THE

MODEL ELECTRONIC NOTARIZATION ACT

January 2017

Published As A Public Service

By The

NATIONAL NOTARY ASSOCIATION

A Non-Profit Educational Organization

Model Electronic Notarization Act Review Committee

The Model Electronic Notarization Act Review Committee comprised public-spirited individuals who generously contributed their time and expertise. No part of the Model Electronic Notarization Act necessarily has been approved by every individual, organization, or agency represented on the Committee. The Committee does not lobby for adoption of the Act. The organizations cited below were represented by Committee members at the time of their participation and are not necessarily their current affiliations.

William A. Anderson*
Vice President, Government Affairs
National Notary Association

Richard Bramhall
Chief Underwriting Counsel
Westcor Land Title Insurance Company

Kathleen Butler
Executive Director
American Society of Notaries

Ray Callahan
Chief Ethics & Compliance Officer
Prospect Mortgage, LLC

Michael Chodos
General Counsel
Notarize.com

John Cole
Electronic Notary Public
Commonwealth of Virginia

Michael L. Closen
Professor Emeritus
The John Marshall Law School

The Honorable Catherine Cortez Masto
Attorney General
State of Nevada

Joan Decker
Commissioner, Department of Records
City of Philadelphia, Pennsylvania

William Denny
Senior Deputy District Attorney (Retired)
Alameda County, California

Charles N. Faerber*
Vice President, Notary Affairs
National Notary Association

William Fritzlen
Attorney-Advisor
U.S. Department of State

Harry Gardner
Executive Vice President of eStrategies
Docutech Corporation

Richard Geisenberger
Chief Deputy Secretary of State
State of Delaware

Tom Heymann
President and Chief Executive Officer
National Notary Association

Patrick Honny
Executive Director
Calif. Electronic Recording Transaction Network

Daniel Lewis
Notary Public
State of Indiana

The Honorable Elaine Marshall
Secretary of State
State of North Carolina

Stephen Mason
Barrister
The Hon. Society of the Middle Temple, England

Darcy Mayer
Chief Technology Officer
DocVerify

Steve McDonald
National Accounts Director
Simplifile

Malcolm L. Morris**
Dean and Professor of Law
Atlanta's John Marshall Law School

Timothy Reiniger
Information Risk Governance Law Counsel
FutureLaw, LLC

Bob Rice
Chief Executive Officer
World Wide Notary

Kathy Sachs
Deputy Assistant Secretary of State
State of Kansas

Carol Salter
Physician Integration Program Director
Banner Health

Thomas Smedinghoff
Of Counsel
Lock Lord, LLP

Mike Smith
Communications Director and Compliance Officer
Ga. Superior Court Clerks' Co-op. Authority

Alicia Stewart
Manager, Notary Public & Special Filings Section
California Secretary of State

Deborah M. Thaw
Executive Vice President
National Notary Association

Milt Valera
Chairman
National Notary Association

Terry Van Bibber
Founder and Chief Executive Officer
SafeDocs

Elaine Wright
Notary Public
State of Maryland

* Drafting Co-Coordinator
** Reporter

Foreword

Purpose

The Model Electronic Notarization Act ("MENA") of 2017 is a comprehensive standard and guide for public officials who are establishing rules to govern the notarization of electronic records. It also is the fifth state-of-the-art model act to regulate the performance of notarial acts that has been created and contributed to the public domain by the National Notary Association ("NNA") over the past half century. These five NNA models wed proven best-practice rules for reliable authenticity and fraud deterrence to the high ethical norms expected of an impartial public officer.

