technology. The specified journal format varies also...

it might be a bound, tangible book or it might be an electronic format or both--it depends on the requirements of the Notary's state of commission.

Among the states mandating that the Notary keep records, typical journal entry requirements are:

- The signer's name and address
- The method used to identify the signer... be it personal knowledge or satisfactory evidence of identification, or a technology used in performance of a remote online notarization
- An indication of the notarial act performed
- Nominal descriptive information about the document presented for notarization
- The date of notarization

It's important to note here that typical journal entry requirements do NOT call for actual identification credential data, such as a serial number, to be entered into a journal record... only the form or method of identification and usually, a credential's issue or expiration date.

This principle holds true with regard to the identification verification methods used for remote online notarization... the method used and the outcome is required for the journal record of a remote online notarial act, but not the actual specifics of any knowledge-based authentication or credential analysis performed (two common technological processes in use today).

That said, some states (11), require a Notary to obtain the signer's signature in the journal record. One state requires the Notary to obtain the signer's thumbprint in the journal. States that have authorized remote online notarizations using audio-video communications technology are requiring the online Notary to retain a recording of the audio-video communications session; some go the additional step of including the audio-video recording as a required information element of the related journal entry.

Still, the mere fact that a journal record concerns a signer's private transaction causes any journal record to be regarded as sensitive. So whether by state law, state administrative rules or widely recommended notarial best practices, a Notary Public is required or urged to protect the privacy of tangible and electronic journal records by:

- Maintaining journal records under the Notary's sole access, custody and control
- Storing journal records in a safe and secure manner
- Not sharing a journal with another Notary
- Not relinquishing journal records to an employer unless the reason for doing so is addressed in law or administrative rules
- Providing journal record copies only in response to a lawful request, a court order, a law enforcement investigation or at the direction of the Notary's commissioning official.

Another security-related electronic journal requirement we've seen, particularly when used by a Notary performing remote online notarizations, is that the electronic journal must be regularly backed-up.

Q: What are current trends in mandating the use and retention of notary journals, the type of journal allowed or specified, and related standards.

Much of this has already been discussed, but I'll add one noticeable trend is that a journal requirement for remote online notarizations is typical of remote online legislative proposals and enactments.

This trend is especially noticeable since several states that enacted remote online notarization require an online Notary to keep a journal of remote online notarial acts, but didn't impose a basic journal requirement for other notarial acts.

This feels like a missed opportunity to implement journaling for all notarial acts performed, as all notarial acts are equally relevant regardless the means and manner used to perform them.

Q: What assurances can eNotaries provide to customers that their documents and identity information are safeguarded? What requirements are states imposing on eNotaries?

On the matter of data privacy and security, it's my belief that the issue and any legislative response would exceed the scope of notary laws. I do not claim to be an expert on data privacy law, but I've read that Illinois has one of our country's most robust state laws governing data privacy. This law is broadly applicable, intentionally so. It would address data privacy issues should they arise from allowing Illinois Notaries to perform electronic and remote online notarizations.

[Additional commentary offered during Q&A – Consider that if practitioner-specific laws like Illinois' notary statutes are amended to address data privacy issues that are already handled by Illinois' current data privacy law, it could be interpreted by some that the current data privacy law isn't as strong or broadly applicable as it actually is – an undesirable possible outcome.]

Finally, I think it's helpful to remember that many sensitive electronic documents are composed, shared and executed daily, electronically, without the transactional security measures that are hallmarks of electronic notarization and remote online notarization. Rather than viewing electronic notarial acts as inherently less secure, I propose that electronic notarial acts performed using widely accepted technologies that address transactional integrity and security will make electronic notarial acts inherently more secure.

Thank you.

Introduction

1. In my remarks today I would like to address two of the questions that were presented by the Chair to Marc, Kathleen and me.
 - A. What general benefit do RULONA and UETA provide for states?
 - B. States have created statutes to authorize eNotarization only to return to their legislature for major statute amendments. Is this prevalent and are there trends identifying why states find it necessary to retrofit their statutes? What can Illinois do to avoid this and reduce delays once enabling statutes are enacted?
2. Let me address these questions by presenting 3 pillars of sound electronic and remote online notarization laws you should strive to implement.

Technology-Neutrality

1. The question, “What general benefit do RULONA and UETA provide for states?”, can be answered directly in part with reference to this point.
 - A. UETA and RULONA avoid naming individual technologies because it makes the statute have a longer shelf life. By contrast, Arizona, which in 1999 enacted the very first electronic notarization statute, ended up repealing it last year because it was simply never implemented past the pilot stage. They ran into technology hurdles with sourcing digital certificates that had to be used by a Notary to electronically sign documents.
2. Just this year, Washington state repealed its digital signature statute. It relied on public key infrastructure technology, a specific technology.
3. Technology neutrality is why in the RULONA you have definitions like “communication technology” and “identity proofing.” The RULONA doesn’t use the term “online notarization” because it plays to a particular technology, the Internet. Rather, they refer to an “online notarization” as a notarial act for a “remotely located individual.” And, it chose to use a more performance-based word, “tamper-evident”, as the adjective to describe the type of technology a Notary must use to notarize electronic records instead of a particular technology that makes a record tamper-evident.
4. By contrast, most of the remote Notary bills name particular technologies — knowledge-based authentication, credential analysis, audio-video communication and such. These are useful technologies today, but there will be newer and better technologies tomorrow that will replace them. And when they’re replaced, legislators will have to come back to fix these statutes.

Uniformity

1. Our members tell us they would like to see more uniformity in Notary laws from jurisdiction to jurisdiction.
2. Many of our association's large corporate clients who employ dozens to hundreds of Notaries across multiple states are asking for uniformity in Notary statutes so that they can standardize their operations from state to state.
3. It is remarkable the degree to which the statutes of the 22 states that have enacted remote notarization agree with each other. Most say you must identify signers for a remote notarization using the same methods. Most require Notaries who perform these acts to keep an electronic journal and a recording of the remote notarization. Most require the certificate for a remote notarization to indicate that the signer appeared before the Notary using communication technology. This is good.
4. Another value of uniformity can be illustrated by the interstate recognition provisions in the RULONA and in state laws in general.
 - A. Virtually every state has a statute which says that a document notarized by a Notary or notarial officer of a sister state will be recognized in their state.
 - B. These laws provide that the only requirement for recognition is that a Notary or notarial officer of a sister state notarized it. States have held the view for decades that it is up to the state that commissions the Notary to determine the means and manner in which a notarial act is performed.
 - C. This allows documents to be freely exchanged across state lines hundreds and thousands of times every single day.
 - D. Now, one state, Iowa, passed a law that modified the uniform interstate recognition provision of the RULONA when it enacted it. Iowa said that for us to recognize a notarial act performed by a Notary or notarial officer of a sister state, it must have been notarized in the physical presence of the Notary or notarial officer. But Iowa is the outlier and no other state has followed it.

