## [Chapter 5A — Audio-Video Communication

### Comment

General: Technological advances and the growth of the Internet have created a global culture where video is omnipresent. The availability of modestly priced "web cams" has made it possible for many people to film videos on their laptop computers, tablets, or smartphones. Broadband data connections allow consumers to conduct video calls with family and friends, businesses to hold meetings involving participants located around the world, and courts to conduct hearings for criminal defendants using audio-video technology.

It is not surprising that audio-video technology has made an inroad into the daily life of the notary public. In fact, it was anticipated. "With technology now enabling 'teleconferences' between parties in different cities, or even different nations, the future will likely bring broadened statutory definitions of 'personal appearance' whereby a notary in Los Angeles might attest to a televised signature affixation by a person in London. The notary's audial interaction with the absent signer and real-time acquisition of the signer's video image would seem prerequisites for such remote electronic notarizations." (Charles N. Faerber, *Being There: The Importance of Physical Presence to the Notary*, 31 J. MARSHALL L. REV. 775 (1998).) Indeed, one state now allows its notaries public to perform electronic notarizations while physically present in another state for a principal in a jurisdiction anywhere in the world. (*See* VA. CODE ANN. § 47.1-13B.)

The MENA drafters determined that a chapter on audio-video communication was necessary in the Act in light of events that have transpired since Virginia's enactment of its remote electronic notarization law. (*See* Section 2-1 and Comment.) With the prospect of more states considering proposals to allow "video conference notarizations," the drafters were convinced that this 2017 Act must contain provisions ensuring the protection of notaries and members of the public who participate in or rely on the integrity of audio-video electronic notarizations.

The entire Chapter 5A is in brackets, reflecting the lack of consensus over this issue both in the notary public community and industries interacting with it. In future editions of the Model Electronic Notarization Act, the National Notary Association and its review panels will carefully weigh arguments for removing the brackets, based on the success of current models and future developments in audio-video technologies.

This Chapter authorizes audio-video notarizations but only for electronic notarizations. By contrast, the Revised Uniform Law on Notarial Acts and Montana statute permit signers of electronic *and* paper documents to have their signatures notarized by means of audio-video communication. (*See* REV. UNIF. LAW ON NOT. ACTS § [14A(c)]; and MONT. CODE ANN. § 1-5-603(7)(a).)

### § 5A-1 Definitions Used in This Chapter.

For the purposes of this Chapter:

(1) "Audio-video communication" means being able to see, hear, and communicate with another individual in real time using electronic means.

(2) "Dynamic knowledge-based authentication assessment" means an

identity assessment that is based on a set of questions formulated from public or private data sources for which the principal has not provided a prior answer.

(3) "Person" means 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.

(4) "Public key certificate" means an electronic credential which is used to identify an individual who signed an electronic record with the certificate.

(5) "Real time" means the actual span of uninterrupted time during which all parts of an electronic notarial act occur.

**Comment**

Section 5A-1 defines terms that apply to Chapter 5A. Subparagraph (1) defines "audio-video communication." The essential components of an appearance before a notary public by means of audio-video communication are the same as for a physical appearance: the notary and principal must be able to "see, hear, and communicate with" each other using either process. (*See* Section 2-1.) An essential element to the definition is that the audio-video transmission be in "real time." "Real time" is defined in Subparagraph (5).

Subparagraph (2) defines "dynamic knowledge-based authentication assessment" ("DKBA"). A DKBA is a series of challenge-response questions formulated by an identity verification provider, such as a credit reporting service. The questions are based upon an individual's life history and circumstances. The questions are highly detailed. For example, a question might ask which of five addresses listed is not the address where the individual resided in a certain year. Some assessments pose questions and require an individual to provide the answers in advance. (For example, "What is your mother's maiden name?") Unlike these "static" assessments, DKBA questions are not posed to the individual in advance, and the answers reasonably could only be known by the true individual.

Subparagraph (3) defines "person." It is the standard definition used by the Uniform Law Commission. (*See* REV. UNIF. LAW ON NOT. ACTS § 2(9).) A person may be an individual or any other entity given legal status under the law. As used in Chapter 5A, "person" refers to an identity service provider that performs a DKBA or other identity verification assessment qualifying under the definition of "satisfactory evidence of identity" for electronic notarizations performed by audio-video communication.

Subparagraph (4) defines "public key certificate." A public key certificate is a computer record issued and digitally signed by a certification authority that implements a public key infrastructure. The certificate contains a private/public key pair that is mathematically linked. The subscriber signs records with the private key using software (for example, a PDF viewer). Anyone may use the subscriber's public key to validate that the record was signed using the subscriber's private key. If specific methods are used to identify the subscriber at the time of application, a public key certificate may

provide high confidence of an individual's asserted identity, provided the subscriber does not compromise the private key. A public key certificate used as satisfactory evidence must comply with rules adopted by the commissioning official. (*See* Appendix II, Model Rule 2 and Comment).

The definition of "real time" was introduced into the Act in Subparagraph (5) to support both the bracketed audio-video communications provisions (*see* Section 2-1 and Comment), and the Model Rules implementing bracketed Section 5A-5. (*See* Appendix II.) The drafters insisted that any electronic notarization system used to facilitate the performance of an electronic notarial act must record, transmit, and preserve all interactions between the parties without interruption or editing. This would rule out any system in which a principal might pre-record a video of her- or himself requesting a notarial act and presenting identification credentials and then, hours or days later, actually appear before the notary via audio-video communication.

### § 5A-2 Audio-Video Communication Permitted.

A notary public may perform an electronic notarial act by means of audio-video communication in compliance with this Chapter and any rules adopted by the [commissioning official] for a principal who is located:

(1) in this [State];
(2) outside of this [State] but within the United States; or
(3) outside the United States if:
    (i) the act is not known by the notary public to be prohibited in the jurisdiction in which the principal 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 territorial jurisdiction of the United States, or a transaction substantially connected with the United States.

**Comment**

Section 5A-2 permits notaries public to perform electronic notarial acts for principals appearing remotely. It broadly allows a principal in any location to appear before the notary public by means of audio-video communication technology, with specific qualifications for principals located outside of the United States. The most restrictive state with a remote appearance law requires the principal to be a legal resident of the state, and for the transaction either to involve real or personal property titled in the state, be under the jurisdiction of a court in the state, or be a proxy marriage. (MONT. CODE ANN. § 1-5-615(3)(b)(iv).)

Subparagraph (3) relates to remote appearances before a notary public by individuals located outside of the United States. Two fundamental qualifications for these principals are given.

First, the notary must not know the act to be prohibited in the jurisdiction in which the principal is physically located at the time of the act. This qualification is substantively borrowed from the amendment to the Revised Uniform Law on Notarial Acts. (REV. UNIF. LAW ON NOT. ACTS § [14A(b)(4)].) The U.S. State Department has expressed concern that in some foreign jurisdictions it is a

criminal act for any individual to perform a public act while not lawfully appointed as a notary public of the foreign jurisdiction. This could subject a notary public commissioned by a U.S. state or jurisdiction and a principal living in the foreign jurisdiction to criminal penalties. The Act does not create a duty for a notary to investigate whether an electronic act performed by audio-video communication is prohibited in a foreign jurisdiction.

Second, the transaction involving the principal located outside of the United States must have a nexus to the United States. This qualification is adopted verbatim from the amendment to the Revised Uniform Law on Notarial Acts. (REV. UNIF. LAW ON NOT. ACTS § [14A(b)(2)].)

### § 5A-3 Surety Bond Required.

(a) A notary public who performs electronic notarial acts by means of audio-video communication shall obtain and maintain a surety bond in the amount of [$25,000] from a surety or insurance company licensed to do business in this [State], and this bond shall be exclusively conditioned on the faithful performance of electronic notarial acts by means of audio-video communication.

(b) [The surety bond required by this Section shall be in addition to any surety bond required to perform notarial acts under other law of this [State], but it shall be the sole means of recovery for contested electronic notarizations performed under this Chapter.]

[(c)] The surety bond shall be filed with [the [commissioning official]] OR [an agency or office designated by the [commissioning official]].

**Comment**

Subsection (a) requires a notary public who performs electronic notarizations by means of audio-video communication to obtain and maintain a surety bond exclusively conditioned on the proper performance of such acts. The drafters favor a $25,000 bond, but the exact amount is left to each enacting jurisdiction. The drafters felt that a bond was required in order to protect any member of the public who might be injured by the notary's negligence or fraud. The bond applies exclusively to electronic notarial acts performed via audio-video communication. A notary must maintain the bond throughout the entire time of registration. A notary whose bond is partially or fully exhausted in paying a claim during the registration term must obtain a new bond.

Subsection (b) is bracketed. It applies to the states and jurisdictions that currently require a notary public surety bond. It clarifies that the bond required by Subsection (a) is in addition to any bond required for the notary's underlying commission. It also clarifies that the bond for electronic notarizations involving audio-video communication would be the sole means of recovery for negligent and fraudulent acts under Chapter 5A. In other words, the provision would prevent a notary's regular surety bond from being attached pursuant to claims involving remote electronic acts. If the notary's bond conditioned for proper performance of electronic acts

involving audio-video communication were exhausted, the notary could not perform any future electronic acts involving audio-video communication, but the bond for the underlying notary public commission would not be affected.

Depending on the jurisdiction, bonds may be filed centrally or locally. In some states, the bond is approved by and filed with the commissioning official (*see* KAN. STAT. ANN. § 53-102), while in others the bond is filed with the county clerk or recorder (*see* CAL. GOV'T CODE § 82139(a)). Subsection (c) is written to accommodate either of these filing scenarios and the enacting state should tailor the provision accordingly.

**§ 5A-4 Requirements for Audio-Video Communication.**

(a) A notary public who performs an electronic notarial act for a principal by means of audio-video communication shall:
  (1) be located within this [State] at the time the electronic notarial act is performed;
  (2) execute the electronic notarial act in a single recorded session that complies with Section 5A-6 of this Chapter;
  (3) be satisfied that any electronic record that is electronically signed, acknowledged, or otherwise presented for electronic notarization by the principal is the same record electronically signed by the notary;
  (4) be satisfied that the quality of the audio-video communication is sufficient to make the determinations required for the electronic notarial act under this [Act] and any other law of this [State]; and
  (5) identify the venue for the electronic notarial act as the jurisdiction within this [State] where the notary is physically located while performing the act.