The Association's Uniform Notary Act of 1973 — created in a special collaboration with Yale Law School — and its Model Notary Acts of 1984, 2002 and 2010 have been used by legislators and notary-regulating officials around the nation as part of notary law reform efforts in more than 40 states and three U.S. territories. In some of these jurisdictions, only selected key sections of an NNA model were adopted. (*See, for example,* N.M. STAT. ANN. §§ 14-12A-2A and 14-12A-2F, providing definitions of "acknowledgment" and "jurat.") In other jurisdictions, virtually the entire comprehensive NNA model was adopted verbatim. (GUAM CODE ANN. tit. 5 ch. 33, "Model Notary Law.") The NNA model acts have been enacted as law (AMER. SAMOA CODE ANN. §§ 31.0301 through 31.0366), adopted by administrative rule (MISS. ADMIN. CODE tit. 25 ch. 33, "Notaries Public"), and put into effect by gubernatorial executive order (MASS. EXEC. ORDER 455 (04-04); and R.I. EXEC. ORDER 09-08).

The National Notary Association's Model Notary Acts of 2002 and 2010 introduced the first set of systematic and comprehensive rules for electronic notarization in the United States. Whereas both the Uniform Law Commission's widely-enacted Uniform Electronic Transactions Act ("UETA") of 1999 and the similar federal Electronic Signatures in Global and National Commerce Act ("E-SIGN") of 2000 (15 U.S.C.A. §§ 7001 *et seq*.) recognized the legal efficacy of electronic signatures and notarizations, neither established standards for performing these acts. Article III of the NNA's 2002 and 2010 acts addressed that need. The ground-breaking rules adopted procedures that mirrored those provided in Articles I and II of the model acts for paper-based notarizations. The primary objective was to ensure that electronically notarized records would be as trustworthy and fraud-free as their paper-based counterparts.

The 2010 Model Notary Act required notaries to use fraud-deterrent electronic tools and techniques of unmatched potency for its time — *e.g.*, rendering an electronically notarized record "tamper evident" — to ensure not only the authenticity but also the integrity of notarized electronic records. This innovative approach provided notaries a powerful defense to combat fraud in electronic transactions. The Model Electronic Notarization Act of 2017

expands and updates the electronic provisions of the 2010 Model Notary Act, reflecting the evolving developments and demands of technology, business and government.

The primary intended purpose of the MENA is to set forth a progressive model for state and territorial officials to weave electronic notarization provisions into an existing paper-based regime in order to form an integrated, single system for both electronic and non-electronic notarial acts. It is designed to be implemented either as a "plug-in" update or complete replacement for Article III of the Model Notary Act of 2010.

To accomplish its goal, the MENA prompts lawmakers to make pertinent existing statutes or regulations governing paper-based notarizations apply to electronic notarizations as well. (*See, e.g.,* Section 5-2, "Applicability of Other Laws and Rules".) In Subparagraphs 5-2(2) and 5-2(3), lawmakers are given the additional option of replacing any outdated paper-based rules that relate to the important notarial processes of signer identification and journal maintenance. (*See* Chapters 8 ("Identification of Principals") and 9 ("Journal of Notarial Acts").) Further, a "Note To Legislators" immediately following Section 5-2 reads: "If law in your jurisdiction does not provide rules for subparagraphs (1) through (9) above, you may choose to adopt provisions from the National Notary Association's Model Notary Act of 2010." This Note evidences the MENA drafters' position that adopting rules for electronic notarizations provides an opportunity for a jurisdiction to modernize, strengthen and unify all of its notarization rules, both electronic and non-electronic.

Drafting Process

The National Notary Association empaneled a review committee of distinguished individuals from the business, governmental, legal and digital technology communities. A wide range of industries and agencies that handle or generate notarized documents was represented.

A series of draft documents was disseminated to the committee for comments. The resulting observations and critiques were integrated into the final draft by an executive subcommittee. The subcommittee then reviewed the edited document and made appropriate changes to bring it into its final form.

Coincident to this effort, detailed "Comment" sections were written to explain the positions taken by the drafters, as well as to clarify related matters. These sections are not an official part of the proposed legislative text. Principally, the commentary represents the views of the Reporter who drafted it, in conjunction with comments submitted by review committee members and discussions with the other members of the executive subcommittee that produced the final draft.