Consistency

1. In many respects the 22 states that have enacted substantive electronic and remote notarization provisions make it hard for even the best, most committed Notary to follow them because of the stark differences between the paper-based and new electronic and remote notarization

2. This is not to say that there aren't some fundamental differences between performing a paper-based notarization and a remote notarization, because there are ways in which the face-to face and remote environments are different.
 - A. How you identify signers remotely is probably the key difference between the two.
 - B. Privacy, the issue Kathleen addressed, has arisen due to the online environment.
3. While complete consistency may not be possible, the more consistent you are the better it will be for Notaries.
4. Let me point out a few areas where consistency is desirable.
 - A. When you prescribe the informational elements that go into a Notary's electronic seal or official stamp, make sure that they match the elements of the Notary's physical stamp.
 - B. Use the title "Notary Public" to refer to who performs paper, electronic and remote notarizations. You see, the notarial act is the same witnessing act regardless of the medium, environment or tools that a Notary uses to perform the act. Unfortunately, most states will use different terms for the Notary who notarizes paper documents (Notary Public), electronic records (Electronic Notary Public) and remote notarizations (Online Notary Public). I'd encourage you to simply use the term "Notary Public" for all three. RULONA does this.
 - C. Record keeping. Another example is the near unanimous requirement for Notaries to keep an electronic journal of remote notarizations only. We support the policy of Notaries keeping a journal for remote notarizations, but we equally support keeping journals for paper acts too, because it's not just electronically notarized records that carry risk; paper notarial acts have risks too.
 - D. The same goes for education requirements. Education is good policy for all notarial acts and not just some. I fear that the states now requiring training only for remote notarial acts are sending the message that there's not much to performing a paper notarization.
 - E. One final example – and probably the most extreme – is in the Florida bill just signed into law. In that bill, for a Notary to perform witnessing services in a remote context related specifically to last wills, trusts, health care directives, powers of attorney and spousal waivers, the Notary is required to ask the witness 5 questions in substantially these words:
 - a. Are you currently married? If so, name your spouse.
 - b. Please state the names of anyone who assisted you in accessing

this video conference today.

- c. Please state the names of anyone who assisted you in preparing the documents you are signing today.
 - d. Where are you currently located?
 - e. Who is in the room with you?
- F. The biggest concern I have with this is that it applies to certain records and not others. How is a Notary supposed to remember the specific transactions that require the questions if the Notary handles a remote notarization involving witnesses to a last will, health care directive, power of attorney or spousal waiver infrequently? And, why wouldn't it be good policy to require a Notary to ask these same questions for a witnessing of a last will on paper?

RULONA 2018

SECTION 14A. NOTARIAL ACT PERFORMED FOR REMOTELY LOCATED INDIVIDUAL.

(a) In this section:

- (1) "Communication technology" means an electronic device or process that:
 - (A) allows a notary public and a remotely located individual to communicate with each other simultaneously by sight and sound; and
 - (B) when necessary and consistent with other applicable law, facilitates communication with a remotely located individual who has a vision, hearing, or speech impairment.
- (2) "Foreign state" means a jurisdiction other than the United States, a state, or a federally recognized Indian tribe.
- (3) "Identity proofing" means a process or service by which a third person provides a notary public with a means to verify the identity of a remotely located individual by a review of personal information from public or private data sources.
- (4) "Outside the United States" means a location outside the geographic boundaries of the United States, Puerto Rico, the United States Virgin Islands, and any territory, insular possession, or other location subject to the jurisdiction of the United States.
- (5) "Remotely located individual" means an individual who is not in the physical presence of the notary public who performs a notarial act under subsection (c).

(b) A remotely located individual may comply with Section 6 by using communication technology to appear before a notary public.

(c) A notary public located in this state may perform a notarial act using communication technology for a remotely located individual if:

- (1) the notary public:
 - (A) has personal knowledge under Section 7(a) of the identity of the individual;
 - (B) has satisfactory evidence of the identity of the remotely located individual by oath or affirmation from a credible witness appearing before the notary public under Section 7(b) or this section; or
 - (C) has obtained satisfactory evidence of the identity of the remotely located individual by using at least two different types of identity proofing;
- (2) the notary public is able reasonably to confirm that a record before the notary public is the same record in which the remotely located individual made a statement or on which the individual executed a signature;
- (3) the notary public, or a person acting on behalf of the notary public, creates an audio-visual recording of the performance of the notarial act; and
- (4) for a remotely located individual located outside the United States:
 - (A) the record:
 - (i) is to be filed with or relates to a matter before a public official or court, governmental entity, or other entity subject to the jurisdiction of the United States; or
 - (ii) involves property located in the territorial jurisdiction of the United States or involves a transaction substantially connected with the United States; and

(B) the act of making the statement or signing the record is not prohibited by the foreign state in which the remotely located individual is located.

(d) If a notarial act is performed under this section, the certificate of notarial act required by Section 15 and the short-form certificate provided in Section 16 must indicate that the notarial act was performed using communication technology.

(e) A short-form certificate provided in Section 16 for a notarial act subject to this section is sufficient if it:

- (1) complies with rules adopted under subsection (h)(1); or
- (2) is in the form provided in Section 16 and contains a statement substantially as follows: "This notarial act involved the use of communication technology."

(f) A notary public, a guardian, conservator, or agent of a notary public, or a personal representative of a deceased notary public shall retain the audio-visual recording created under subsection (c)(3) or cause the recording to be retained by a repository designated by or on behalf of the person required to retain the recording. Unless a different period is required by rule adopted under subsection (h)(4), the recording must be retained for a period of at least [10] years after the recording is made.

(g) Before a notary public performs the notary public's initial notarial act under this section, the notary public must notify the [commissioning officer or agency] that the notary public will be performing notarial acts with respect to remotely located individuals and identify the technologies the notary public intends to use. If the [commissioning officer or agency] has established standards under subsection (h) and Section 27 for approval of communication technology or identity proofing, the communication technology and identity proofing must conform to the standards.

(h) In addition to adopting rules under Section 27, the [commissioning officer or agency] may adopt rules under this section regarding performance of a notarial act. The rules may:

- (1) prescribe the means of performing a notarial act involving a remotely located individual using communication technology;
- (2) establish standards for communication technology and identity proofing;
- (3) establish requirements or procedures to approve providers of communication technology and the process of identity proofing; and
- (4) establish standards and a period for the retention of an audio-visual recording created under subsection (c)(3).

(i) Before adopting, amending, or repealing a rule governing performance of a notarial act with respect to a remotely located individual, the [commissioning officer or agency] must consider:

- (1) the most recent standards regarding the performance of a notarial act with respect to a remotely located individual promulgated by national standard-setting organizations and the recommendations of the National Association of Secretaries of State;
- (2) standards, practices, and customs of other jurisdictions that have laws substantially similar to this section; and
- (3) the views of governmental officials and entities and other interested persons.

[(j) By allowing its communication technology or identity proofing to facilitate a notarial act for a remotely located individual or by providing storage of the audio-visual recording created under subsection (c)(3), the provider of the communication technology, identity proofing, or storage appoints

the [commissioning officer or agency] as the provider’s agent for service of process in any civil action in this state related to the notarial act.]