(b) In addition to the provisions of Chapter 4 of this [Act], an electronic notarization system used to perform electronic notarial acts by means of audio-video communication shall:
  (1) require the notary public, the principal, and any required witness to access the system through an authentication procedure that is reasonably secure from unauthorized access;
  (2) enable the notary public to verify the identity of the principal and any required witness by means of personal knowledge or satisfactory evidence of identity in compliance with Section 5A-5;
  (3) provide reasonable certainty that the notary public, principal, and any required witness are viewing the same electronic record and that all signatures, changes, and attachments to the electronic record are made in real time; and
  (4) be capable of creating, archiving, and protecting the audio-video recording and of providing public and official access, inspection, and copying of this recording as required by Section 5A-6(a).

**Comment**

Section 5A-4 provides requirements for remote electronic notarizations and electronic notarization systems. Subsection (a) contains provisions that parallel similar requirements for paper-based notarial acts. (*See* Subparagraphs (a)(1), (2), and (5).) Two others are unique to remote electronic notarial acts.

Subparagraph (a)(3) presents a particular challenge: How can a notary be sure that the principal and notary are viewing and signing the same electronic record? When a principal appears physically before a notary, the document changes hands and the notary can readily establish that the document requiring the notary's signature is the same document the principal signed. The record may be presented through the use of an electronic notarization system that allows the electronic record to be uploaded and managed in the system (*see* Subparagraph (b)(3) and Comment), but it could also be satisfied by the principal transmitting the electronically-signed record to the notary via email or personally acknowledging to the notary that the record under the notary's control is the same record the principal signed. (*See* REV. UNIF. LAW ON NOT. ACTS § [14A(b)(3)].)

Subparagraph (a)(4) requires the notary public to be satisfied that the quality of the audio-video transmission allows the notary to perform all facets of the electronic notarial act. If, for example, the video transmission is slow and choppy, the communication between the principal and notary may be impaired to the point where the notary must determine that the electronic notarization cannot continue.

Section 5A-4(b) deals with requirements for electronic notarization systems. Chapter 4 lays out requirements for these systems in general, but specific requirements for remote electronic notarizations are stipulated.

Subparagraph (b)(1) requires a means of authentication to the system that reasonably ensures only the proper parties have access to the system. For example, the parties may have unique login credentials or be given a one-time passcode that admits them to the session.

Subparagraph (b)(2) simply requires the system to allow the notary to verify the identity of the principal as required under Section 5A-5. For example, the system may facilitate a DKBA identity proofing from within the system. Some systems are designed so that a principal must pass the DKBA before being connected to the audio-video stream with the notary. The provision also highlights that it may be a matter of law or custom in a particular state to identify additional signing witnesses to a document.

Subparagraph (b)(3) addresses the issue concerning certainty that all parties to the electronic notarization are viewing the same record simultaneously. (*See* Subparagraph (a)(3) and Comment.) It requires real-time display of all actions taken on an electronic record involved in the electronic notarial act, just as would be observable by a notary with a paper notarization.

Subparagraph (b)(4) introduces the subject of Section 5A-6, the recording of the audio-video session. A system must facilitate the recording, but also provide a means for access to and copying of the recording in the future.

## § 5A-5 Identification of Principal by Audio-Video Communication.

(a) A notary public shall determine from personal knowledge or satisfactory evidence of identity as described in Subsection (b) that the principal appearing before the notary by means of audio-video

communication is the individual that he or she purports to be.

(b) A notary public has satisfactory evidence of identity if the notary can identify the individual who appears in person before the notary by means of audio-video communication based on:
  (i) the oath or affirmation of a credible witness who personally knows the principal, is personally known to the notary public, and who is in the physical presence of the notary or the principal during the electronic notarial act;
  (ii) a dynamic knowledge-based authentication assessment by a trusted third person that complies with rules adopted by the [commissioning official];
  (iii) a valid public key certificate that complies with rules adopted by the [commissioning official]; or
  (iv) an identity verification by a trusted third person that complies with rules adopted by the [commissioning official].

*(NOTE TO LEGISLATORS: If a jurisdiction opts to allow identification of principals by "dynamic knowledge-based authentication assessment" or "public key certificate" (see above Subparagraphs 5A-5(b)(ii) and 5A-5(b)(iii)), sample implementing rules are provided in Appendix II. The commissioning official is required by Section 15-2 to provide such rules.)*

**Comment**

Section 5A-5 provides the requirements for identifying principals appearing before the notary public by means of audio-video communication. Chapter 8-2 describes satisfactory evidence of identity for electronic notarizations performed when the principal appears in the physical presence of the notary public. Section 5A-5 does not apply to those types of "traditional" electronic acts.

Arguably the most critical policy issue in implementing this Chapter is determining what constitutes convincing evidence for identifying principals appearing by audio-video communication. It would be inherently insecure to allow principals to present tangible identification credentials to the notary via a video screen. Therefore, one state has authorized other forms of satisfactory evidence more germane to the online environment. (*Accord*, VA. CODE ANN. § 47.1-2 — "satisfactory evidence of identity.")

Subparagraph (b)(i) allows principals appearing before the notary remotely to be identified upon the oath of a credible witness. (*See* MONT. CODE ANN. § 1-6-615(3)(a).) An antecedent in-person identity proofing process in accordance with the specifications of the Federal Bridge Certification Authority, a valid digital certificate accessed by biometric data, and an interoperable Personal Identity Verification (PIV) card also are viable options. The PIV card is the tangible and electronic credential issued to employees of the U.S. federal government that allows the cardholder to access federal facilities and information systems, as well as sign electronic records.

Two forms of satisfactory evidence of identity allowed under Section 5A-5(b) correspond with prevailing law. (*See* VA. CODE ANN. § 47.1-2.) A dynamic knowledge-based authentication assessment (Subparagraph (b)(ii)) is

a qualified "antecedent identity proofing process." In addition, a public key certificate (Subparagraph (b)(iii)) is an acceptable "digital certificate" but without the additional requirement that it be accessed by biometric information, such as a thumb- or fingerprint.

Subparagraph (b)(iv) reflects the fact that new identification methods could emerge in the future that prove reliable in verifying the identity of online subjects. It authorizes the use of any identity verification method adopted by the commissioning official by rule.

The "Note To Legislators" clarifies that Chapter 5A and Section 5A-5 in particular are enacted, Section 15-2 requires the commissioning official to promulgate rules to implement Section 5A-1. (*See* Appendix II.)

**§ 5A-6 Recording of Audio-Video Communication.**

(a) A notary public shall create an audio-video recording of every electronic notarial act performed by audio-video communication, and provide for public and official access, inspection, and copying of this recording.

(b) A notary public who uses an electronic notarization system to create the audio-video recording required by this Section shall enable the provider to perform the functions prescribed by Section 5A-4(b)(4).

(c) The audio-video recording required by this Section shall be in addition to the journal entry for the electronic notarial act required by Chapter 9 of this [Act] and shall include:

(1) at the commencement of the recording, a recitation by the notary public of information sufficient to identify the electronic notarial act;

(2) a declaration by the principal that the principal's electronic signature on the record was knowingly and voluntarily made; [and]

(3) all actions and spoken words of the principal, notary public, and any required witness during the entire electronic notarial act[.][; and

(4) at the discretion of the principal, an accurate and complete image of the entire electronic record that was viewed and electronically signed by the principal and notary public.]

(d) The provisions of Sections 9-5, 9-6, and 9-7 of this [Act], related respectively to security, inspection, copying, and disposition of the journal shall also apply to security, inspection, and copying, and disposition of audio-video recordings required by this Section.

**Comment**

Section 5A-6 requires a notary public to record and retain the recording of the audio-video session for an electronic notarial act. Two states have adopted this requirement. (*See* VA. CODE ANN. § 47.1-14C; and MONT. CODE ANN. § 1-6-618(4).) The Uniform Law Commission's amendment to the Revised Uniform Law on Notarial Acts contains a similar requirement as well. (*See* REV. UNIF. LAW ON NOT. ACTS § [14A(g)].) The protection of the public is

heightened by the availability of the recording. For example, would-be impostors could be deterred from committing forgeries involving electronic records by knowing their words and actions would be recorded and archived.

Subsection (a) requires a notary to make available the audio-video recording for public and official access, inspection, and copying. In this regard, it is to be treated similarly to a notary's official journal of notarial acts. (*See* Section 9-6.)

Subsection (b) clarifies that since the recording of the audio-video transmission of an electronic notarial act is the property of the notary public, the notary must allow the provider of the system to archive and allow inspection and copying of the recording. It is envisioned that any user licensing agreement or contract between the system provider and notary will include an authorization by the notary to enable the provider to perform these functions.

Subparagraphs (c)(1) and (2) specify that the audio-video recording must include certain recitations by the notary public and principal at the beginning of the act. (*See* ADMIN. RULES OF MONT. § 44.15.108 for Montana's detailed recitation requirements.) The notary must recite information sufficient to identify the electronic notarial act being performed. Since the notary must keep a journal record for the electronic notarization, more detailed information about the transaction may be recorded there. The principal must declare that the principal's electronic signature on the record was signed knowingly and voluntarily, without duress or coercion. Subparagraphs (c)(3) and (4) require all words and actions of both the notary and principal to be recorded, as well as a complete image of the record being electronically notarized. [Subparagraph (c)(4) is bracketed because the record itself may contain personal identifying or other confidential information, which may prompt a state to consider whether the image of the record ought to be included in the audio-video recording.]

Subsection (d) applies certain provisions related to the notary public's journal of notarial acts to recordings of audio-video electronic notarizations. (*See* Sections 9-5, 9-6, and 9-7 and Comment). This would include keeping the recordings under the sole control of the notary (*see* Section 9-5(b)) and archiving the recordings for ten years (*see* Section 9-7(a)).

### [§ 5A-7 Prohibited Records and Transactions.

A notary public shall not perform an electronic notarial act for a principal based on audio-video communication for the following types of records and transactions: _____.

**Comment**

Section 5A-7 allows an enacting jurisdiction to prohibit the use of audio-video communication for certain high-value or sensitive types of records or transactions. Limiting the procedure to real or personal property titled in the state, or other transactions subject to the jurisdiction of a state court effectively prohibits all other transaction types. (*See, for example,* MONT. CODE ANN. § 1-5-615(3)(b).) The bracketing of this section indicates that other jurisdictions might not choose to impose such restrictions.]]

# Chapter 6 — Electronic Notarial Certificate

**Comment**

General: Chapter 6 specifies rules for the electronic notarial certificates that evidence performance of an electronic notarial act. The certificate of a notary public is presumptive evidence of the facts recorded in it. (*See* IND. CODE ANN. § 33-42-2-6; COLO. REV. STAT. § 38-35-101; ME. REV. STAT. ANN. tit. 16 § 355; N.D. CENT. CODE § 39-04-17; N.J. STAT. ANN. § 2A:82-17; and TENN. CODE ANN. § 24-5-103.) Thus, proper completion of a certificate for an electronic notarial act is of critical importance. Section 6-1 states that a notary must complete an electronic notarial certificate for every electronic act at the time the act is performed. Section 6-2 prescribes the form for an electronic notarial certificate. Section 6-3 recognizes the electronic notarial acts that are performed by notaries public and notarial officers of other jurisdictions.