Challenge of "Remote Electronic Notarization"

The greatest challenge faced by the MENA drafters was deciding whether

the Act should ignore, bar, legitimize or strictly condition "remote electronic notarizations" that are based on the use of advanced "video and audio conference technology." (*See* VA. CODE ANN. § 47.1-2 addressing "satisfactory evidence of identity.") Initially, all rules for electronic notarization inflexibly required face-to-face, physical appearance between the electronic signer and the notary public performing the electronic notarial act. Article III of the NNA's 2010 Model Notary Act adopted that position: "An electronic notary public shall perform an electronic notarization only if the principal…is in the presence of the notary at the time of notarization…" (Section 17-2(1)). Similarly, the National Electronic Notarization Standards adopted by the National Association of Secretaries of State ("NASS") in 2006 and reaffirmed in 2011 and 2016 provided: "A notary public shall not perform an electronic notarization if the document signer does not appear in person before the notary public at the time of notarization" (*see* "Physical Appearance Requirement" § 1). Additionally, over a dozen states published in official handbooks or posted on websites warnings to notaries about the dangers posed to the public by notarizing records electronically without the signer being physically present. The California admonishment is illustrative: "California notaries public are authorized under current law to perform electronic notarizations as long as all the requirements for a traditional paper-based notarial act are met … This means the party must be physically present before the notary public. A video image or other form of non-physical representation is not a personal appearance before a notary…" (www.sos.ca.gov/notary/customer-alert/: "Customer Alert — California Notaries Public Cannot Perform Notarial Services Online"). A number of states enacted statutes explicitly to proscribe electronic notarization without the signer's physical presence (*see, e.g.*, N.C. GEN. STAT. § 10B-116; and W.VA. CODE § 39-4-6).

Virginia, however, took a different tack and in 2012 became the first state to authorize remote electronic notarizations based on video and audio conference technology. (VA. CODE ANN. §§ 47.1-1 through 47.1-30. In 2000, Utah had enacted legislation designed for a similar purpose, but it was repealed as being unworkable (*see* Appendix IV, Utah, S.B. 145, Ch. 312).) The Virginia statute has prompted some voices in government and private industry to consider whether the stringent bans on remote electronic notarization are necessary for the public welfare or merely overprotective measures that will impede innovation.

In 2015, Montana became the second state to enact legislation allowing remote electronic notarizations without physical appearance by the signer before the notary. (MONT. CODE ANN. §§ 1-5-603(7) and 1-5-615.) In 2016, the Uniform Law Commission approved an amendment to its Revised Uniform Law on Notarial Acts authorizing American notaries located *inside* the United States to notarize for signers *outside* the United States via "communication technology." (REV. UNIF. LAW ON NOT. ACTS § [14A(c)]). More recently, the National Association of Secretaries of State has formed a

NASS Remote Notarization Task Force to study the issue and ponder whether to incorporate new standards for remote electronic notarization.

The MENA drafters decided that remote electronic notarization could not be passively ignored in the Act, but neither could it be unconditionally endorsed nor affirmatively banned. There is no doubt that remote electronic notarization can solve certain problems that flow from a signer's lack of geographic proximity to an available notary. It, however, also is clear that remote electronic notarization carries a high potential for fraudulent exploitation and legal challenge unless the governing rules are carefully crafted and enforced. One such requirement would be to use only electronic, as opposed to tangible, records in remote electronic notarizations. The drafters realized they would be remiss in their efforts if remote electronic notarization was not addressed in the model act. Chapter 5A is the product of that decision.

The National Notary Association posits that remote electronic notarization executed via "audio-video communication" only is advisable and in the public interest when governed by rigorous rules to ensure trustworthy notarizations. Chapter 5A and other bracketed portions of the Model Electronic Notarization Act of 2017 were designed to provide that protection.