Legislative Note: *Subsection (j) is an optional subsection.*

Comment

This section authorizes a notary public to perform notarial acts in the state in which he or she is commissioned on behalf of an individual who is not physically present before the notary public. That remote individual may be located elsewhere in the state in which the notary is located, elsewhere in the United States, or outside the United States.

This section requires that a notary public perform the notarial act in the state in which he or she is commissioned or in another state in which he or she is authorized to act, to the extent that a neighboring state, by other law, may authorize a notary public, usually as a matter of comity and convenience, to perform a notarial act in the state or part of the state.

Subsection (a):

“Communication technology.” Subsection (b) authorizes a remotely located individual to appear before a notary public by means of communication technology. Subsection (a)(1) defines the method of electronic communication by which the notary public and the remote individual must communicate. Subsection (a)(1)(A) provides that the technology must afford synchronous communication between the notary public and the remotely located individual; asynchronous communication is not permitted.

The technology must consist of both audio and video components. The notary public and the remotely located individual must be able to see and hear each other interactively in real time. This will provide a notary public an opportunity to assess the competency of the remotely located individual and evaluate whether the individual’s acts are knowingly and voluntarily made.

Over time communication technology will change. Currently a number of communication systems exist. However, it is recognized that these systems will be updated and that other processes will make their appearance and that other providers will enter the communication technology community. Consequently, communication technology is not limited to a specific protocol or technology. The regulation and approval of communication technology, any changes to it, and their providers resides with the commissioning officer or agency pursuant to subsection (h)(2).

Subsection (a)(1)(B) recognizes that some individuals may have a vision, hearing or speech impairment and may not be able to communicate by sight or sound in the same way as a person who does not have such an impairment. Consequently, this subsection allows for an accommodation that will facilitate communication by and with the person with the impairment. For example, the accommodation might allow for a visual transcription of the other party’s spoken words.

This subsection does not itself state when such an accommodation is required or how it will be implemented. That determination is based on other applicable law at either the federal or state level. Further, the commissioning officer or agency may adopt rules regarding the provision of accommodations to persons with a vision, hearing or speech impairment pursuant to subsections (h)(1) and (h)(2).

“Foreign state.” Subsection (a)(2) defines a foreign state as a foreign country and not the United States, a state in the United States federal system, a federally recognized Indian tribe, or any other location subject to the jurisdiction of the United States.

“Identity proofing.” Subsection (c)(1)(C) authorizes the use of identity proofing to verify the identity of the remotely located individual. This subsection defines that term.

Identity proofing is a service or process that is provided by a third person. The verification is performed by comparing and reviewing data from public or private data sources with information from or provided by the remotely located individual.

The precise methodologies for identity proofing will change over time and this subsection recognizes that fact. Currently, some frequently used technologies involve asking the remotely located individual a number of personal questions, the verification of which can be ascertained from public or private data sources (which is generally referred to as “knowledge-based authentication”), or the remote analysis of the characteristics and security features of identity cards (which is generally referred to as “credential analysis”). Correct answers to identity proofing questions or the analysis of identity cards provide a reasonable degree of certainty regarding the identity of a remotely located individual that is comparable to or better than what occurs in face-to-face notarization. However, the methodologies are not limited to that process. Other methodologies currently exist or may develop. They include, for example, secure password identification or biometric identification.

The regulation and approval of identity-proofing, any changes to it, and its providers resides with the [commissioning officer or agency] pursuant to subsections (h)(2) and (3). Some states may prefer a simple mandate to use reasonably reliable methods of identity proofing subject to compliance actions for failure to do so; others may prefer to adopt standards for communication technologies; while some states may elect to require the pre-approval of all technologies that are used in identity proofing.

“Outside the United States.” In accordance with subsection (c)(4) a notary public may perform a notarial act on behalf of a remotely located individual who is “located outside the United States.” This subsection defines the venues that are located outside the United States as those located outside the geographic boundaries of the United States, Puerto Rico, the United States Virgin Islands, and any territory, insular possession, or other location subject to the jurisdiction of the United States.

“Remotely located individual.” The provisions of this Section apply only to a notarial act performed by a notary public for a remotely located individual. This subsection defines a remotely located individual as a person who is not in the physical presence of the notary public performing the notarial act. The performance of a notarial act on behalf of an individual who is

in the physical presence of the notary public must comply with provisions specified elsewhere in this act.

The remotely located individual may be located in the state in which the notary public is commissioned or elsewhere in the United States. The remotely located individual may also be located outside the United States although, in that case, the requirements specified in subsection (c)(4) apply.

Subsection (b): Section 6 states that an individual for whom a notary public performs a notarial act must appear personally before the notary public. This subsection states that an individual appearing before a notary public by means of communication technology complies with the requirements of that section. In effect, this provision provides a new definition for the personal appearance requirement for a remotely located individual appearing before a notary public by means of communication technology in accordance with this section.

Subsection (c): This subsection sets out specific requirements for the performance of a notarial act on behalf of a remotely located individual.

Subsection (c)(1) states three methods by which a notary public may identify a remotely located individual. Subsection (c)(1)(A) allows the notary public to identify the remotely located individual by personal knowledge as provided in Section 7(a). Thus, a notary public may identify the remotely located individual if the notary public has had prior dealings with the remotely located individual and is able to identify that individual with a reasonable certainty.

Subsection (c)(1)(B) allows a notary public to identify the remotely located individual by means of an oath or affirmation from a credible witness. That witness may be located in the physical presence of the notary public and able to be identified by the notary public in accordance with Section 7(b)(2). Alternatively, the witness may be remotely located and appear before the notary public by means of communication technology, in which case the witness must be able to be identified by the notary public by identity proofing in accordance with the provisions of this Section.

Subsection (c)(1)(C) provides that reasonable identification of a remotely located individual requires the application of at least two different types of identity-proofing processes or services. Thus, for example, an individual may be identified by two of the following technologies: (1) knowledge-based authentication; (2) credential analysis; and (3) biometric identification technology. This subsection does not evaluate or specify which processes or services are to be used. It also permits other identity proofing technologies to be used as they become available and reliable. This act does not mandate that one of the methods of identity proofing utilized must be credential analysis because such an approach would freeze into law technology specific requirements. Subsections (h)(2) and (3) authorize the commissioning officer or agency to establish standards for identity proofing and to establish requirements and procedures to approve providers of identity proofing.

Subsection (c)(2) requires that the notary public be reasonably able to identify the record before the notary public as the same record in which the remotely located individual made a statement or on which the remotely located individual executed a signature.

Thus, for example, a remotely located individual might electronically transmit a record to a notary public; alternatively, the remotely located individual might simply submit the original paper record to the notary public by mail. In either case the notary public might visually display the record to the individual (perhaps reading some or all of the record to the individual) and ask the individual whether the statement or signature is that of the individual.

Alternatively, a notary public might verify the record by means of a secure electronic signature tied to the tamper-evident electronic record which the notary public is notarizing.