## § 6-1 Completion of Electronic Notarial Certificate.

(a) For every electronic notarial act performed, a notary public shall complete an electronic notarial certificate that complies with the requirements of this [Act].

(b) An electronic notarial certificate shall be completed at the time of the electronic notarization and in the physical presence of the principal [or during the single recorded session required by Section 5A-4(a)(2) for any electronic notarial act performed using audio-video communication].

**Comment**

Section 6-1 sets down the general rule requiring a notary to complete an electronic notarial certificate for every electronic notarial act performed. The requirements for the certificate are delineated in the following sections.

Subsection (b) prohibits the practice, not uncommon with paper certificates, of pre-signing and pre-sealing notarial certificates to save time. This is both an improper and a dangerous practice that could result in theft and subsequent fraudulent use of the completed certificates. By implication, the Act would prohibit an electronic notarization system from allowing a notary to complete an electronic certificate prior to performance of the electronic notarial act. (*See* Section 4-1(a).) [The bracketed wording pertains when the electronic notarial act is performed by audio-video communication.]

## § 6-2 Form of Electronic Notarial Certificate.

[(a)] An electronic notarial certificate shall include a venue for the notarial act and shall be in a form as [set forth in Section [____] of [_____]] OR [permitted by custom in this [State]] for a non-electronic notarial act of the same type.

[(b) If an electronic notarial act was performed by means of audio-video communication in compliance with Chapter 5A of this [Act], the certificate shall include a statement to that effect.]

**Comment**

The form required for an electronic notarial act should mirror the same prescribed form for a paper-based notarization. Many jurisdictions provide statutory forms in their notary code (*see* IOWA CODE ANN. § 9B.16; MINN. STAT. ANN. § 358.48; N.M. STAT. ANN. § 14-14-8; and WASH. REV. CODE ANN. § 42.44.100.), or property statutes (*see* ALA. CODE § 35-4-29; FLA. STAT. ANN. § 695.25; and N.Y. REAL PROP. LAW § 309-a), or permit forms derived from customary use.

[Subsection (b) is bracketed. Its inclusion is dependent upon enactment of the bracketed Chapter 5A. The certificate for an electronic notarial act must indicate that the act was performed by means of audio-video communication.

Two states do not require a certificate for an electronic notarial act performed online to indicate the act was performed by means of audio-video communication. These states have modified their laws to clarify that a remote "appearance" before a notary qualifies as a "personal appearance." (*See* MONT. CODE ANN. § 1-5-603(7)(a); VA. ELEC. NOT. ASSURANCE STAND., ver. 1.0, Definition (a).)

Subsection (b) leaves open how to implement this requirement. Two possible ways are described below.

In the first, the language of the certificate itself could be modified to state, "This record was acknowledged before me by means of audio-video communication on (date) by (name of principal)." Indeed, the amendment to the Revised Uniform Law on Notarial Acts requires the use of notarial certificates which explicitly state not only that the principal appeared before the notarial officer by means of communication technology but also the physical location of the principal during the electronic notarization: "This record was acknowledged before me by use of communication technology on (date) by (name of principal), who verified that (he)(she)(they) is/are physically located in (name of foreign state)..." (*See* REV. UNIF. LAW ON NOT. ACTS § [14A(h)].)

In the second, the certificate for the electronic notarial act may be substantially in the form allowed under other existing law (*see* Section 5-2(4)), but include a notice at the top of the certificate stating that the electronic notarial act was performed by means of audio-video communication. An example of such a notice might be: "This electronic notarial act is based on audio-video communication between the notary and the principal, who declared that he or she was physically located in _____(jurisdiction) at the time of the notarial act, and who was identified by the notary through _____(means of identification), in compliance with Chapter 5A of [Act]." In early drafts of the MENA, some drafters opposed such a provision, believing it would relegate electronic notarial acts performed by means of audio-video communication to "second class citizen" status *vis-à-vis* traditional paper-based or electronic notarizations performed in the physical presence of the notary.

Other MENA drafters maintained that such a notice would foster acceptance, not rejection, of these remote electronic acts.

Remote electronic notarizations are so new the public might be wary of trusting them. For support, the drafters point to the states that have authorized a notary public or other individual to sign on behalf of a principal with a physical disability. These laws require the notary or other individual to write a notice below the signature, "Signature affixed by (name of individual) pursuant to (applicable section of state law)," or

words of similar import. (*See* COLO. REV. STAT. § 12-55-110.5(1); FLA. STAT. ANN. § 117.05(14)(d); MICH. COMP. LAWS § 55.293; MONT. CODE ANN. § 1-5-623; NEB. REV. STAT. § 64-105.02(2); N.M. STAT. ANN. § 14-12A-7D; N.C. GEN. STAT. § 10B-20(e); S.C. CODE ANN. § 26-1-90(G); TEX. GOV'T CODE § 406.0165; WASH. REV. CODE ANN. § 42.44.080(2); and WYO. STAT. ANN. § 34-26-201(d).) To parties relying on a notarized document who might not otherwise trust a signature made by proxy, the notice below the signature is intended to promote acceptance. In fact, the Florida statute directs the notary to state the circumstances of the signing in the notarial certificate for a signature made by proxy, and the Texas statute expressly states that the signature made by the notary on behalf of the physically-disabled principal is as effective as the signature of the individual, and any bona fide purchaser for value may rely on the signature of the notary as evidence of the principal's consent to sign the document. (*See* FLA. STAT. ANN. § 117.05(14)(d)(3) and TEX. GOV'T CODE § 406.0165(c).) The notice on the certificate for a remote electronic notarial act promotes a similar positive goal.

While preferring the second option, a majority of the drafters ultimately determined that allowing flexibility on how Subsection (b) was achieved was the best policy, as long as the certificate of the electronic notarial act, at a minimum, indicated in some manner that the act was performed by means of audio-video communication.]

**§ 6-3 Recognition of Acts from Other Jurisdictions.**

(a) An electronic notarial act shall have the same effect under the law of this [State] as if performed by a notary public of this [State] if the act is performed by a notary public or notarial officer under authority of:
  (1) another state of the United States;
  (2) the government of the United States;
  (3) the government of a foreign nation; or
  (4) a tribal government recognized by the United States.

(b) The electronic signature, title, and, if required by law, electronic seal of the individual described in this Section are prima facie evidence that the electronic signature and seal are genuine and that the individual holds the indicated title.

(c) The authority of an individual described in Subsection (a)(3) is conclusively established if the title of the office and indication of authority to perform electronic notarial acts appears either in a digest of foreign law or a list customarily used as a source for that information.

(d) An electronic Apostille in compliance with the Hague Convention Abolishing the Requirement of Legalization for Foreign Public Documents of October 5, 1961, or certificate of foreign service or consular officer of a nation stationed in the United States, conclusively establishes that the electronic signature and seal of an individual described in Subsection (a)(3) are genuine and that the individual holds the indicated title.

**Comment**

In Section 6-3, the issue of recognition of electronic notarial acts performed in other states and jurisdictions is addressed. With respect to the official electronic notarial acts of notaries and notarial officers of other U.S. states, Subparagraph (a)(1) states the general rule that an out-of-state electronic act is to be recognized provided it was performed by a notary or notarial officer of that jurisdiction in compliance with the law of that jurisdiction. This policy is consistent with existing laws on the recognition of acknowledgments and other notarial acts in jurisdictions of the United States. (*See* ALA. CODE § 35-4-26; ALASKA STAT. § 09.63.050 and § 09.63.080; ARIZ. REV. STAT. ANN. § 33-501 and § 33-504; ARK. CODE ANN. § 16-47-103(a)(2) and § 16-47-203; CAL. CIV. CODE § 1182 and § 1189(b); COLO. REV. STAT. § 12-55-203 and § 12-55-206; CONN. GEN. STAT. ANN. § 1-30; § 1-57; and § 1-60; DEL. CODE ANN. tit. 29 § 4324; D.C. CODE ANN. § 42-144; FLA. STAT. ANN. § 92.50(2); GA. CODE ANN. § 44-2-21; HAW. REV. STAT. § 502-45; IDAHO CODE § 55-703; 765 ILCS § 30/2 and § 30/5; IND. CODE ANN. § 32-21-2-5; IOWA CODE ANN. § 9B.11; KAN. STAT ANN. § 53-505; KY. REV. STAT. ANN. § 423.110 and § 423.140; LA. REV. STAT. ANN. § 35:6; ME. REV. STAT. ANN. tit. 4, § 1011 and § 1014; MD. CODE ANN. (STATE GOV'T) § 19-103 and § 19-110; MASS. GEN. LAWS ANN. ch. 183, § 30(b); MICH. COMP. LAWS § 565.262 and § 565.265; MINN. STAT. ANN. § 358.44; MISS. CODE ANN. § 89-3-9 and § 89-3-11; MO. ANN. STAT. § 442.150; MONT. CODE ANN. § 1-5-605; NEV. REV. STAT. ANN. § 240.164; N.H. REV. STAT. ANN. § 456-B:4; N.J. STAT. ANN. § 46:14-6.1; N.M. STAT. ANN. § 14-14-4; N.Y. REAL PROP. LAW § 299 and § 299-a; N.C. GEN. STAT. § 47-2; N.D. CENT. CODE § 44-06.1-10; OHIO REV. CODE ANN. § 147.51 and § 147.54; OKLA. STAT. ANN. tit. 49, § 115; OR. REV. STAT. § 194.260; 57 PA. CONST. STAT. ANN. § 311; R.I. GEN. LAWS § 34-12-1 and § 34-12-2(2); S.C. CODE ANN. § 26-3-20 and § 26-3-50; S.D. CODIFIED LAWS § 18-5-3 and § 18-5-15; TENN. CODE ANN. § 66-22-103 and § 66-22-115; TEX. CIV. PRAC. AND REMEDIES CODE § 121.001(b); UTAH CODE ANN. § 57-2a-3(2); VT. STAT. ANN. tit. 27 § 379; VA. CODE ANN. § 55-118.1; WASH. REV. CODE ANN. § 42.44.130; W.VA. CODE § 39-4-11; WIS. STAT. ANN. § 706.07(4); and WYO. STAT. ANN. § 34-26-104.)

