



NASS SUPPORT FOR THE REVISED NATIONAL ELECTRONIC NOTARIZATION STANDARDS AND REMOTE ONLINE NOTARIZATION STANDARDS

Adopted July 12th, 2006;
Reauthorized July 2011 and July 2016;
Amended and readopted February 2018;
Amended and reauthorized July 2023

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 to 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, electronic notarization Standards were again reaffirmed. Included were amendments proposed by the NASS Notary Public Administrators (NPA) Section 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 facilitate adoption of remote notarization and advance secure electronic commerce through development of standards to protect the credibility of remote notarizations, help prevent identity fraud and provide accountability to the public. Through a series of in-person meetings and conference calls the Task Force developed a remote electronic notarization Addendum to the in-person electronic notarization Standards. These changes were adopted by the NASS membership at the Winter 2018 Conference.

In 2022, the NPA Section convened a working group to review the Revised National Electronic Notarization Standards, including the remote notarization Addendum, prior to the Standards' scheduled

2023 expiration. The NPA Section's recommendations are presented herein (underlined text indicates new or revised text).

The 2022 NPA working group's recommendations contemplate models of technology-assisted notarization currently authorized in various state laws:

1. Electronic notarization -- performed for a physically present individual executing an electronic record. The individual is personally known to the notary, presents government-issued ID credentials or, where authorized, produces a credible witness or witnesses to verify the individual's identity.
2. Remote online notarization (RON)—performed as specified by state law for a remotely located individual executing an electronic record. The individual appears by means of real-time audio-visual communication technology and is personally known to the notary, identified by means of a credible witness, or identified by state-authorized, multi-factor identity verification methods.

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. "Authorization" means a separate commission to perform electronic or remote notarial acts under the laws of this State; or a registration or notification of intent, filed with the commissioning/appointing official, to perform electronic or remote notarial acts in compliance with these standards. The term "authorized" indicates such authorization.¹
2. "Capable of independent verification" means that any interested person may confirm, through the commissioning/appointing official or official custodian of state notary public commission or appointment records, that a notary public² who signed an electronic record is that person and had the authority at that time to perform electronic notarial acts.
3. "Electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.
4. "Electronic record" means information that is created, generated, sent, communicated, received, or stored by electronic means.
5. "Electronic notarial act" means an official act by a notary public on or involving an electronic record and using electronic means authorized by the [commissioning/appointing official] or the laws of the jurisdiction of appointment. The term includes "electronic notarization."

¹ This new Definition accommodates states' varying administrative requirements for a notary public to actually begin performing electronic or remote notarial acts. The terms "authorization" and "authorized" indicate an individual permitted to perform electronic or remote notarial acts under the law of the commissioning state, whether the individual was required to "register," "notify," be separately "commissioned," etc.

² These Standards refer to "notary public" and "notaries public," but they may be construed to contemplate other notarial officers performing electronic and remote notarizations.

6. “Electronic notarial certificate” means the portion of a notarized electronic record that is completed by the notary public, bears the notary public's electronic signature and/or official electronic seal, official title, commission number if applicable, commission expiration date if applicable, any required information concerning the date and place of the electronic notarization, and such other information required by state law including the method of performing the notarial act, and states the facts attested to or certified by the notary public in a particular electronic notarization.³
7. “Electronic notary seal” and “official electronic seal”⁴ mean information within a notarized electronic record 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 tangible records.
8. “Electronic signature” means an electronic sound, symbol, or process attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the electronic record.
9. “Law” and “laws” mean all of the following: a state’s statutes or code of laws; a state’s administrative rules or regulations; a state’s executive order, declaration, or proclamation; any directive or guidance of the state official regulating notaries public.
10. “Non-repudiation” means the inability of the signer of an electronic record to deny their electronic signature without factual basis.⁵
11. “Notary electronic signature” means those forms of electronic signature approved, specified or allowed by state law as an acceptable method for an electronic notary to affix the notary's official signature to an electronic record that is being notarized.
12. “Notary public” means an individual commissioned or appointed to perform a notarial act by the [commissioning/appointing officer or agency] of this State.⁶
13. “Notarial officer” means a notary public or other individual authorized under state law to perform a notarial act.
14. “Person” — “a person,” “any person” or “all other persons” mean an individual, corporation, business trust, statutory trust, estate, trust, partnership, limited liability company, association, joint venture, public corporation, government or governmental subdivision, agency, or instrumentality, or any other legal or commercial entity.
15. “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

³ The definitions for “electronic notarial certificate” and “electronic notary seal” refer to “commission number,” “commission expiration” and “notary seal,” though some jurisdictions do not issue commission numbers or require notary seals. Other jurisdictions issue life-long notary commissions that do not have expiration dates.

⁴ See Footnote 3.