Subsection (c)(3) requires that an audio-visual recording of the performance of the notarial act be created. Being able to witness the sight and sound of the conversation between a notary public and a remotely located individual provides substantial evidence as to the validity of the performance of a notarial act as well as evidence as to compliance with the requirements of this Section. The recording may be created either by the notary public or by a person acting on behalf of the notary public. The period for retention of the recording is specified in subsection (f).

Subsection (c)(4) specifies the requirements for the performance of a notarial act for an individual who is located outside the United States.

Subsection (c)(4)(A) provides that the record with regard to which a notarial act is to be performed on behalf of an individual who is located outside the United States must satisfy either of two requirements:

(i) The record may be part of or pertain to a matter that is to be filed with or relates to a matter before a court, governmental entity, or other entity subject to the jurisdiction of the United States. This may be a judicial proceeding (e.g. a lawsuit in which the record will be submitted), a matter before an administrative agency (e.g. a matter before a federal or state regulatory board), or a matter that is before another governmental or non-governmental entity (e.g. a record that will be submitted to a corporate entity). In any case, the court, agency, or other entity must be located in the territorial jurisdiction of the United States, although the location of the court, agency, or other entity need not be in the same state in which the notary public is performing the notarial act.

(ii) The record may involve property located in the territorial jurisdiction of the United States, or it may involve a transaction that is substantially connected with the United States. The property described in the first clause may be either real or personal property. It need not be located in the same state in which the notary public is performing the notarial act. Thus, for example, the matter may involve an acknowledgement on a deed that is transferring real property located anywhere in the United States, or it may involve an affidavit filed with regard to a transfer of a decedent's personal property located anywhere in the United States.

Subsection (c)(4)(B) provides that the act of making the statement or signing the record must not be prohibited by the foreign country in which the remotely located individual is located. Under this Section the notarial act is performed in the state in which the notary public is located at the time of the performance of the notarial act. If the act is performed on behalf of an individual located in a foreign country, that nation nevertheless might seek to impose a penalty

on the remotely located individual, the notary public, or both for performing the notarial act. Thus, this subsection states that, in order for the notarial act to be permitted under this Section, the act of making the statement or signing the record must not be prohibited in the foreign country in which the remotely located individual is situated.

It is hoped that the United States Department of State will be able to provide a listing of foreign countries that would seek to impose a penalty in the case of a remote notarization. If provided, that listing should be consulted by the notary public and the individual located outside the United States before attempting to perform the notarial act.

This subsection is not intended to impose a requirement upon a notary public to translate, understand, or interpret the laws of foreign countries. Instead, it is intended to respect the sovereignty of other nations and to alert international users of remote notarial services that they may be exposed to sanctions under the laws of other countries.

Subsection (d): This subsection provides that the certificate of notarial act must, in addition to the requirements imposed by Section 15, indicate that the notarial act was performed by communication technology. This notation on the certificate is, in effect, a notice to interested parties that the notarial act was performed for a remotely located individual by means of communication technology.

Subsection (e): This subsection states that a short-form certificate set out in Section 16 is sufficient to comply with subsection (d) in either of the following:

- (i) The certificate complies with any requirements adopted under subsection (h)(1) by the commissioning officer or agency, or
- (ii) The certificate is in the form of a certificate set out in Section 16 and contains an additional statement providing substantially as follows: "This notarial act involved the use of communication technology."

Subsection (f): This subsection requires that a notary public; a guardian, conservator, or agent of the notary public; or a personal representative of a deceased notary public must retain the audio-visual recording created under subsection (c)(3). Alternatively, the recording may be retained by a repository on behalf of a person required to retain the recording. The suggested period for retention of the recording is ten years, although this may be varied by the legislature at the time of enactment. Furthermore, the commissioning officer or agency may require a different period by rule pursuant to its powers under subsection (h)(4) and may vary retention period for different types of documents.

Subsection (g): Prior to performing his or her first notarial act under this Section, a notary public must notify the commissioning officer or agency that the notary public will be performing notarial acts for remotely located individuals by means of communication technology. The notary public must identify all of the technologies that she or he will be using to provide the notarial service. In this regard, the term "technologies" is broader than merely communication technology. It includes not only communication technology but also, for example, any technology used to perform identity proofing.

The commissioning officer or agency may have established standards for the approval of communication technology under subsection (h)(2) and Section 27. If so, the communication technology must conform to those standards. If the communication technology does so conform, the commissioning officer or agency will then approve the technology. If the commissioning officer or agency has not established standards, the notification provided to the commissioning officer or agency containing the required information suffices to comply with this subsection.

Subsection (h): This subsection authorizes the commissioning officer or agency to adopt rules regarding the performance of a notarial act by communication technology for a remotely located individual. Adopting such rules will be of particular importance since the provisions of this Section are a significant revision of prior notarial practice.

Specifically listed in the subsection is the authority to adopt rules regarding: (1) the means of performing a notarial act involving a remotely located individual using communication technology; (2) standards for communication technology and identity proofing; (3) requirements or procedures to approve providers of communication technology and the process of identity proofing; and (4) standards and the period for the retention of an audio-visual recording created 40 under subsection (c)(3).

Further authority for the adoption of rules regarding the performance of a notarial act for a remotely located individual are provided in Section 27.

Subsection (i): This subsection directs that the commissioning officer or agency must consider certain factors before adopting, amending, or repealing a rule governing the performance of a notarial act with respect to a remotely located individual. Specifically listed are: (1) the most recent standards regarding the performance of a notarial act with respect to a remotely located individual promulgated by national standard-setting organization and particularly by the National Association of Secretaries of State; (2) standards, practices, and customs of other jurisdictions that have laws substantially similar to this Section; and (3) the views of governmental officials and entities and other interested persons.

Subsection (j): This subsection provides that a supplier of communication or identity proofing technology or a provider of storage for the audio-visual recording appoints the commissioning officer or agency as the supplier's or provider's agent for service of process in a civil action relating to the notarial act. Since the subsection only applies to civil actions "in this state related to the notarial act," only claims arising out of notarial acts performed in the state are subject to its provisions.

RULONA 2018

SECTION 20. NOTIFICATION REGARDING PERFORMANCE OF NOTARIAL ACT ON ELECTRONIC RECORD; SELECTION OF TECHNOLOGY; ACCEPTANCE OF TANGIBLE COPY OF ELECTRONIC RECORD.

(a) A notary public may select one or more tamper-evident technologies to perform notarial acts with respect to electronic records. A person may not require a notary public to perform a notarial act with respect to an electronic record with a technology that the notary public has not selected.

(b) Before a notary public performs the notary public's initial notarial act with respect to an electronic record, a notary public shall notify the [commissioning officer or agency] that the notary public will be performing notarial acts with respect to electronic records and identify the technology the notary public intends to use. If the [commissioning officer or agency] has established standards for approval of technology pursuant to Section 27, the technology must conform to the standards. If the technology conforms to the standards, the [commissioning officer or agency] shall approve the use of the technology.