Despite the settled law regarding the recognition of notarial acts performed by notaries public of other jurisdictions of the United States, the drafters note the existence of a statute that requires the notarial act to be performed *in the physical presence* of the notary or notarial officer of the other jurisdiction. (*See* IOWA CODE ANN. § 9B.11.4 and § 9B.2.10, where "personal appearance" is defined as a *physical* appearance and specifically excludes "appearances which require video, optical, or technology with similar capabilities.") This law sets an unwelcome precedent of requiring a notarial act to be performed in conformance with the law of Iowa as a qualification for recognition in Iowa. Presumably, this law might imperil acceptance of electronic records validly notarized under another jurisdiction's remote electronic notarization laws when presented for recording in Iowa.

Section 6-3 recognizes notarial acts performed by notaries public and notarial officers operating under the law of the United States, foreign governments, and federally-recognized tribal governments. The 2010 Model Notary Act included separate sections for recognition of notarial acts performed by notaries and notarial officers under U.S.

federal authority and under the authority of a foreign government. (*See* Sections 11-3 and 11-4.) It omitted, however, recognizing the notarial acts of notaries and notarial officers operating under the authority of federally-recognized tribal governments. Following the lead of the Revised Uniform Law on Notarial Acts, the drafters determined to include a provision in Subparagraph 6-3(a)(4) recognizing these acts as well. (*See*, REV. UNIF. LAW ON NOT. ACTS § 12.)

Subsection (b) allows any of these notarizing officials' certificates to be self-proving if it bears an official's electronic signature, title, and, if law requires its use, an electronic seal of office.

Subsection (c) states that the foreign official's authority to perform notarial acts is proven if the title and authority of the officer is listed in a commonly-accepted source.

Subsection (d) mandates that an Apostille issued in compliance with the Hague Apostille Convention (*see* Section 11-1(a)(1)) authenticating a foreign notarial certificate must be accepted as genuine. For countries not party to the Hague Apostille Convention, Subsection (d) also asserts that the certificate of a foreign service or consular official of that nation stationed in the United States accompanying the electronically-notarized record will conclusively establish the electronic signature, seal and title of the notarizing official.

## Appendix I — Verification of Identities in Online Transactions

MENA Section 15-2 specifically requires rules for Section 5A-5 to be adopted. Section 5A-5 provides a definition of satisfactory evidence for identifying principals appearing before the notary public by means of audio-video communication.

Electronic notarizations performed by means of audio-video communication present a unique challenge. In most notarization scenarios today, tangible identity credentials are presented to the notary. While newer credentials contain computer chips, bar codes, or magnetic swipe strips which allow the information in a credential to be read and validated electronically, most notaries are not equipped to use these technologies. They must rely on sight and touch to visually and tactilely inspect a credential for authenticity in comparison to the principal appearing physically in front of them.

In an electronic notarization using audio-video communication, the notary is unable to hold the credential. Further, the quality of the camera and video transmission limits visual inspection. Clearly, simply holding a driver's license or passport up to the video camera could allow impostors to foist as genuine an altered or counterfeit identity credential.

Thus, new methods of identifying principals are needed for notarizations involving audio-video communication. In recent years, the emerging identity management ("IdM") field has sought to standardize the means by which individuals are identified in the digital world. Its work forms the framework for the model rules proposed in Appendix II for verifying the identities of principals in online electronic notarizations.

IdM standards typically begin by identifying "levels of authentication." For example, the federal Office of Management and Budget's "E-Authentication Guidance for Federal Agencies"[1] defines four levels of assurance ("LOA") to indicate the degree of confidence given an individual's asserted identity:

- LOA 1: little or no confidence
- LOA 2: some confidence
- LOA 3: high confidence
- LOA 4: very high confidence

Beginning with LOA 2, each LOA is associated with increasingly rigorous methods for verifying the asserted identity of an individual.[2] At LOA

---

[1] Executive Office of the President OMB Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, December 16, 2003, last viewed on December 8, 2016, at https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf.

[2] National Institute of Standards and Technology (NIST), Special Publication 800-63-2, *Electronic Authentication Guideline,* August 2013, last viewed on December 8, 2016, at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf.

2, an in-person or remote[3] identity proofing of applicants is required.[4] At LOA 3, an in-person or remote identity proofing and verification of identifying materials and information is required.[5] In addition, at least two authentication factors are necessary.[6] At LOA 4, only in-person identity proofing is allowed.[7]

The goal is to apply the appropriate level of authentication to a transaction based upon the perceived risks and the potential harm or impact. The risks usually consider several impact categories (damaged reputation, financial loss or liability, personal safety, public interest, etc.) and range from low to moderate to high. A low impact at worst would have a limited adverse effect, while a moderate impact at worst would have a serious effect. A high impact would present a severe or catastrophic adverse effect.[8] The table below charts the maximum potential impacts for each assurance level.[9]

| | **Assurance Level Impact Profiles** | | | |
|---|---|---|---|---|
| **Potential Impact Categories for Authentication Errors** | **1** | **2** | **3** | **4** |
| Inconvenience, distress or damage to standing or reputation | Low | Mod | Mod | High |
| Financial loss or agency liability | Low | Mod | Mod | High |
| Harm to agency programs or public interests | N/A | Low | Mod | High |
| Unauthorized release of sensitive information | N/A | Low | Mod | High |
| Personal Safety | N/A | N/A | Low | Mod High |
| Civil or criminal violations | N/A | Low | Mod | High |

Which level of assurance is appropriate for an online electronic notarization conducted by means of audio-video communication? LOA 1 may be dismissed since a notarization of a signature requires higher confidence in an individual's asserted identity than LOA 1 provides, and the risk of loss for

---

[3] In this context, a "remote" identity proofing is conducted through record checks with an applicable agency or institution that issued an identity credential or through credit bureaus or similar databases.

[4] NIST Special Publication 800-63-2, at vi and vii.

[5] *Id.*

[6] The three authentication factors are: (1) something you *have* (one-time password token, employee ID card, mobile phone, etc.); (2) something you *know* (password) and (3) something you *are* (biometric identifier such as a fingerprint, retina scan or voice recognition).

[7] NIST Special Publication 800-63-2, at vii.

[8] OMB Memorandum M-04-04.

[9] *Id.*

many of these transactions is greater.

At the other extreme, LOA 4 also may be dismissed. A notarization of a signature generally does not require the level of confidence in an individual's asserted identity that LOA 4 requires, and the risk of loss for most of these transactions is less severe. An example of a LOA 4 identity verification is the U.S. federal government Personal Identity Verification ("PIV") card application process that meets the minimum requirements mandated by Homeland Security Presidential Directive-12 ("HSPD-12").[10] An HSPD-12 identity credential is used by federal government workers and contractors to access federal buildings and computer networks. Since the potential risk of loss across all impact levels is moderately high or high, applicants must appear in person before an agent and present two forms of written of identification, submit a full set of fingerprint images for comparison against FBI databases, and have a facial photograph taken.[11] That level of identity proofing for an electronic notarial act is excessive.

A LOA 2 or 3 identity verification process[12] would be appropriate for most notarizations. Some notarized records, however, carry higher risks than others. For example, from low to high, a parental permission slip, a signature gatherer's election petition, a conveyance for a valuable piece of property, and a power of attorney for finances or healthcare. Since it is impractical to adopt a flexible methodology for authenticating principals based upon the individual risk of a particular notarization, Section 5A-5 and Model Rules 1 and 2 presented in Appendix II propose standards for verifying identity at LOA 2.

---

[10] Homeland Security Presidential Directive 12: *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004, last viewed on December 8, 2016 at https://www.dhs.gov/homeland-security-presidential-directive-12.

[11] Federal Information Processing Standards Publication (FIPS) Pub 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, August, 2013, last viewed on December 8, 2016, at http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf, at 6.

[12] Federal specifications in the IdM world are evolving. At the time of publication, NIST was preparing Draft Special Publication 800-63-3 for a 60-day public comment period, and, if released, it would supersede Special Publication 800-63-2. The draft proposes a new mapping scheme for the levels of assurance. It introduces the new terms "identity assurance level" ("IAL"), defined as an ordinal that conveys the degree of confidence that the applicant's claimed identity is the real identity; "authenticator assurance level" ("AAL"), defined as "a metric describing robustness of the authentication process proving that the claimant is in control of a given subscriber's authenticator(s)"; and "federation assurance level" ("FAL"), defined as "a metric describing the robustness of the assertion protocol utilized by the federation to communicate authentication and attribute information (if applicable) to a relying party." Instead of four levels of authentication, the new draft standard proposes three, with current LOAs 2 and 3 mapping at new level 2.

## Appendix II — Model Rules Implementing MENA Section 5A-5

Appendix II provides model rules for jurisdictions enacting bracketed Sections 5A-5(b)(ii) and (iii) of the Model Electronic Notarization Act. These Sections prescribe two acceptable methods of establishing satisfactory evidence of identity for electronic notarizations performed by means of audio-video communication: a dynamic knowledge-based authentication assessment and a public key certificate. Rule 1 provides rules for the former and Rule 2, the latter. Bracketed Section 15-2 provides the authority for adopting these rules.

**Rule 1 Dynamic Knowledge-Based Authentication Assessment.**

(a) A dynamic knowledge-based authentication assessment satisfying the requirement of [statute codifying Subparagraph 5A-5(b)(ii)] shall:
  (1) contain a series of five (5) random multiple choice questions with a minimum of five (5) choices each;
  (2) require a score of eighty (80) percent or higher to pass;
  (3) require the individual to answer all questions in a total time of two (2) minutes or less;
  (4) allow any individual who fails the assessment to undergo a second assessment with different questions than those in the first assessment; and
  (5) return as part of the assessment a "pass" or "fail" score as well as a transaction identification number that is unique to the identification verification session.

(b) An identity verification provider that offers the services of a dynamic knowledge-based authentication assessment shall ensure that only the principal whose identity is being verified is shown the questions and that the assessment is protected in an encrypted session.

(c) The principal shall bear the cost of the dynamic knowledge-based authentication assessment described in this Section.

(d) The result of the dynamic knowledge-based authentication assessment and the transaction identification number shall be recorded in the notary's journal.

*Explanatory Note*

Rule 1 allows the principal to be identified through a dynamic knowledge-based authentication ("DKBA") assessment. The standards for the DKBA — the number of questions asked, the number of answers provided, the time limit imposed, and the number of repeat assessments allowed — generally are implemented by identity verification providers today.

An electronic notarization system may provide the DKBA assessment, but Rule 1(b) requires, first, that only the principal may view the questions

and answers, and, second, that the assessment must be presented in an encrypted session. Since an identity verification provider requires an individual's Social Security number in order to create the questions, allowing any other individual — including the notary — to view the questions and answers would constitute a breach of privacy. Rule 1(a)(5) only requires that the pass/fail result and transaction identification number be provided to the notary. Rule 1(d) requires the notary to record the result and transaction identification number in his or her journal.