Brackets and Parentheses

Certain material in the Model Electronic Notarization Act has been put in brackets ("[ ]"). This serves any one of the following five purposes:

1) An indication that a generic term (*e.g.*, "[commissioning official]") has been used. The adopting jurisdiction should here insert appropriate specific terminology that is consistent with its statutory scheme (*e.g.*, "secretary of state").

2) An indication that insertion of a numerical or dollar amount is necessary. If a particular amount is strongly preferred by the MENA drafters, this number will be placed within brackets (*e.g.*, "[$25,000]"); if there is no preference for a particular amount, the brackets will enclose a space containing the words "amount in dollars" ("[amount in dollars]") to be filled in by the legislators adopting the MENA.

3) The need for the lawmakers to fill in the blank space with a pertinent citation (*e.g.*, "…as set forth in [Section 10B-116] of [the North Carolina General Statutes]"). There are many instances in the MENA where reference is made to an existing statute or administrative rule.

4) The need for lawmakers to choose an option when two sets of brackets each enclose lengthier phrases separated by the word "OR" to indicate that a critical choice must be made.

5) To alert lawmakers that a particular topic engendered considerable debate among the MENA drafters, as was the case with Chapter 5A (*i.e.*, "Audio-Video Communication"). The lawmakers have the option of including, excluding or modifying the bracketed material.

For any set of brackets enclosing a section, subsection or subparagraph of

the MENA that prompted debate among the drafters and was left for legislators to decide, a corresponding set of brackets may be found in the Comment. (*See, e.g.*, the bracketed paragraphs in the Comment for Section 2-1(2) pertaining to definition of "appear in person," which accommodate audio-video communication.)

Parentheses ("( )") on cited records and certificates indicate options or instructions for document signers or notaries.

Citations

There are numerous citations throughout the Foreword and Comment sections. All references to the Model Electronic Notarization Act are made merely by citing to the section (*e.g.*, Section 3-4). Standard citation form is used to refer to reported cases and state statutes and regulations, except that publishers and dates of publication for the latter have been eliminated.

Appendices

The Model Electronic Notarization Act contains four appendices which should prove valuable not only to legislators, officials and administrators, but also in private industry to executives, attorneys, technologists, educators and notaries who want to achieve a better understanding of electronic notarization. The appendices and purpose of each are noted below.

Appendix I – Verification of Identities in Online Transactions: Discusses the unique challenge of identifying signers by means of audio-video communication.

Appendix II — Model Rules Implementing MENA Section 5A-5: Responds to MENA Section 15-2, which requires the commissioning official to adopt implementing rules if MENA Section 5A-5 is enacted to allow electronic notarization by audio-video communication.

Appendix III — How to Implement the MENA as an Administrative Rule Under the Revised Uniform Law on Notarial Acts: Explains that the MENA may serve as the administrative rules authorized by the Uniform Law Commission's RULONA that a commissioning official may provide when laws are enacted or adopted to permit notarization of electronic records.

Appendix IV — History of Electronic Notarization Laws: Chronicles the major legislative enactments affecting electronic notarization in the United States since 1996, as well as pertinent regulatory adoptions achieved through administrative rule-making.

Acknowledgements

I would like to thank Charles (Chuck) Faerber, formerly Vice President of Notary Affairs, and William (Bill) Anderson, Vice-President of Government Affairs. They worked tirelessly to ensure the Act maintains the

high standards of diligence and care imposed on notaries in the context of using new technology.

Through his many years working at the National Notary Association, Chuck Faerber became the most knowledgeable person extant on notary rules and procedures. He was the principal draftsman of the Model Notary Acts of 2002 and 2010, as well as a major contributor to the *Notary Public Code of Professional Responsibility*. Many of the concepts and rules of this Act were drawn from Chuck's work on the electronic notarization provisions of the Model Notary Act of 2002, Chapter 16, and the Model Notary Act of 2010, Article III.