(c) A [recorder] may accept for recording a tangible copy of an electronic record containing a notarial certificate as satisfying any requirement that a record accepted for recording be an original, if the notarial officer executing the notarial certificate certifies that the tangible copy is an accurate copy of the electronic record.

Comment

Subsection (a) provides that a notary public may elect to perform notarial acts with respect to electronic records and, for the purpose of performing those notarial acts, may select one or more technologies. This allows a notary to use more than one technology in order to accommodate clients using different technologies to perform their electronic transactions. However, a notary public may determine whether to use a technology requested by a client and may refuse to do so.

Any technology that the notary selects must be a tamper evident technology. A tamper evident technology is one that is designed to allow a person inspecting an electronic record to determine whether there has been any tampering with the integrity of a certificate of notarial act logically associated with a record or with the attachment or association of the notarial act with that electronic record.

Subsection (b) requires that, before performing the notary public's initial notarial act with respect to an electronic record, a notary public must notify the commissioning officer or agency that the notary will be performing notarial acts with respect to electronic records. When a notary provides a notification to the commissioning officer or agency, the notary must also identify the technology or technologies that the notary intends to use to perform the notarial acts.

If, at the time that a notary public provides the notification to the commissioning officer or agency, the commissioning officer or agency has established standards for the approval of technology to be used to perform notarial acts with respect to electronic records, any technology selected by the notary must conform to those standards. If the technology conforms to those standards, the commissioning officer or agency must approve it for use by the notary. In the absence of standards adopted by the commissioning officer or agency, the notary public may proceed with performing notarial acts with

respect to electronic records as long as the notary public employs tamper evident technologies as required by this section.

Subsection (c) authorizes a recorder to accept a tangible or paper copy of an electronic record that is certified by a notarial officer under subsection 4(c). This “papered-out” copy satisfies any requirement that a record must be an original in order to be accepted for recording.

RULONA 2018

SECTION 4. AUTHORITY TO PERFORM NOTARIAL ACT.

(a) A notarial officer may perform a notarial act authorized by this [act] or by law of this state other than this [act].

(b) A notarial officer may not perform a notarial act with respect to a record to which the officer or the officer's spouse [or civil partner] is a party or in which either of them has a direct beneficial interest. A notarial act performed in violation of this subsection is voidable.

(c) A notarial officer may certify that a tangible copy of an electronic record is an accurate copy of the electronic record.

Comment

Subsection (a) is the enabling provision of this Act and grants a notarial officer the authority to perform notarial acts. It authorizes a notarial officer to perform notarial acts that are authorized by this Act as well as those authorized by other law of this State.

When taken in conjunction with the definition of a notarial act in Section 2(5), subsection (a) also authorizes a notarial officer to perform notarial acts regardless of the format of the record. Thus, a notarial officer may perform notarial acts on tangible records as well as electronic records. However, before a notary public may begin to perform notarial acts on electronic records, the notary must notify the commissioning officer or agency that the notary will be performing notarial acts with respect to electronic records (see Section 20(b)).

Subsection (b) prohibits a notarial officer from performing a notarial act in a circumstance in which performance of that act might create a conflict of interest. It provides that a notarial officer may not perform a notarial act with respect to any record in which the officer or the officer's spouse (or civil partner, as defined by state law) is a party. The prohibition is absolute and clear; there is no need to demonstrate a direct beneficial interest even though the interest may be obvious. For example, a notarial officer may not take an acknowledgment of a deed in which the officer or the officer's spouse is a grantor or grantee.

In addition, subsection (b) provides that a notarial officer may not perform a notarial act with respect to any record in which the officer or the officer's spouse (or civil partner) has a direct beneficial interest. This prohibition depends on whether there is a direct beneficial interest derived from the record (see, e.g. *Galloway v. Cinello*, 188 W. Va. 266, 423 S.E.2d 875 (1992)). For example, a deed by a third party (perhaps a grandparent) creating a trust in which a child of the notarial officer is a beneficiary might involve a direct beneficial interest to the notarial officer that is derived from the trust document (record), especially if the trust relieves support obligations of the officer. If it does provide a direct beneficial interest derived from the record, the officer would be prohibited from taking the acknowledgment of the deed of trust. While further information would be necessary to determine whether there is a direct beneficial interest derived from the record, a notarial officer should avoid performing a notarial act in any situation when doing so would raise the appearance of an impropriety.

This prohibition does not, however, extend to situations in which the beneficial interest is indirect and not the result of the operation of the record or transaction itself. For example, if the interest received is merely the payment of a notarial fee, the benefit is indirect and derived from the performance of notarial duties and not the result of the operation of the record or transaction itself (see, e.g. *Hass v. Neth*, 265 Neb. 321, 657 N.W.2d 11 (2003)). Similarly, a notary public who is hired by an employer to be available to perform notarial acts on multiple transactions does not derive a beneficial interest as a result of the operation of the records or transactions themselves. For example, a notary public may be an employee and the expenses of obtaining and maintaining the commission may be paid by the notary's employer. The obvious purpose of such an arrangement, at least in part, is that the notary public will perform notarial acts in appropriate situations as needed and requested by the employer. The fact that the notary public's salary and expenses are paid by the employer does not prevent the notary public from performing notarial acts when requested by the employer. Even though the notary receives a salary and the notary's salary may even depend on the fact that the notary performs notarial acts for the employer generally, the notary does not have a direct beneficial interest in the transactions or one that is derived from the operation of the records or transactions.

Likewise, if a notarial officer is an attorney, the attorney/notarial officer may perform notarial acts for a client as long as the attorney does not receive a direct beneficial interest as a result of operation of the record or transaction with regard to which the notarial act is performed. The fact that the attorney receives a fee for performing legal services, presently or in the future, is not a direct beneficial interest resulting from the operation of the record or transaction. Thus, receiving a fee for drafting a will or for subsequently representing the estate are fees for legal services and not a direct beneficial interest received as a result of the operation of the will (record) itself.

If a notarial officer should perform a notarial act in violation of subsection (b), the notarial act is not void per se. It may, however, be voidable in an action brought by a party who is adversely affected by the officer's misdeed. See *Galloway v. Cinello*, 188 W. Va. 266, 423 S.E.2d 875 (1992), where the court stated that the document was not void per se but was voidable; in making a determination the court should consider whether an improper benefit was obtained by the notary or any party to the instrument, as well as whether any harm flowed from the transaction. But see *Estate of McKusick*, 629 A.2d 41 (Me. 1993) in which the court questioned the validity of a will because the affidavit of a witness was made before a notary public who was the spouse of the witness.

Subsection (c) allows a notarial officer to certify that a tangible or paper copy of an electronic record is an accurate copy of the electronic record. The notarial officer providing the certification may be the same notarial officer who performed the notarial act regarding the electronic record or different notarial officer who has the ability to read the electronic record and compare it with the tangible or paper copy.