**Rule 2 Public Key Certificate.**

(a) A public key certificate satisfying the requirement of [statute codifying Subparagraph 5A-5(b)(iii)] shall:
  (1) conform to the International Telecommunication Union ITU-T X.509 v3 standard, and any updates thereto;
  (2) be issued at or equivalent to the [second] or higher level of assurance, as most currently defined by the United States National Institute of Standards and Technology; and
  (3) be capable of validation in real time at the time of the electronic notarization.

(b) For every public key certificate, an electronic notarization system shall be capable of validating:
  (1) the type of certificate;
  (2) the certification authority that issued the certificate;
  (3) the name or identity of the individual to whom the certificate was issued;
  (4) the operational period of the certificate; and
  (5) the date and time of signing by the principal.

(c) The information returned by the validation check required by Subparagraphs (1) through (5) of Subsection (b) shall be recorded in the notary's journal.

(d) A notary public shall not perform an electronic notarial act if the principal's public key certificate fails the validation check required by Subsection (b).

*Explanatory Note*

Rule 2 allows a signer to present a valid public key certificate issued at or equivalent to the [second] level of assurance, as currently specified by the United States National Institute of Standards and Technology ("NIST"). (*See* Appendix I for a description of the levels of authentication.) The public key certificate must conform to existing technical standards (Rule 2(a)(1)). At the time of publication NIST was preparing Draft NIST Special Publication 800-63-3 for a 60-day comment period. The draft redefines, renumbers and renames the LOAs. Under the new scheme, LOA 2 would correspond with the new Identity Assurance Level ("IAL") 2.

A public certificate issued at LOA 2 requires an applicant to have his or her identity vetted more stringently than for credentials issued at LOA 1. For example, an applicant may go to a notary public with a government-issued photo ID. The applicant then must complete a paper document or electronic record with the information from these identification credentials. The notary verifies the applicant's identity and notarizes the individual's signature. Based upon the evidence of this identity proofing, the certification authority issues the public key certificate to the applicant.

Rule 2(a)(2) also allows a notary public to accept a public key certificate that is equivalent to one issued at NIST LOA 2. This would allow a notary to accept a certificate issued by a certification authority from a country outside of the United States as long as it is issued under the standards for a LOA 2 certificate.

The principal will sign the electronic record with his or her public key certificate. This will allow the notary to validate the certificate (Rule 2(a)(3)) for the attributes specified in Rule 2(b). The electronic notarization system must be capable of enabling the notary to perform this validation. Rule 2(c) requires the notary to record details from the validation result in his or her journal.

The rules are written using terminology adopted by the RULONA in place of the MENA language. Below are six key examples of differing terminology meaning the same thing:

| RULONA | MENA |
|---|---|
| Communication technology | Audio-video communication |
| Communicate simultaneously by sight and sound | Communicate in real time |
| Official stamp | Electronic seal |
| Notarial acts with respect to electronic records | Electronic notarial acts |
| Notification (to notarize electronic records) | Registration (to perform electronic notarizations) |
| Tamper-evident technology | Electronic notarization system |

It should be kept in mind that the rules proposed in this Appendix can stand alone as workable regulations, but they also can be modified by the commissioning officer or agency to accommodate the needs and preferences in a given jurisdiction.

## Chapter 1 — Implementation

**Rule 1.1 Authority.**
Chapters 1-12 of this [title of administrative code] implement [statutes codifying the RULONA].

**Rule 1.2 Scope.**

[(a)] Consistent with [statute codifying RULONA Section 27], these rules:

(1) prescribe the manner of performing notarial acts regarding electronic records;

(2) include provisions to ensure integrity in the creation, transmittal, storage, or authentication of electronic records or signatures;

(3) include provisions to prevent fraud or mistake in the performance of notarial acts related to electronic records; and

(4) set procedures for notifying the [commissioning officer or agency] of a notary public's intent to notarize electronic records pursuant to [statute codifying RULONA Section 20].

[(b) Consistent with [statute codifying RULONA Section [14A]], these rules:

(1) prescribe the means of performing a notarial act involving communication technology to interact with an individual located outside of the United States;

(2) establish standards for the approval of communication technology by the [commissioning officer or agency]; and

(3) establish standards for the retention of a video and audio copy of the performance of notarial acts.]

*Explanatory Note*

Rule 1.2 restates the scope of the rules as set forth in RULONA Sections 27 and [14A]. It should be noted that Section 27 vests the commissioning officer or agency with broad rule-making authority over the entire act. (*See* Rule 1.1 and RULONA Section 27(a).) Section 27 also allows rules to be adopted for provisions in the RULONA not specifically covered under the MENA (*e.g.,* the commissioning process). Only the specific provisions related to the scope of the MENA are stated in Rule 1.2.

**Rule 1.3 Implementation Date.**
Chapters 1-12 of this [title of administrative code or other regulatory citation] were adopted on [_____].

## Chapter 2 — Definitions

**Rule 2.1 Appear Personally.**
For purposes of [statute codifying RULONA Section[s] 6 [and 14A]] and these rules, "appear personally" means:

[(1)] being in the same physical location as another person and close enough to see, hear, communicate with, and exchange tangible identification credentials with that individual[.][; or

(2) interacting with another individual by means of communication technology in compliance with Chapter 5A of these [Rules].

*Explanatory Note*

RULONA Section 6 requires an individual to appear personally before the notary public if the notarial act relates to a statement made in or a signature executed on a record. "Appear personally," however, is not defined. Rule 2.1 provides a definition of this term based upon MENA Section 2-1.

[Jurisdictions enacting the audio-video communication provisions of MENA Section 2-1(b), Chapter 5A and Section 6-2(b) should include Rule 2.1(2), while those that choose not to enact these provisions should remove it. RULONA Section [14A] uses "communication technology," while the MENA uses the term "audio-video communication." Rule 2.1 adopts the former.]

**Rule 2.2 Electronic Journal.**
"Electronic journal" means a chronological record of notarizations maintained by a notary public in an electronic format in compliance with Chapter 9.

*Explanatory Note*

A jurisdiction that has not enacted RULONA Section [19] (relating to a journal of notarial acts) should consider adopting a rule requiring notaries public to keep and maintain a journal of notarial acts for electronic notarizations. The journal helps prevent both fraud and mistakes. (*See*

RULONA § 27(a)(5), authorizing the commissioning official to promulgate rules to prevent fraud and mistakes with respect to notarial acts, and Rule 1.2.) The official comment to RULONA Section 20 highlights the assurances provided by the journal in protecting the integrity of the notarial system and concludes, "In that regard, it (the journal) provides protection to both the notary and to the public whom the notary serves."

In adopting the definition from MENA Section 2-4 here, jurisdictions should consider the Chapter 9 provisions on the journal, especially if it has no current rules requiring notarial records for paper-based acts. Applicable sections from MENA Chapter 9 are incorporated into Chapter 9 of these rules.

**Rule 2.3 Electronic Notarial Certificate.**
"Electronic notarial certificate" means the part of, or attachment to, an electronic record that is completed by the notary public, contains the information required under [statute codifying RULONA Section 15(b)] or the notary's official stamp, bears that notary's electronic signature, and states the facts attested to by the notary in a notarization performed on an electronic record.

*Explanatory Note*

Rule 2.3 has been crafted to be consistent with RULONA Section 15, which allows a notary public to include the information specified in Subsections (a)(2), (3), and (4) in lieu of adding an official stamp on an electronic record. (*See* RULONA Section 15(b).) If this information is added to the electronic record, an official stamp is permitted but not required.

**Rule 2.4 Enrollment.**
"Enrollment" means a process for registering a notary public to access and use a tamper-evident technology in order to perform notarial acts with respect to electronic records.

*Explanatory Note*

The MENA definition "enrollment" (s*ee* MENA § 2-10) is carried over in substance and modified to reflect the style of the RULONA.

**Rule 2.5 Principal.**
"Principal" means:

(1) an individual whose electronic signature is notarized; or
(2) an individual, other than a witness required for a notarization with respect to an electronic record, taking an oath or affirmation from the notary public.

**Rule 2.6 Provider.**
"Provider" means an individual or entity that offers the services of a tamper-evident technology.

**Rule 2.7 Sole Control.**
"Sole control" means at all times being in the direct physical custody of the notary public or safeguarded by the notary with a password or other secure means of authentication.

*Explanatory Note*

The term "sole control" is defined in Rule 2.7 and implemented in rules pertaining to the Notary's electronic signature, electronic journal, and use of tamper-evident technology. (*See* Rules 7.2(b), 9.4(b) and 12.2(d).)

**Rule 2.8 Tamper-Evident Technology.**
"Tamper-evident technology" means a set of applications, programs, hardware, software, or other technologies designed to enable a notary public to perform notarial acts with respect to electronic records and to display evidence of any changes made to an electronic record.

*Explanatory Note*

The RULONA does not use the MENA term "electronic notarization system." Instead, it uses "tamper-evident technology." "Tamper-evident," however, is not defined in RULONA. Thus, it is defined here using the substance of the MENA term.

**Rule 2.9 Venue.**
"Venue" means the jurisdiction where the notary public is physically located while performing a notarial act with respect to an electronic record.

## Chapter 3 — Notification to Perform Notarial Acts on Electronic Records

**Rule 3.1 Notification of [Commissioning Officer or Agency].**

(a) A notary public shall notify the [commissioning officer or agency] that the notary public will be performing notarial acts with respect to electronic records with the name that appears on the notary's commission.
(b) A notary public shall notify the [commissioning officer or agency] for each commission term before performing notarial acts with respect to electronic records.
(c) An individual may apply for a notary public commission and provide the notification required by this Rule at the same time.
(d) An individual may elect not to perform notarial acts with respect to electronic records.

*Explanatory Note*

Rule 3.1 expands on matters that RULONA Section 20(a) implies. Rule 3.1(a) provides that notification to perform notarial acts with respect to

electronic records must be undertaken for each commission term. Rule 3.1(c) gives notary commission applicants the flexibility to notify the commissioning officer or agency at the same time they apply for a commission or renewal commission. Rule 3.1(d) also clarifies that an individual may choose not to perform notarial acts with respect to electronic records.

**Rule 3.2 Course of Instruction and Examination.**

(a) Before the notification required by Rule 3.1, an individual shall complete a course of instruction of [_____] hours approved by the [commissioning officer or agency] and pass an examination based on the course.

(b) The content of the course shall include notarial rules, procedures, and ethical obligations pertaining to electronic notarization in [Section [___] of [_____]] OR [any pertinent law or official guideline of this [State]].