Bill Anderson was the laboring oar on the Act. He probably is the leading authority on identification technology needed to provide secure electronic notarizations. That expertise coupled with his thorough understanding of notarial rules and practice used throughout the country enabled him to draft provisions that wed modern technology to traditional procedures to make electronic notarizations secure, trustworthy and practicable. The provisions in the Act that transition notary practice from "pen and paper" to the electronic world are covered with Bill's fingerprints.

It has been my pleasure to work with the men and women of the National Notary Association over the years, and share their hope that this Act will provide the framework for trustworthy and efficient electronic notarizations.

Malcolm L. Morris, Reporter
Dean and Professor of Law
Atlanta's John Marshall Law School

Contents

Chapter 1 — Implementation

Comment

General: This Chapter states the purposes and sets out the applicability of the Model Electronic Notarization Act (hereinafter "the Act"). Section 1-2 is particularly noteworthy because its goals undergird most of the provisions found throughout the Act, and help justify a number of the positions taken. The balance of the Chapter addresses standard legislative matters.

§ 1-1 Short Title.

This [Act] may be cited as the [Model Electronic Notarization Act of 2017].

§ 1-2 Purposes.

This [Act] shall be construed and applied to advance its underlying purposes, which are:

(1) to promote, serve, and protect the public interest;
(2) to modernize the law governing notaries public;
(3) to integrate laws for traditional and electronic notarial acts; [and]
(4) to enhance cross-border recognition of electronic notarial acts[.][; and
(5) to prescribe rules for ensuring the authenticity and integrity of records used in online transactions.]

Comment

Section 1-2 enunciates the overarching purposes of the Act.

Subparagraph (1) places the public's interest above all else. The Act adopts the position that notaries are first and foremost public servants. All notaries public, especially those who perform electronic notarizations, are duty-bound to protect the general public by following the provisions of this Act.

Subparagraph (2) stakes out equally important territory: bringing notarial laws into the 21st century. Some state notary laws cede control of the screening of commission applicants in favor of hallowed but inconsistent county customs (*see, e.g.,* OHIO REV. CODE tit. 1, ch. 147 §§ 147.01 to 147.99), some are quite minimalist (*see, e.g.,* VT. STAT. ANN. tit. 24 §§ 441 to 446), and others a patchwork product of numerous unrelated legislative amendments (*see, e.g.,* CAL. GOV'T. CODE §§ 8200 to 8230 & CAL. CIV. CODE §§ 1181 to 1197). The Act offers a comprehensive statute that addresses and introduces rules for electronic notarizations. The Act makes the effort to detail proper procedures for performing electronic notarial acts. The focus clearly is on ensuring that notaries understand their roles in the new electronic realm. This works toward satisfying the public interest objective set out in Subparagraph (1). The drafters addressed issues principally involving the training and registration of notaries to perform electronic acts and the security and effective performance of those notarizations.

Subparagraph (3) addresses the reality that electronic transactions are becoming more prevalent. The primary goal of the Act is to ensure that workable notarial procedures are in place to accommodate that fact. To this end, the Act is devoted to establishing rules for

electronic notarizations in a statutory scheme that can exist alongside or be integrated with existing notarial statutes.

Subparagraph (4) recognizes the modern reality of cross-border commerce. Principals who migrate from one jurisdiction to another or enterprises that conduct multi-state businesses need to have both tangible and electronic records that are recognized wherever presented. The law regarding recognition of traditional paper-based notarial acts is established (*see* Section 6-3 and Comment). This Act extends this basic recognition to electronic notarial acts.

[Subparagraph (5) states that one major purpose of the Act is to ensure that electronic notarial acts performed remotely by means of audio-video communication are authentic and secure. (*See* Foreword; Section 2-1 and Comment; and Chapter 5A and Comment.)]

§ 1-3 Prospective Effect.

This [Act] shall only apply to electronic notarizations performed on or after the effective date of this [Act].

Comment

Section 1-3 clarifies that the new operating rules of electronic notarization and concomitant obligations must be followed by all notaries immediately, including those who were commissioned prior to the adoption of the Act.