MISMO Remote Online Notarization Standards

FINAL Candidate Recommendation (CR) Version

Version 1

August 28, 2019

©2019 The Mortgage Industry Standards Maintenance Organization. All rights reserved

NOTE: *The above copyright notice must be included in all copies of this MISMO Product and in any derivative works based on this MISMO Product that are produced by Distributor.*

AUTHORIZED COMMERCIAL USAGE: This MISMO Product (as defined in [MISMO's 2018 Intellectual Property Rights Policy](#)) is subject to a commercial [MISMO Product Distributor License](#) (the "Distributor License") and grants the licensee the right to use this Product in Commercial transactions in accordance with the terms of that license. Accordingly, the licensee may incorporate this Product, in whole or in part, into material that may be shared outside of the licensee and made available for sale.

REQUIRED LEGAL NOTICES: Per Section 8 of the Distributor License, there are Legal Notices that must be included in all copies of this MISMO Product and in any derivative works based on this MISMO Product including any software applications developed by Distributor based upon this Product. For details, see [Distributor Required Legal Notices](#).

MISMO PRODUCT USER REGISTRY: Per Section 8 of the Distributor License, by downloading and using this MISMO Product, each Distributor agrees that, when providing any product or service to its customers or associated businesses that incorporates or utilizes the Product in anyway, the Distributor will use commercially reasonable efforts to encourage recipients of such products to register with MISMO as a [MISMO Product User](#).

DISCLAIMERS. Attention is drawn to the possibility that some of the elements of this MISMO Product may be the subject of patent rights. MISMO will not be held responsible for identifying any or all such patent rights. This MISMO Product is subject to the [MISMO Product Distributor License Disclaimer](#) and is provided "as is" with no warranties of any kind

Standards for Remote Online Notarization

Summary

This document outlines technical and procedural guidance and establishes underlying principles that should be considered as organizations move towards implementation of Remote Online Notarization.

The intended audience includes but is not limited to: state regulators, commissioning or licensing officials; financial institutions; service providers; technology providers; title insurance underwriters; trade associations; mortgage and title/settlement service providers.

It is worth noting that these are the minimum set of technical and procedural standards and parties are free to implement additional requirements, practices or processes for the items addressed by these standards¹. While not specifically addressed in these standards, remote online notarization system implementations should accommodate ADA (Americans with Disabilities Act) computer user interface standards and/or best practices as required by state and/or federal law².

Capitalized terms not defined in the text are defined in Section 7, entitled “DEFINITIONS”.

1. CREDENTIAL ANALYSIS AND AUTHENTICATION

The following authentication and analysis protocols are intended to support the notary public (Notary) in making the determination that satisfactory evidence of each Principal’s identity has been established for a Remote Online Notarization. This section specifies standards for States to reference when identity proofing involving Knowledge-Based Authentication (KBA) and/or credential analysis is required to perform Remote Online Notarization³. If a State specifies additional or alternative means for identity verification aside from identity proofing or credential analysis (such as by oath or affirmation of a credible witness, by a Notary’s personal knowledge of the Principal, or by other methods), such additional or alternative means are not addressed by these standards.

- a. Principal identity verification for Remote Online Notarization services must include consistent Multi-Factor Authentication procedures:
 - i. Each Principal’s identity credential must be verified against trusted third-party data sources;

¹ Mortgage lenders, insurance underwriters or other parties may impose more restrictive or additional standards based on jurisdiction, transaction type, financial implications or other factors.

² ADA requirements are a separate and distinct body of work and are not addressed by these standards.

³ As of the time of this writing, KBA, and credential analysis procedures and technology are widely accepted as identity proofing processes and are therefore specifically addressed, however, MISMO supports efforts to explore and permit other types of analysis and authentication.

- i. Each Principal's identity must be bound to each individual Principal following successful Knowledge-Based Authentication, or another form of authentication or trusted third-party identity verification such as online banking authentication; and
 - ii. Procedures must provide for human visual comparison between the Principal's identity credential presented to the Notary and the Principal himself or herself.
- b. Credential Analysis of Government Issued Identification**
- Remote Online Notarization service providers must use automated software processes to aid the Notary with their role in verifying each Principal's identity.
- i. The credential must pass an authenticity test, consistent with sound commercial practices that:
 - 1. Use appropriate technologies to confirm the integrity of visual, physical or cryptographic security features;
 - 2. Use appropriate technologies to confirm that the credential is not fraudulent or inappropriately modified;
 - 3. Use information held or published by the issuing source or authoritative source(s), as available, to confirm the validity of credential details; and
 - 4. Provide the output of the authenticity test to the Notary.⁴
 - ii. The credential analysis procedure must enable the Notary to visually compare both of the following for consistency:
 - 1. The information and photo on the presented credential image; and
 - 2. The Principal as viewed by the Notary in real time through the audio/video system.
 - iii. Credential Type Requirements
 - 1. Must be a government-issued document meeting the requirements of the State that contains a photograph of the individual, may be imaged, photographed and video recorded under applicable state and federal law⁵, and can be subjected to credential analysis.
 - iv. Credential Image Capture
 - 1. The credential image capture procedure must confirm that:
 - a. The Principal is in possession of the credential at the time of the Notarial Act;
 - b. Credential images submitted for credential analysis have not been manipulated; and
 - c. Credential images match the credential in the Principal's possession.

⁴ The output may simply indicate a "pass" or "fail" type score, or may provide more information to indicate the outcome of the authenticity test to the Notary.

⁵ State or federal law may prohibit the capture of certain credential images.

2. The following general principles should be considered in the context of image resolution:
 - a. Captured image resolution should be sufficient enough for the service provider to perform credential analysis per the requirements above.
 - b. Image resolution should be sufficient to enable visual inspection by the Notary, including legible text and clarity of photographs, barcodes, and other credential features.
 - c. All images necessary to perform visual inspection and credential analysis must be captured—e.g. U.S. Passport requires identity page; state driver’s licenses require front and back.
- c. **Dynamic Knowledge-Based Authentication**
 Dynamic Knowledge-Based Authentication (KBA) is an identity assessment that is based on a set of questions formulated from public or private data sources. A Dynamic Knowledge-Based Authentication procedure must meet the following requirements:
 - i. Each Principal must answer questions and achieve a passing score.
 1. MISMO Recommends:
 - a. Five questions, drawn from public or private data sources.
 - b. A minimum of five possible answer choices per question.
 - c. At least four of the five questions answered correctly (a passing score of 80%).
 - d. All five questions answered within two minutes.
 - ii. Each Principal to be provided a reasonable number of attempts per Signing Session.
 1. MISMO Recommends:
 - a. If a Principal fails their first quiz, they may attempt up to two additional quizzes within 48 hours from the first failure⁶.
 - b. During any quiz retake, a minimum of 40% (two) of the prior questions must be replaced⁷.
 - iii. The Remote Online Notarization system provider must not include the KBA procedure as part of the video recording or as part of the system provided person-to-person video interaction between the Notary and the Signatory, and must not store the data or information presented in the KBA questions and answers.