(c) The course may be taken in conjunction with any course required by [the [commissioning officer or agency]] OR [Section [____] of [_____]] for a notary public commission.

*Explanatory Note*

Rule 3.2 requires a notary to take a course and pass an examination before initial notification of the commissioning officer or agency. A jurisdiction considering whether to require a course or examination, or both, should carefully consider the benefits. (*See* MENA § 3-2 and Comment.)

**Rule 3.3 Term of Notification.**

Unless terminated pursuant to Rule 12.2, the term in which a notary may perform notarizations with respect to electronic records shall begin on the notification starting date set by the [commissioning officer or agency] pursuant to Rule 3.1, and shall continue as long as the notary public's current commission remains valid.

*Explanatory Note*

Rule 3.3 delineates the specific term of a notary public's authorization to perform notarizations with respect to electronic records, establishing the effective date set by the commissioning officer or agency. Although Rule 3.3 does not explicitly require the commissioning officer or agency to provide an official written notification of this date, it is implied.

**Rule 3.4 Notification Application.**

An individual notifying the [commissioning officer or agency] that he or she will be performing notarial acts with respect to electronic records shall submit to the [commissioning officer or agency] an application which includes:

(1) proof of successful completion of the course and examination

required under Rule 3.2;

(2) disclosure of any and all license or commission revocations or other disciplinary actions against the applicant; [and]

(3) any other information, evidence, or declaration required by the [commissioning officer or agency][.][; and

(4) evidence that the surety bond prescribed by Rule 5A.3 for performance of notarial acts by communication technology has been issued.]

*Explanatory Note*

Rule 3.4 specifies the information that must be included in an application to notify the commission official of an applicant's intent to perform notarial acts with respect to electronic records. Subsection (2) applies to notaries who apply to perform notarial acts with respect to electronic records after a notary's commission has been granted, and requires a notary to disclose any action taken against a professional license or other disciplinary action subsequent to the application for a commission or that has not been previously disclosed.

[Subparagraph (4) applies to jurisdictions that have enacted RULONA Section [14A] and also have specific authority to adopt a rule requiring notaries public to have a separate surety bond as prescribed under MENA Section 5A-3. Since Section [14A] allows notarization of both paper documents and electronic records, Subparagraph (4) has been modified to allow for this.]

**Rule 3.5 Approval or Rejection of Notification Application.**

(a) Upon the applicant's fulfillment of the requirements for notification under this Chapter, the [commissioning officer or agency] shall approve the notification and issue to the applicant a unique registration number.

(b) The [commissioning officer or agency] may reject a notification application if the applicant fails to comply with this Chapter.

**Rule 3.6 Confidentiality.**

Information in the notification application shall be safeguarded under the same standards as an application for a notary public commission [as set forth in Section [____] of [_____]].

**Rule 3.7 Database of Notaries Public.**

In addition to the requirements of [statute codifying RULONA Section 24], the electronic database of notaries public maintained by the [commissioning officer or agency] shall describe every administrative or disciplinary action taken against the notary public.

*Explanatory Note*

Both MENA Section 3-7 and RULONA Section 24 require the commissioning officer or agency to create a database of notaries public.

MENA Section 3-7, however, additionally requires the database to include any disciplinary action taken against a notary. Rule 3.7 adds this substantive provision from MENA Section 3-7 lacking in RULONA Section 24.

## Chapter 4 — Tamper-Evident Technology

**Rule 4.1 Requirements for Technologies and Providers.**

(a) A tamper-evident technology shall comply with these Rules adopted by the [commissioning officer or agency].

(b) A tamper-evident technology requiring enrollment prior to performance of notarial acts with respect to electronic records shall enroll only notaries public who have notified the [commissioning officer or agency] that they will be performing such acts pursuant to Chapter 3 of these [Rules].

(c) A tamper-evident technology provider shall take reasonable steps to ensure that a notary public who has enrolled to use the technology has the knowledge to use it to perform notarial acts with respect to electronic records in compliance with these [Rules].

(d) A provider of a tamper-evident technology requiring enrollment shall notify the [commissioning officer or agency] of the name of each notary public who enrolls within five days after enrollment.

(e) A notary public who uses a tamper-evident technology not requiring enrollment shall notify the [commissioning officer or agency] of the date of initial use of the technology within five days after the initial use by means prescribed by the [commissioning officer or agency].

(f) A tamper-evident technology shall require access to the system by a password or other secure means of authentication.

(g) A tamper-evident technology shall enable a notary public to affix the notary's electronic signature in a manner that attributes such signature to the notary.

(h) A tamper-evident technology shall render every electronic notarial act tamper-evident.

*Explanatory Note*

MENA Chapter 4 requires any electronic notarization system used to perform a notarial act with respect to electronic records to meet certain performance standards. The standards of MENA Section 4-1 have been incorporated into Rule 4.1 largely intact, except that the RULONA term "tamper-evident technology" replaces the MENA's "electronic notarization system.

**Rule 4.2 Notary Not Liable for Technology Failure.**

A notary public who exercised reasonable care enrolling in and using a tamper-evident technology shall not be liable for any damages resulting from the technology's failure to comply with the requirements of these [Rules].

Any provision in a contract or agreement between the notary and provider that attempts to waive this immunity shall be null, void, and of no effect.

*Explanatory Note*

Rule 4.2 protects a blameless notary public from liability resulting from any failure of a tamper-evident technology to comply with the legal requirements as long as the Notary used the technology with reasonable care. Rule 4.2 substantially reflects MENA Section 4-2.

**Rule 4.3 Refusal of Requests to Use System.**
A notary public shall refuse a request to:

(1) use a tamper-evident technology that the notary does not know how to operate;
(2) perform a notarial act with respect to an electronic record if the notary does not possess or have access to an appropriate tamper-evident technology; or
(3) perform an electronic notarial act if the notary has a reasonable belief that a tamper-evident technology does not meet the requirements set forth in these [Rules].

*Explanatory Note*

RULONA Section 8 permits a notary to refuse to perform a notarial act for specified reasons. Rule 4.3 adds additional grounds for a refusal that are applicable to electronic records.

Subparagraph (1) supports Rule 4.2. Training on how to use a tamper-evident technology is necessary for a notary's exercise of reasonable care in using the technology, with resulting immunity to liability.

**Chapter 5 —Notarial Acts with Respect to Electronic Records**

**Rule 5.1 Authorized Notarial Acts with Respect to Electronic Records.**
A notary public of this [State] who has notified the [commissioning officer or agency] in compliance with Rule 3.1 may perform the following notarial acts with respect to electronic records:

(1) taking an acknowledgment;
(2) taking a verification on oath or affirmation;
(3) witnessing or attesting a signature;
(4) certifying or attesting a copy; and
(5) noting a protest of a negotiable instrument.

*Explanatory Note*

Except for the notarial act of administering an oath or affirmation, the notarial acts listed in Rule 5.1 match the list of notarial acts in RULONA Section 2(5). As explained in the Comment, oaths and affirmations were

intentionally omitted. (*See* MENA § 5-1 and Comment.) By design, Rule 5.1 omits the notarial act of verification of fact in MENA Section 5-1 since this notarial act is unique to the MENA.

**5.2 Applicability of Other Laws and Rules.**
In performing notarial acts with respect to electronic records, the notary public shall adhere to [statutes codifying the RULONA].

**5.3 Requirements for Notarial Acts Performed with Electronic Records.**

(a) In performing a notarial act with respect to an electronic record, a notary public shall be within the geographic boundaries of this [State].

(b) If a notarial act with respect to an electronic record requires a record to be signed, the principal shall appear personally before the notary public.

[(c) If a notarial act requires administration of an oath or affirmation to a principal, or administration of an oath or affirmation to a witness required for a notarial act related to an electronic record, the notary public may administer that oath or affirmation by means of communication technology.]

*Explanatory Note*

Subsection (b) applies both to notarial acts with respect to electronic records that are performed in the physical presence of the notary public and by using communication technology. It was modified to fit with RULONA Section [14A] by removing the requirement that an electronic record must be signed with an electronic signature. Section [14A] allows a notarization involving communication technology to be performed on both tangible and electronic records. In contrast, the MENA allows it for the notarization of electronic records only.

**[Chapter 5A — Signer Located Outside of United States**

**Rule 5A.1 Definitions Used in This Chapter.**
For the purposes of this Chapter:

(1) "Communication technology" means an electronic device or process that allows an individual located outside of the United States and a notary public located in this state to communicate with each other simultaneously by sight and sound.

(2) "Dynamic knowledge-based authentication assessment" means an identity proofing that is based on a set of questions formulated from public or private data sources for which the principal has not provided a prior answer.

(3) "Person" means 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.

(4) "Personal knowledge" means that the individual appearing before the notarial officer is known to the officer through dealings sufficient to provide reasonable certainty that the individual has the identity claimed.

(5) "Satisfactory evidence of identity" means:

(i) a dynamic knowledge-based authentication assessment by a trusted third person that complies with Rule 5A.2; or

(ii) an identity proofing by a trusted third person that complies with rules adopted by the [commissioning officer or agency].

*Explanatory Note*

Rule 5A.1 is a considerably shortened form of MENA Section 5A-1. It omits several definitions and modifies others. The rule omits the terms "public key certificate" and "real time." "Real time" (*see* MENA § 5A-1(5)) is conveyed in the phrase "…communicate with each other simultaneously by sight and sound" in Subparagraph (1).

Subparagraph (1) adopts the RULONA term and definition found in RULONA Section 14(a)(1) instead of "audio-video communication" in MENA Section 5A-1(1).

Subparagraph (2) defines the term "dynamic knowledge-based authentication assessment" ("DKBA"). DKBA relates closest to the RULONA concept of "identity proofing" in RULONA Section [14A(a)(2)]. Section [14A(j)(3)] allows the commissioning officer or agency to adopt rules to approve providers of third-person identity verification and the process of identity proofing. Therefore, MENA Section 5A-1(2) has been included in this rule.

Subparagraph (3) uses the RULONA definition of "person." (*See* RULONA § 2(9).)

Subparagraph (4) uses the RULONA definition of "personal knowledge" (*see* RULONA Section 7(a)) and not the definition from MENA Section 2-11.

Subparagraph (5) defines the term "satisfactory evidence of identity." Subparagraph (i) allows a DKBA, a form of identity proofing. Subparagraph (ii) allows the commissioning officer or agency to identify an identity verification process or method in addition to the means of satisfactory evidence already defined. MENA provisions allowing the use of a credible witness (*see* MENA § 5A-5(b)(i)) and a valid public key certificate (*see* MENA § 5A-5(b)(iii)) have been omitted.