§ 1-4 Interpretation.

In this [Act], unless the context otherwise requires, words in the singular include the plural, and words in the plural include the singular.

Comment

Section 1-4 is a standard provision protecting the Act from a possible pretext for legal challenge. Note that legislators in some jurisdictions may prefer to place this provision at the end of the Act rather than in the Implementation chapter.

§ 1-5 Severability Clause.

If any provision of this [Act] or its application to any person or circumstance is held invalid, the invalidity does not affect other provisions or applications of this [Act] that can be given effect without the invalid provision or application, and to this end the provisions of this [Act] are severable.

Comment

Similar to Section 1-4, Section 1-5 is a standard provision protecting valid portions of the Act from a possible pretext for legal challenge in the event that "severed" portions of the Act have been invalidated.

[§ 1-6 Repeals.

The following acts and parts of acts are hereby repealed:

[_____].

Comment

Section [1-6] recognizes that, in enacting the MENA, legislators may need to amend or repeal existing statutes that are superseded by the Act. It is possible that some existing rules affecting electronic notarization are not inconsistent with the Act, and ought to remain unchanged. This might include rules for registering notaries to perform electronic notarial acts. (*See, e.g.*, N.C. GEN. STAT. 10B-106.)]

§ 1-[6][7] Effective Date.
This [Act] shall take effect [_____].

Comment

Subsection 1-[6][7] provides an effective date for any or all of the provisions of the Model Electronic Notarization Act that are put in place in a given jurisdiction by legislative enactment. A well-considered effective date is an indispensable planning metric for all in government and private industry who will be affected by this important development in commerce and law.

Chapter 2 — Definitions Used in This Act

Comment

General: Chapter 2 provides definitions of terms integral to the process of electronic notarization. Six are closely based on definitions in the UETA or other Uniform Law Commission acts (*viz.*, "electronic," "electronic record," "electronic signature," "record," "security procedure," and "state"). These terms tie the Model Electronic Notarization Act to fundamental understandings of electronic transactions that now permeate state and federal law, through enactments of both the UETA and E-SIGN. Five of the terms ("electronic journal," "electronic notarial act and electronic notarization," "electronic notarial certificate," "principal," and "verification of fact") were defined in the 2002 or 2010 Model Notary Acts but have been amended by the drafters in this Act. New to this Act are the definitions of "appear in person," "credential," "electronic notarization system," "enrollment," "provider," "sole control," "tamper-evident," and "venue."

The Act defines additional terms used exclusively within certain chapters. The definitions of "audio-video communication" and "real-time" have been added to Chapter [5A] and depend on the adoption of that bracketed chapter. (*See* Section [5A-1] and Comment.) The definition of "capable of independent verification" has been added to Chapter 7. (*See* Section 7-2(d) and Comment.) The definitions of "foreign" and "tribal government" have been added to Chapter 8. (*See* Section 8-3 and Comment.) Finally, the definition of "biometric identifier" has been added to Chapter 9. (*See* Sections 9-3 and 9-4 and Comments.)

§ 2-1 Appear in Person.

"Appear in person" 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 audio-video communication in compliance with Chapter 5A of this [Act].]

Comment

Section 2-1 defines "appear in person" to require that a principal (defined in Section 2-12) be in the physical presence of the notary at the time of performing an electronic notarization. (*See* Section 5-3(b).) This is necessary in order for the notary to perform the essential task of determining that the principal is exactly who he or she purports to be. To properly perform this duty (*see* Section 8-2 for rules to determine "satisfactory evidence of identity") — and to make a necessary commonsense judgment that the principal appears to be acting without coercion and with adequate awareness — the notary must be able to question and closely observe the principal. A telephone call or an email message to the notary will not serve this purpose. The notary and principal must be "close enough to see, hear, communicate with, and exchange tangible identification credentials with..." each other.