⁵ “Non-repudiation” as defined in these Standards establishes a presumption of the integrity of electronically executed records.

⁶ The Revised Uniform Law on Notarial Acts differentiates “notary public” from “notarial officer,” which is a notary public OR other individual—for example, judges, clerks, etc.—authorized under state law to perform a notarial act.

credentials to each other, or interact through the use of communication technology as defined in “Standards—Notarial Acts Performed for a Remotely Located Individual by Means of Communication Technology.”

16. “Principal” means an individual who appears before a notarial officer for an electronic notarial act or a notarial act involving the use of communication technology as defined in “Standards—Notarial Acts Performed for a Remotely Located Principal by Means of Communication Technology.”
17. “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.
18. “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.
19. “Tamper-evident” means that any change to an electronic record displays evidence of the change.
20. “Under the notary public’s sole control” means accessible by the notary public to the exclusion of all other persons.
21. “Unique to the notary public means, with respect to an electronic notarial act, that the notary electronic signature is attributable solely to the notary public, to the exclusion of all other persons.”⁷

STANDARDS, ELECTRONIC NOTARIAL ACTS

Personal Appearance Requirement

1. A notary public shall not perform an electronic notarial act if the individual executing the electronic record does not appear before the notary public at the time of notarization.
2. The methods for identifying physically present individuals appearing for notarization of an electronic record shall at a minimum be the same as the methods required for identifying physically present individuals appearing for notarization of a tangible record.⁸

Authorization Requirement

3. The commissioning/appointing official shall require a notary public to be duly authorized prior to performing any electronic notarial act. Authorization shall be by means prescribed in law of the commissioning/appointing state, and shall be subject to update, renewal, non-renewal and termination requirements prescribed in law.
4. The commissioning/appointing official may require a notary public [filing for, requesting] authorization to perform electronic notarial acts to provide the following information: a) the electronic technology or technologies to be used in attaching or logically associating the notary’s

⁷ As defined, the term “unique to the notary public” does 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 and remote notarizations that satisfy these Standards.

⁸ Under no circumstances shall a notary public base identification merely upon familiarity with a principal’s electronic signature, or an electronic verification process that authenticates the principal’s electronic signature, when the principal does not appear personally before a notary public.

electronic signature, seal and certificate to an electronic record; b) an image of the notary's electronic signature and official electronic seal; c) any necessary instructions or techniques supplied by the vendor that allow the notary's electronic signature and official electronic seal to be read; and d) any other information specified by the commissioning/appointing official.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.
6. The notary's electronic signature and official electronic seal are deemed to be reliable if they are:
 - (a) unique to the notary public,
 - (b) capable of independent verification,
 - (c) retained under the notary public's sole control,¹⁰ and
 - (d) attached to or logically associated with the electronic record in a tamper-evident manner.
7. The notary's electronic signature in combination with the official electronic seal shall be used only for the purpose of performing electronic notarial acts.
8. A notary public's liability, and the sanctions and remedies for improperly performing electronic notarial acts, are the same as described in and provided by law for the notary's improper performance of non-electronic notarial acts.

Security Requirements

9. A notary public shall not disclose any access information used to affix the electronic notary's signature and seal except when requested by the commissioning/appointing official, law enforcement, the courts, and with reasonable precautions, electronic record preparation and transmission vendors.¹¹

Authenticating the Notarial Act; Requirements

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 record will be accomplished. The electronic signature and seal may possibly be combined in a single element; or 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 record. Although the Uniform Electronic Transactions Act (UETA), the 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 record is an "original" versus a copy, the seal requirement remains essential to authenticating records under federal and state rules of evidence. What is important is that the basic identifying and (*con't. from Page 4*) commissioning information—contained in the notary public's holographic signature and traditional inking and embossing notary seals—are also elements of a notarized electronic record.

¹⁰ Control of security aspects such as but not limited to passwords, token devices, biometrics, PINs, phrases, and software on protected hardware shall remain only under the control of the commissioned notary public.

¹¹ Control of security aspects such as but not limited to passwords, token devices, biometrics, PINs, phrases, and software on protected hardware shall remain only under the control of the commissioned/appointed notary.

10. Electronic notarial acts shall fulfill certain basic requirements to ensure non-repudiation and the capability of being authenticated by the-competent authority¹² for purposes of issuing Apostilles and Certificates of Authentication. Those requirements are: a) the fact of the notarial act, including the notary's identity, signature, and commission status, is verifiable by the competent authority and b) the notarized electronic record is rendered ineligible for authentication by the competent authority if it is improperly modified after the time of notarization, including any unauthorized alterations to the record's content, the electronic notarial certificate, the notary electronic signature, and/or the notary public 's or notarial officer's official electronic seal.¹³

Issuance of Electronic Apostilles and Certificates of Authentication, Requirements

11. Electronic Apostilles must fulfill certain basic requirements to ensure non-repudiation: a) the fact of the issuance of the Apostille by the competent authority must be independently verifiable and b) the underlying record must not be improperly modified as when, for example, a person attempts to remove the Apostille from the public document.¹⁴
12. Electronic Certificates of Authentication (or Appointment) must fulfill certain basic requirements to ensure non-repudiation: a) the fact of the issuance of the Certificate by the competent authority must be independently verifiable and b) the underlying record must not be improperly modified as when, for example, a person attempts to remove the Certificate from the public document.