**Rule 5A.2 Dynamic Knowledge-Based Authentication Assessment.**

(a) A dynamic knowledge-based authentication assessment satisfying the requirement of Rule 5A.1 shall:

(1) contain a series of five (5) random multiple choice questions with a minimum of five (5) choices each;
(2) require a score of eighty (80) percent or higher to pass;
(3) require the individual to answer all questions in a total time of two (2) minutes or less;
(4) allow any individual who fails the assessment to take a second assessment with different questions than those in the first assessment; and
(5) return as part of the assessment a "pass" or "fail" score as well as a transaction identification number that is unique to the identification verification session.

(b) An identity verification provider that offers the services of a dynamic knowledge-based authentication assessment shall ensure that only the principal whose identity is being verified is shown the questions and that the assessment is protected in an encrypted session.

(c) The principal shall bear the cost of the dynamic knowledge-based authentication assessment described in this Rule.

(d) The result of the dynamic knowledge-based authentication assessment and the transaction identification number shall be recorded in the notary's journal.

*Explanatory Note*

Rule 5A.2 sets the requirements for use of dynamic knowledge-based authentication (DKBA) as a means of achieving satisfactory evidence of identity for remote electronic notarizations. DKBA qualifies as an "identity proofing" under the RULONA (*see* RULONA § [14A(2)]). Rule 5A.2 is based upon Model 1 Rule in Appendix II (where *see* Comment).

**Rule 5A.3 Communication Technology Permitted.**

A notary public may perform an electronic notarial act by means of communication technology in compliance with this Chapter for a principal who is located outside the United States if:

(1) the act is not prohibited in the jurisdiction in which the principal is physically located at the time of the act; and
(2) 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 territorial jurisdiction of the United States, or a transaction substantially connected with the United States.

*Explanatory Note*

MENA Section 5A-2 both conforms with and departs from RULONA Section [14A.] MENA Section 5A-2(3) is substantively congruent with RULONA Subparagraphs [14A(b)(2)] and [14A(b)(4)]. MENA Sections 5A-

2(1) and (2), however, allow remote electronic notarizations to be performed for individuals located in the enacting jurisdiction or elsewhere in the United States, while RULONA Section [14A(b)] limits remote notarizations to individuals located outside of the United States. Therefore, the scope of Rule 5A.3 is limited to these individuals.

**Rule 5A.4 Requirements for Communication Technology.**

(a) A notary public who performs an electronic notarial act for a principal by means of communication technology shall:
  (1) be located within this [State] at the time the electronic notarial act is performed;
  (2) execute the notarial act in a single recorded session that complies with Rule 5A.5 of this Chapter;
  (3) verify the identity of the principal by means of personal knowledge or satisfactory evidence in compliance with Rule 5A.1 of this Chapter;
  (4) be satisfied that any record that is signed, acknowledged, or otherwise presented for notarization by the principal is the same record signed by the notary;
  (5) be satisfied that the quality of the communication technology transmission is sufficient to make the determinations required for the electronic notarial act under these [Rules] and other law of this [State]; and
  (6) identify the venue for the electronic notarial act as the jurisdiction within this [State] where the notary is physically located while performing the act.

(b) In addition to the provisions of Chapter 3 of these [Rules], a tamper-evident technology used to perform notarial acts by means of communication technology shall:
  (1) require the notary public, the principal, and any required witness to access the technology through an authentication procedure that is reasonably secure from unauthorized access;
  (2) enable the notary public to verify the identity of the principal and any required witness by means of personal knowledge or satisfactory evidence of identity in compliance with [statute enacting RULONA Section [14A(d)]] and Rule 5A.1;
  (3) provide reasonable certainty that the notary public, principal, and any required witness are viewing the same electronic record and that all signatures, changes, and attachments to the electronic record are made simultaneously by sight and sound; and
  (4) be capable of creating, archiving, and protecting the audio-video recording and of providing public and official access, inspection, and copying of this recording as required by Rule 5A.5(a).

*Explanatory Note*

RULONA Section [14A(j)] allows the commissioning officer or agency to adopt rules to "prescribe the means of performing a notarial act involving communication technology with an individual located outside of the United States." MENA Section 5A-4 has been substantively adopted in Rule 5A.4 to implement RULONA Section [14A(j)].

In addition, since RULONA Subsections [14A(i)] and [14A(j)(2)] make clear that the commissioning officer or agency may establish standards for approval of communication technology, the rules in MENA Section 5A-4(b) for electronic notarization systems that utilize audio-video communication also have been included in Rule 5A.4.

**Rule 5A.5 Recording of Audio-Video Communication.**

(a) A notary public shall create an audio-video recording of every notarial act performed by communication technology, and provide for public and official access, inspection, and copying of this recording.

(b) A notary public who uses a tamper-evident technology to create the audio-video recording required by this Rule shall enable the provider to perform the functions prescribed by Rule 5A.4(b)(4).

(c) The audio-video recording required by this Section shall be in addition to the journal entry for the electronic notarial act required by [statute codifying RULONA Section [19]] and shall include:
   (1) at the commencement of the recording, a recitation by the notary public of information sufficient to identify the notarial act;
   (2) a declaration by the principal that the principal's signature on the record was knowingly and voluntarily made; [and]
   (3) all actions and spoken words of the principal, notary public, and any required witness during the entire notarial act[.][; and
   (4) at the discretion of the principal, an accurate and complete image of the entire record that was viewed and signed by the principal and notary public.]

(d) The provisions of Rules 9.4, 9.5, and 9.6, related respectively to security, inspection and copying, and disposition of the journal shall also apply to security, inspection and copying, and disposition of audio-video recordings required by this Section.

*Explanatory Note*

RULONA Subsection [14A(j)(4)] authorizes rule-making for the retention of this recording required under Section [14A(g)]. Section 27(a), however, more broadly authorizes rules for the *entire* Act. Therefore, Rule 5A.5 provides more comprehensive rules for all matters related to the audio-video recording, and not just the retention of it.

Rule 5A.5(d) applies three provisions in MENA Chapter 9 for the journal of notarial acts to the audio-video recording of a notarial act — security,

inspection and copying, and disposition. The substantive rules for these provisions are found in Rules 9.4, 9.5 and 9.6.]

## Chapter 6 — Electronic Notarial Certificate

**Rule 6.1 Completion of Electronic Notarial Certificate.**

(a) For every notarial act performed with respect to an electronic record, a notary public shall complete an electronic notarial certificate that complies with the requirements of these [Rules].

(b) An electronic notarial certificate shall be completed at the time of notarization and in the physical presence of the principal [or during the single recorded session required by Rule 5A.4(a)(2) for any notarial act performed using communication technology].

*Explanatory Note*

Rule 6.1 reinforces RULONA Section 15. Subsection (a) requires completion of an electronic notarial certificate for every notarization performed with respect to an electronic record. Subsection (b) clarifies RULONA Section 15(a)(1) — a certificate must be completed "contemporaneously" with the act. It requires the certificate to be completed at the time of notarization and in the physical presence of the notary, or during the single recorded session of the act performed using communication technology under Section [14A].

**Rule 6.2 Form of Electronic Notarial Certificate.**

[(a)] An electronic notarial certificate shall include a venue for the notarial act and shall be in a form as set forth in [statute codifying RULONA Section 16].

[(b) A certificate for a notarial act performed by means of communication technology shall be in a form as set forth in [statute codifying RULONA Section [14A(h)].]

*Explanatory Note*

Rule 6.2 points to the statute containing the RULONA short-form certificates for notarial acts performed on tangible and electronic records. For notarial acts performed by means of communication technology, Rule 6.2(b) points to the statute enacting RULONA Section [14A(h)].

## Chapter 7 — Electronic Signature and Seal of Notary Public

**Rule 7.1 Certification of Notarial Act with Respect to Electronic Record.** A notary public shall sign each electronic notarial certificate with an electronic signature that complies with Rule 7.2 and authenticate a notarial act with respect to an electronic record with an official stamp that complies with Rule 7.3.

**Rule 7.2 Electronic Signature of Notary.**

(a) A notary public shall use a tamper-evident technology that complies with Chapter 4 of these [Rules] to produce the notary's electronic signature in a manner that is capable of independent verification.

(b) A notary public shall take reasonable steps to ensure that no other individual may possess or access a tamper-evident technology in order to produce the notary's electronic signature.

(c) A notary public shall keep in the sole control of the notary all or any part of a tamper-evident technology whose exclusive purpose is to produce the notary's electronic signature.

(d) For the purposes of this Section, "capable of independent verification" means that any interested person may confirm through the [commissioning official or agency] that a notary public who signed an electronic record in an official capacity had authority at that time to perform notarial acts with respect to electronic records.

*Explanatory Note*

RULONA Section 20(a) requires a notary public to use a "tamper-evident technology" in performing a notarial act on an electronic record while MENA Section 7-2 requires the notary's electronic signature to be affixed by means of an electronic notarization system. Rule 7.2 adapts this rule by substituting "electronic notarization system" with "tamper-evident technology."

The justification for including MENA Sections 7-2(b) and 7-2(c) in Rule 7.2 is that these provisions help to "prevent fraud or mistake in the performance of notarial acts" (*see* RULONA § 24(a)(5)) by preventing unauthorized individuals from using a tamper-evident technology to produce a notary public's electronic signature in the notary's name.

**§ 7-3 Official Stamp of Notary.**

(a) An official stamp of a notary public used to authenticate a notarial act with respect to an electronic record shall contain the information required by [statute codifying RULONA Section 17]. If an electronic notarial certificate contains the signature of the notary public, date of the notarial act, venue for the notarial act, and notary public's title, an official stamp may be used to authenticate a notarial act with respect to an electronic record.

(b) The official stamp of a notary public may be a digital image that appears in the likeness or representation of a traditional physical notary public official stamp.

(c) The stamping device of a notary public shall not be used for any purpose other than performing notarizations with respect to electronic records under [statute enacting the RULONA] and these [Rules].

(d) Only the notary public whose name and registration number appear on a stamping device shall generate an official stamp.

*Explanatory Note*

In Rule 7.3, the MENA term "electronic seal" has been replaced with "official stamp." Instead of listing the information required in the official stamp, Rule 7.2(a) points to the statute codifying RULONA Section 17.

Rule 1.2(a)(3) is the basis for incorporating MENA Section 7-3(d) in Rule 7.3(d). In Rule 7.2(c) and (d) the RULONA term "stamping device" is used to clarify it is the electronic tool that creates an official stamp.

## Chapter 8 — Identification of Principals

Rules implementing MENA Chapter 8 have been omitted since the RULONA contains specific provisions for identification of principals for notarial acts. For the identification rules that apply specifically to notarial acts performed by communication technology, see Rule 5A.1.