⁶ The standard of three total attempts within 48 hours accommodates a security provision (a maximum number of attempts per Signing Session) and a business provision (a reasonable time frame for such attempts) for a wide range of notarial scenarios. These standards also accommodate known technical limitations imposed by KBA service providers.

⁷ The purpose of replacing questions in subsequent KBA quizzes is to reduce the statistical probability of an individual guessing correct answers.

However, the output of the KBA assessment procedure must be provided to the Notary.⁸

d. **Biometrics and Other Requirements**

Biometricsensing technologies have potential application to Remote Online Notarization in the areas of authentication, credential analysis, and identity verification. These technologies include but are not limited to: facial, voice, and fingerprint recognition.⁹

e. **Workflow Continuity Requirement**

If a Principal must exit the workflow, they must meet the criteria outlined in this section and restart the Credential Analysis and Authentication workflow from the beginning.¹⁰

2. AUDIO/VIDEO QUALITY

- a. A reliable Remote Online Notarization operating model should consist of continuous, synchronous audio and video feeds with good clarity such that all participants can be clearly seen and understood at all times.
- b. Inherent in online audio/video technology is the presence of temporary surges or spikes in quantitative measures like bitrate and/or frequency of communications and no simple technical limits are practical or prudent. Rather, a sounder approach to ensuring reliable real-time communications is to rely on the judgement of the Notary to determine the adequacy of the communications and provide direction to terminate the session if those conditions are not met¹¹.
- c. The audio/video recording must include the person-to-person interaction required as part of the Notarial Act as defined by the State¹², must be logically associated to the electronic Audit Trail¹³, and must be capable of being viewed and heard using broadly available audio/video players.
- d. The video recording of the transaction documents executed in the Remote Online Notarization process is not required as part of these standards.¹⁴

⁸ The output may simply indicate a “pass” or “fail” type score, and/or may provide more information to indicate the outcome of the KBA assessment to the Notary.

⁹ MISMO does not offer specific guidance in applying this type of authentication protocol due to the lack of available industry standards regarding biometric technology.

¹⁰ Principals may have to exit the workflow for various valid or invalid reasons and may do so for an unpredictable amount of time. Therefore, to simplify these standards and provide unambiguous guidance, MISMO requires a new Remote Online Notarization workflow be started each time a Principal exits the workflow.

¹¹ Uniform standards that take into account all potential audio/video disruptions and whether they affect the integrity of the Notarial Act are not practical, and therefore, these standards provide for human judgement to determine adequate audio/video quality.

¹² The specific activities required in the Notarial Act may vary by state and therefore are not defined here.

¹³ One must be able to match the application of eSignatures, and other trackable events recorded in the Audit Trail, to the people and actions in the audio/video recording.

¹⁴ Many documents that may be notarized in this manner may contain non-public personal information (NPI) as defined under applicable law. Therefore, MISMO does not require video capture of documents or credentials as part

3. STORAGE OF NOTARIAL RECORDS

- a. Where applicable, and in accordance with State laws, rules and regulations, the Notary must maintain accurate and reliable Notarial Records. These State laws, rules and regulations may or may not require that a copy of the audio/video recording be part of a notarial journal (which may be subject to public access under State law)¹⁵. Notaries must have the ability to electronically capture the required Notarial Records or to direct a third party to do so on their behalf. In either case, the Remote Online Notarization system must:
 - i. Facilitate the process of collecting the required Notarial Records;
 - ii. Provide a method by which a Notary can access and/or export the Notarial Records; and
 - iii. Provide automated backup of the Notarial Records and audio/video recording to ensure redundancy.
- b. The Remote Online Notarization technology solution must employ data protection safeguards consistent with generally accepted information security standards.
- c. Retention of the audio/video recording and Notarial Records by either the Notary public or their designated third party, as directed by the Notary, must adhere to the laws, directives, rules and regulations of the State.

4. POST-EXECUTION RECORDS

- a. Significant actions completed as part of a Remote Online Notarization Signing Session should be recorded in an Audit Trail. Each entry in this Audit Trail should clearly indicate the action performed (e.g. addition of an electronic signature), the date/time of its performance (e.g. Coordinated Universal Time, 2018-08-21 01:14:22 UTC), the name of the party performing the action (e.g. John Doe) and the IP address of the party performing the action. Further detailed guidance on the contents of the Audit Trail or its form is beyond the scope of these standards.
- b. Each document completed as part of a Remote Online Notarization should be electronically signed and rendered Tamper-Evident.

5. SECURITY CONSIDERATIONS

Remote Online Notarization technology providers must have comprehensive security programs in place to ensure privacy and data security. Technology providers should be vigilant to ensure consumer data, privacy and information security laws and regulations are satisfied through their information security programs. There are many industry accepted models, standards and frameworks for how to develop such programs.

of these standards. Including the documents and/or credentials in the video recording may be considered as a matter of policy on a state-by-state basis.

¹⁵ Treatment of the audio/video recording in the context of the Notarial Record or journal is a matter of public policy and not addressed in these standards.

6. COUNTY RECORDING CONSIDERATIONS FOR ELECTRONICALLY NOTARIZED DOCUMENTS

- a. The Remote Online Notarization system, process, and procedures must be capable of generating a printable version of all documents executed in the system, including but not limited to the documents executed in the Notarial Act, and associated certifications as required by the State, county and/or other governing or regulatory body.¹⁶
- b. Any document notarized remotely online must clearly state, in the remote online notarial certificate, that the person making the acknowledgment, oath or affirmation and signing the document appeared remotely online using audio/video communication technology.

7. DEFINITIONS

- a. **“Audit Trail”** means a chronological and detailed list of critical events and actions, from the beginning to the end of the Remote Online Notarization process, including the dates and times the events and actions took place and identification of the individuals and/or systems that performed the events or actions. Also known as: Audit Log or Event Log.
- b. **“Knowledge-Based Authentication” or “KBA”** means an identity verification method based on knowledge of private information associated with the claimed identity of a person.¹⁷
- c. **“Multi-Factor Authentication” or “MFA”** means a method of access control in which a user is granted access after successfully presenting identity evidence through a minimum of two of the following mechanisms: something they *have* (e.g. an ID credential), something they *know* (e.g. KBA), something they *are* (e.g. iris, retinal, thumbprint scans, facial recognition and other forms of biometric identification).
- d. **“Notarial Act”** means an act, whether performed with respect to a tangible or electronic record, that a notarial officer may perform under the law of a specific State. The term includes taking an acknowledgment, administering an oath or affirmation, taking a verification on oath or affirmation, witnessing or attesting a signature, certifying or attesting a copy, and noting a protest of a negotiable instrument.¹⁸
- e. **“Notarial Records”** means details of the Notarial Act common to the State’s notarial journal or register requirements.

¹⁶ While outside the scope of these standards, the concept of “papering out” and printing eNotarized documents for use in a paper county recording process may be permissible under the law of some states. These standards require electronically created documents be printable for this purpose.