STANDARDS: NOTARIAL ACTS PERFORMED FOR A REMOTELY LOCATED INDIVIDUAL BY MEANS OF COMMUNICATION TECHNOLOGY

The preceding Definitions 1-21 have the meanings provided therein. In addition:

1. "Communication technology" means an electronic device or process that: (a) allows a notary public¹⁵ 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.

¹² "Competent authority": An authority designated by a Contracting Party under Article 6 of the Apostille Convention to issue Apostilles (see <https://www.hcch.net/en/instruments/specialised-sections/apostille>). A Contracting Party may determine how many Competent Authorities are designated and the extent of their competence (e.g., issuing Apostilles only for certain types of public document). Information about Competent Authorities designated by Contracting Parties is available on the Apostille Section of the HCCH website.

¹³ "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 record which has been executed or issued in one jurisdiction to be recognized in another jurisdiction. Records 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)]

¹⁴ The Apostille (or Certificate of Authentication) and the underlying record are legally joined. Therefore, any separation legally invalidates the Apostille (or Certificate of Authentication). To ensure a recipient the necessary degree of security and trust in deciding whether to accept, an electronic Apostille (or electronic Certificate of Authentication) 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.

¹⁵ These Standards refer to "notary public" and "notaries public," but they may be construed to contemplate other notarial officers as well, particularly in states whose law authorizes electronic and remote notarizations to be performed by notaries public and other notarial officers.

2. "Credential analysis" means a process or service operating according to criteria authorized by the commissioning/appointing official through which a third person or party affirms the validity of a government-issued identification credential through a 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 remotely located individual has not provided a prior answer.
4. "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.
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 a notary public to perform electronic notarial acts through communication technology.
8. "Remote notarial act" means a notarial act performed by a notary public for a remotely located individual, in accordance with applicable law.
9. "Remotely located individual" means an individual who is not physically present with a notary public, but appears before the notary public by means of communication technology.
10. "Remotely presented" means the transmission of an image of a government-issued identification credential that meets any rules or standards required by state law to a notary public for the purpose of enabling the notary public to identify the remotely located individual appearing before the notary public.

Authority to Perform Electronic Notarization Using Communication Technology

11. A duly authorized notary public may perform a remote notarial act for a remotely located individual who is not in the same location as the notary public but is located:
 - (a) in the state where the notary is commissioned;
 - (b) outside of the state where the notary is commissioned but within the United States; or
 - (c) outside the United States if:
 - i. the act is not prohibited in the jurisdiction in which the remotely located individual is physically located at the time of the act; and
 - ii. the record is part of or pertains to a matter that is to be filed with or is before a court, governmental entity, or other entity located in the United States or involves property located in, or a transaction substantially connected with, the United States.
10. A notary public who performs a remote notarial act shall be physically located within the state where the notary public is commissioned, appointed or authorized 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 remote notarial act was performed by means of communication technology. The statement may also be included in the official electronic seal.

Remote Electronic Notarization Systems, Requirements

11. A remote electronic notarization system used to perform remote notarial acts by means of communication technology shall:
 - (a) provide sufficient audio clarity and video resolution to enable the Notary and the remotely located individual to see and speak to each other simultaneously through live, real-time transmission; and
 - (b) include a means of authentication that reasonably ensures only the authorized parties have access to the communication technology; and
 - (c) provide some manner of ensuring that the electronic record that is presented for a remote notarial act is the same record electronically signed by the remotely located individual; and
 - (d) enable the notary public to verify the identity of the remotely located individual through multiple identity verification methods, which may include any other identity proofing method adopted by the commissioning/appointing official¹⁶; and
 - (e) be capable of securely creating, storing, accessing and reproducing a copy of an electronic recording of the remote electronic notarial act; and
 - (f) be capable of producing recordings of remote electronic notarial acts in response to a request from the notary public, commissioning/appointing official, a court, or law enforcement in the course of an investigation; and
 - (g) provide reasonable security measures to prevent unauthorized access to the: live communication between the notary public and remotely located individual; recording; verification methods and credentials used to verify the identity of the remotely located individual; and electronic records presented for a remote notarial act.

Adopted July 12th, 2023, in Washington D.C

EXPIRES: Summer 2028

¹⁶ Examples of identity verification methods are 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 remotely located individual; or a valid public key certificate.