## Chapter 9 — Journal of Notarial Acts

**Rule 9.1 Journal of Notarial Acts Required.**

(a) A notary public shall record each notarial act in a chronological journal at the time of notarization in compliance with [statute codifying RULONA Section [19]] and this Chapter.

(b) The fact that the notary public's employer or contractor keeps a record of notarial acts shall not relieve the notary of the duties required by this Chapter.

(c) For the purposes of this Chapter, "notarial acts" includes any act that a notary public may perform under this [statute codifying RULONA Section 2(5)] or other law of this [State].

*Explanatory Note*

Rule 9.1 omits MENA Section 9-1(b), allowing notaries to maintain multiple journals at a time, since RULONA Section [19(b)] takes the position that notaries may keep only one journal at a time.

In citing RULONA Section 2(5), Subsection (c) clarifies that a notary public must maintain a journal for all notarial acts, and not only acts performed with respect to electronic records.

**Rule 9.2 Format of Journal of Notarial Acts.**

(a) The journal of a notary public shall be:

(1) a permanently bound book with numbered pages;

(2) any journal in compliance with Section [_____] of [_____] or allowed by custom in this jurisdiction; or

(3) an electronic journal as set forth in this Chapter.

(b) The requirements for journals of notarial acts set forth in this Chapter shall apply also to electronic journals.

*Explanatory Note*

MENA Section 9-2 provides three options for the format of a journal of notarial acts. The first and third are consistent with RULONA Section [19(b)].

**Rule 9.3 Requirements of Electronic Journal.**

An electronic journal shall:

(1) enable access by a password or other secure means of authentication;

(2) be tamper-evident;

(3) create a duplicate record as a backup; and

(4) be capable of providing tangible or electronic copies of any entry made in the journal.

*Explanatory Note*

Rule 9.3 provides rules specific to electronic journals. They address accessing an electronic journal (Subparagraph (1)), making the journal tamper-evident (Subparagraph (2)), creating a back-up record of the electronic journal (Subparagraph (3)), and creating copies of entries in the journal (Subparagraph (4)).

The provision requiring the capture and storing of an electronic signature or the data related to a recognized biometric identifier from MENA Section 9-3(4) and the definition of "biometric identifier" in MENA Section 9-3(b) have been omitted. RULONA Section [19(c)] does not require a signature or biometric identifier for a journal entry.

**Rule 9.4 Security of Journal.**

(a) A notary public shall safeguard the journal and all other notarial records, and surrender or destroy them only by rule of law, by court order, or at the direction of the [commissioning officer or agency].

(b) When not in use, the journal shall be kept in a secure area under the sole control of the notary public.

(c) A notary public shall not allow the notary's journal to be used by any other notary, nor surrender the journal to an employer upon termination of employment.

(d) An employer shall not retain the journal of an employee who is a notary public when the notary's employment ceases.

*Explanatory Note*

MENA Section 9-5(a), (b), and (c) have no counterpart in RULONA Section [19] but are included in Rule 9.4 because they provide helpful rules

on the surrender, security, and exclusive use of a notary journal. MENA Section 9-5(d), prohibiting an employer from retaining a notary's journal, has been added. MENA Section 9-5(e) mirrors RULONA Section [19(d)], and has been omitted.

**Rule 9.5 Inspection and Copying of Journal.**

(a) Any person may inspect or request a copy of an entry or entries in the notary public's journal, provided that:
  (1) the person specifies the month, year, type of record, and name of the principal for the notarial act, in a signed tangible or electronic request;
  (2) the notary does not surrender possession or control of the journal;
  (3) the person is shown or given a copy of only the entry or entries specified; and
  (4) a separate new entry is made in the journal, explaining the circumstances of the request and noting any related act of copy certification by the notary.

(b) A notary who has a reasonable and explainable belief that a person requesting information from the notary's journal has a criminal or other inappropriate purpose may deny access to any entry or entries.

(c) The journal may be examined and copied without restriction by a law enforcement officer in the course of an official investigation, subpoenaed by court order, or surrendered at the direction of the [commissioning officer or agency].

*Explanatory Note*

RULONA Section [19] does not contain rules for inspection and copying of the journal. Rule 9.5 articulates the policy that the journal exists for the benefit of principals and any other parties relying on the records, and not just the notary public. MENA Section 9-6 in its entirety has been incorporated into Rule 9.5.

**Rule 9.6 Disposition of Journal.**

(a) A notary public shall follow [statutes codifying RULONA Sections [19(a)], [(e)], and [(f)]] related to the retention and disposition of the journal.

(b) The personal representative or guardian of a notary public shall follow [statute codifying RULONA Section [19(g)] related to the disposition of the notary public's journal upon the death or adjudication of incompetency of the notary public.

(c) The notary public, or the notary's personal representative, shall provide access instructions to the [commissioning official] for any electronic journal maintained or stored by the notary, upon commission resignation, revocation, or expiration without renewal, or upon the death or adjudicated incompetence of the notary.

*Explanatory Note*

Rule 9.6 defers to RULONA Section [19] for rules related to the retention and disposition of the notary public's journal. The corresponding provisions in the MENA are similar. MENA Section 9-7(d) is retained as Rule 9.6(c) since there is no corresponding provision in RULONA Section [19]. The same standards that relate to the retention and disposition of the journal apply equally to the recording of the audio-video communication under Rule 5A.5(d).

## Chapter 10 — Fees for Electronic Notarial Acts

**Rule 10.1 Maximum Fees.**

(a) The maximum fee that may be charged by a notary public for performing a notarial act with respect to an electronic record may be no more than the amount specified in [statute on maximum fees].

(b) The fee authorized under [statute on maximum fees] includes the reasonable cost associated with using or accessing an electronic system [and, when applicable, an audio-video communication session].

**Rule 10.2 Travel Fee.**

In addition to the maximum fee for performing a notarial act with respect to an electronic record, a notary public may charge a fee for traveling to perform such an act [in the same manner as allowed by this [State] for travel to perform a non-electronic act, as set forth in Section [____] in [_____]] OR [if the notary and the person requesting the electronic notarial act agree upon the travel fee in advance of the travel, and the notary explains to the person that the travel fee is both separate from the maximum fee for the notarial act allowed by law and neither specified nor mandated by law].

*Explanatory Note*

Rule 10.2 authorizes a fee for travel to perform a notarial act with respect to an electronic record. It permits two options. Option 1 points to the applicable rule in a jurisdiction's notary code. Option 2 may be adopted as the rule if a jurisdiction does not have a specific authorization.

**Rule 10.3 Copying Fee.**

A notary public may charge a reasonable fee pursuant to Rule 9.5 to recover any cost of providing a copy of an entry in the journal of notarial acts [or of a recording of a communication technology session pursuant to Rule 5A.5].

*Explanatory Note*

Rule 10.3 authorizes a notary to recover the cost of providing a copy of an entry in the notary's journal. It also allows the notary to charge a fee for

providing a copy of the recording of a notarial act performed by means of communication technology. In both instances, the fee must be "reasonable."

## Chapter 11 — Authenticity of Notarial Act with Respect to Electronic Records.

**Rule 11.1 Evidence of Authenticity.**

(a) Electronic evidence of the authenticity of the electronic signature and official stamp of a notary public of this [State] who has notified the [commissioning officer or agency] that the notary intends to perform notarial acts with respect to electronic records, if required, shall be in the form of:
   (1) an electronic Apostille in compliance with the Hague Convention Abolishing the Requirement of Legalization for Foreign Public Documents of October 5, 1961, if the electronic record is exchanged between nations that are party to the Convention; or
   (2) an electronic certificate of authority signed by the [commissioning officer or agency] of this [State].

(b) The electronic Apostille or certificate of authority described in this Section shall be attached to, or logically associated with, the electronically notarized record in a manner that produces evidence of any changes after it has been issued.

**Rule 11.2 Certificate of Authority.**

Unless otherwise stipulated by law or treaty, an electronic certificate of authority evidencing the authenticity of the electronic signature and official stamp of a notary public of this [State] who has notified the [commissioning officer or agency] that the notary intends to perform notarial acts with respect to electronic records shall be in substantially the following form:

Certificate of Authority for an Electronic Notarial Act

As _____(title of [commissioning official]) of the _____ (name of [State]), I, _____(name of [commissioning official]), hereby certify that _____, the individual named as notary public in the attached or logically associated electronic record, has notified this office of the notary's intent to notarize electronic records and was authorized to act at the time and place the notary signed and sealed the electronic record.

To authenticate this Certificate of Authority for an Electronic Notarial Act, I have included herewith my electronic signature and seal of office this ___day of _____, 20__.

*Explanatory Note*

While RULONA Section 14(e) describes the means for issuing

authentications for a foreign notarial officer who performed a notarial act in a foreign state, the RULONA does not provide explicit provisions for competent authorities of U.S. jurisdictions to authenticate the notarial acts of its notaries on tangible or electronic records for use in foreign nations abroad.

RULONA Section 27(a)(3) permits rules that "include provisions to ensure integrity in the creation, transmittal, storage, or *authentication* of electronic records or signatures" (emphasis added). If a jurisdiction has enacted RULONA Section 27(a)(3), the provisions of MENA Chapter 11 can provide a helpful framework and for issuing these authentications.

## Chapter 12 — Changes of Status of Notary

**Rule 12.1 Change of Registration Information.**
Any change to the information submitted by a notary public in notifying the [commissioning officer or agency] of the notary's intent to perform notarial acts with respect to electronic records in compliance with Rule 3.4 shall be reported within [five] business days to the [commissioning officer or agency].

**Rule 12-2 Termination or Suspension of Authorization.**

(a) Any revocation, resignation, expiration, or suspension of the commission of a notary public terminates or suspends any authorization to notarize electronic records.
(b) The [commissioning official or agency] may terminate or suspend the authorization to perform notarial acts with respect to electronic records of a notary public who fails to comply with these [Rules].
(c) A notary public may terminate the authorization to notarize electronic records and maintain the underlying notary public commission.
(d) A notary public may terminate the authorization to notarize electronic records by notifying the [commissioning officer or agency] of that fact by means approved by the [commissioning officer or agency] and disposing of all or any part of a tamper-evident technology in the notary's sole control whose exclusive purpose was to perform notarial acts with respect to electronic records.

*Explanatory Note*

As discussed in Chapter 2, RULONA Section 20(b) requires a notary public to notify the commissioning officer or agency of his or her intent to perform notarial acts on electronic records. It provides no rules for the notification process itself or any subsequent responsibility of a notary to inform the commissioning officer or agency of changes in status. The provisions of MENA Chapter 12 add these duties and should be considered for inclusion in a rule implementing RULONA Section 20(b).