¹⁷ DIGITAL IDENTITY GUIDELINES NIST SP 800-63-3 (page 46 for definition of KBV a.k.a. KBA)

¹⁸ Mortgage Bankers Association – American Land Title Association Model Legislation for Remote Online Notarization Sec.1 Definitions (9) “Notarial Act” page 3

- f. **“Principal”** means an individual whose electronic signature is notarized in a remote online notarization; or making an oath or affirmation or an acknowledgment other than in the capacity of a witness for the remote online notarization.¹⁹
- g. **“Record”** means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.²⁰
- h. **“Remote Online Notarization”** means a Notarial Act performed by means of an electronic device or process that allows a notary public and a Principal, who is not in the same physical location as the notary public, to complete a Notarial Act and communicate with each other simultaneously by sight and sound.²¹
- i. **“Signing Session”** means one or more Notarial Acts performed on a single set of documents as a single event by a single Notary with one or more Principals and any applicable witnesses.
- j. **“State”** means the state or jurisdiction under which the notary public is commissioned and for which the notary public is performing the Remote Online Notarization.²²
- k. **“Tamper-Evident”** A technology based process that indicates whether a change has been made to the record since the technology was applied.

¹⁹ Mortgage Bankers Association – American Land Title Association Model Legislation for Remote Online Notarization Sec.1 Definitions (11) “Notarial Act” page 3

²⁰ RULONA Section 2. Definition for Record (Page 5)

²¹ Adapted from the Mortgage Bankers Association – American Land Title Association Model Legislation for Remote Online Notarization Sec.1 Definitions (13) “Remote online notarization” page 4 and “(2) “Communication technology” page 1.

²² This state definition provides clarity for which jurisdiction rules, requirements or regulations must be referenced when there is more than one state related to a Notarial Act: (1) the state where the Principal is located, (2) the state where a property related to the Notarial Act is located, (3) the state in which the Notary is located, or (4) other state references.



NASS Support for the Revised National Electronic Notarization Standards

Adopted on July 12, 2006;
Reaffirmed on July 13, 2011 and July 17, 2016;
Amended and readopted on February 19, 2018

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 in-person electronic notarization, and amended to include remote 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 developed the original in-person, electronic notarization standards. These standards were presented NASS members for consideration at our 2006 Summer Conference. The members voted unanimously to adopt the standards, and voted to reaffirm the standards at the NASS 2011 Summer Conference. At our 2016 Conference, the in-person, e-notarization Standards were again reaffirmed, however this version included several amendments proposed by the NASS Notary Public Administrators Section (NPA) designed to streamline and clarify the standards.

In April 2016, NASS formed the Remote Electronic Notarization Task Force to examine the topic of remote electronic notarization. The Task Force consisted of NASS members, members of NPA, various industry/government stakeholders and private sector advisors. At the Summer 2017 Conference, NASS adopted a resolution authorizing the convening of appropriate parties to develop remote notarization standards enabling remote notarizations that will protect the credibility of the process, help prevent identity fraud and provide accountability to the public in order to advance secure electronic commerce. Through a series of in-person meetings and conference calls the Task Force developed an addendum to the in-person electronic notarization standards to accommodate remote electronic notarization. These changes were adopted by the NASS membership at the Winter 2018 Conference.

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. “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.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. “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 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

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.

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 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 another individual—for example, judges, clerks, etc.—authorized to perform a notarial act. These Standards contemplate only notaries public.

11. "Personal 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 credentials to each other, or;
- interact through the use of audio- video communication as defined in addendum.

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

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.

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

Standards

Personal 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 where the signer is in the physical presence of the notary shall be the same as the methods required for a paper-based notarization.⁸

Registration Requirement

3. The commissioning official shall require a notary public to 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. 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

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.

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.

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 does not appear personally before notary public.

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

Form and Manner of Performing the Electronic Notarial Act

5. 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.

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.

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.

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.

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.

Security Requirements

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

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

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.

Requirements for Authenticating the Notarial Act

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)

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

13. Electronic 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

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 Legalization 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 Legalization for Foreign Public Documents.

Addendum: Audio-Video Communication

In this Addendum, the terms in Standards 1-15 (Definitions) have the meanings ascribed. In addition:

1. "Audio-video communication" means being able to see, hear, and communicate with another individual in real time using electronic means.
2. "Credential analysis" means a process or service operating according to criteria allowed by the commissioning authority through which a third person or party affirms the validity of a government-issued identification credential through review of public or proprietary data sources.
3. "Dynamic knowledge-based authentication assessment" means an identity assessment that is based on a set of questions formulated from public or proprietary data sources for which the principal has not provided a prior answer.
4. "Identity proofing" means a process or service operating according to criteria approved by the commissioning official through which a third person or party affirms the identity of an individual through review of personal information from public or proprietary data sources.
5. "Public key certificate" means an electronic credential which is used to identify an individual who signed an electronic record with the certificate.
6. "Real time" means the actual span of uninterrupted, simultaneous communication during which all parts of an electronic notarial act occur.
7. "Remote electronic notarization system" means a set of applications, programs, hardware, software, or technology designed to enable an electronic notary to perform electronic notarial acts through audio- video communication.
8. "Remotely presented" means the transmission of a quality image of a government-issued identification credential to an electronic notary public through communication technology for the purpose of enabling the electronic notary public to identify the person appearing before the electronic notary public and to perform a credential analysis.

Authority to Perform Electronic Notarizations Using Audio-Video Communication

A notary public may perform an electronic notarial act for an electronic document by means of audio- video communication for a principal who is located:

- in the state where the notary is commissioned;
- outside of the state where the notary is commissioned but within the United States; or
- outside the United States if:
 - the act is not prohibited in the jurisdiction in which the principal is physically located at the time of the act.

A notary public who performs an electronic notarial act for a principal by means of audio-video communication shall be located within the state where the notary is commissioned at the time the electronic notarial act is performed. The notary public shall include a statement in the electronic

notarial certificate to indicate that the electronic notarial act was performed by means of audio-video communication. The statement may also be included in the electronic notary seal.

Requirements for Remote Electronic Notarization Systems

A remote electronic notarization system used to perform electronic notarial acts by means of audio-video communication shall:

- provide sufficient audio clarity and video resolution to enable the notary and the principal to see and speak to each other simultaneously through live, real time transmission; and
- include a means of authentication that reasonably ensures only the proper parties have access to the audio-video communication; and
- provide some manner of ensuring that the electronic record that is presented for electronic notarization is the same record electronically signed by the principal; and
- enable the notary public to verify the identity of the principal through multiple identity verification methods, which may include: completion of a dynamic knowledge-based authentication assessment; credential analysis of a remotely presented government-issued identification that contains the signature and a photograph of the principal; a valid public key certificate; or any other identity proofing method adopted by the commissioning official; and
- be capable of creating, storing, and accessing an electronic recording of the audio-video communication; and
- provide reasonable security measures to prevent unauthorized access to: the live transmission of the audio-video communication; a recording of the audio-video communication; the verification methods and credentials used to verify the identity of the principal; and the electronic documents presented for electronic notarization.

Adopted the 19th day of February 2018
in Washington, DC

EXPIRES: Winter 2023