"Personal appearance" is the fundamental manner in which principals avail themselves of the jurisdiction, authority, and legal power of a notary public as a public officer. (*See, e.g., Colburn v. Mid-States Homes, Inc.*, 266 So.2d 865 (Ala., 1972), *Commonwealth v. Haines*, 97 Pa. 228 (Pa. 1881), *Humble Oil & Refining Co. v. Downey*, 183 S.W.2d 426 (Tex. 1944), and *Yates v. Ley*, 92 S.E. 837 (Va., 1917).)

The majority of states and jurisdictions which allow electronic notarizations today stipulate physical presence of the principal before the notary or prohibit the notary from performing an electronic notarial act when the principal is not present. (*See* IOWA CODE ANN. §§ 9B.6 and 9B.2.10; W.VA. CODE § 39-4-6; and N.C. GEN. STAT. § 10B-116).) Moreover, provisions in four jurisdictions explicitly state that audio-video communication in any form does not qualify as an "appearance" before a notary public. (*See* IOWA CODE ANN. § 9B.2.10; N.C. ADMIN. CODE § 07C.0403; N.M. ADMIN. CODE § 12.9.2.8; and W.VA. CODE § 39-4-6.)

[In 2000, Utah became the first jurisdiction allowing a notarial act to be performed by electronic communication. (UTAH CODE ANN. § 46-1-2 (2000), where "acknowledgment" was defined as "an admission made in the notary's presence or by an electronic communication that is as reliable as an admission made in the presence of the notary, provided that the electronic communication is authorized by law or rule…") This law and its implementing regulation (UTAH ADMIN. CODE R154-10-502 (2001)) were repealed in 2006 and 2008, respectively.

In 2012, Virginia authorized notaries public to use audio-video conference technology to perform electronic notarial acts. (*See* VA. CODE ANN. § 47.1-2 — "satisfactory evidence of identity.") In 2015, Montana enacted a statute allowing notaries to use audio-video communication technology (MONT. CODE ANN. § 1-6-603(7) and § 1-6-615). Another state passed a resolution to study the matter (Louisiana House Concurrent Resolution 218, passed June 10, 2015). Two states introduced similar measures that failed (Texas House Bill 3309 of 2015 and Maryland HB 1111 of 2016).

In July, 2016, the Uniform Law Commission amended its Revised Uniform Law on Notarial Acts to allow signers located outside of the United States to "appear" before a notary public located inside the United States to have their signatures notarized by means of "communication technology." The ULC has also formed a committee to study expanding the scope of such remote notarizations in order to serve principals located in domestic jurisdictions as well as foreign.

Personal appearance by means of communication technology has received widespread acceptance as a way of invoking the jurisdiction and authority of federal and state courts. In a number of states, videoconference technology has been deemed trustworthy and reliable in criminal and civil proceedings. (*See* http://www.ncsc.org for a survey. Note also, the discussion of the use of video conferencing for criminal arraignments and parole hearings by the Michigan state correctional facilities in Elaine Pittman, Virtual Justice, GOVERNMENT TECHNOLOGY, January 10, 2011, at 34-5.) In Virginia, for example, standards governing appearance by two-way audio and video communication for courtroom use require that the parties must be able to "simultaneously see and speak to one another" using a live, real-time signal that is secure from unlawful interception. (*See, e.g.*, VA. CODE ANN. § 19.2-3.1B. Note also, pursuant to VA. CODE ANN. § 47.1-13D, the notarial acts performed by means of audio-video communication are deemed to have taken place in

Virginia and under Virginia law.) Where such audio-video conference technology is available, the use of this technology constitutes an "appearance" before "a magistrate, intake officer or, prior to trial, before a judge" and these officers "may exercise all powers conferred by law and all communications and proceedings shall be conducted in the same manner as if the appearance were in person." (*See* VA. CODE ANN. § 19.2-3.1A. *See also,* 725 ILCS § 5/106D-1; MONT. CODE ANN. § 46-7-101; N.C. GEN. STAT. § 15A-601; and W.VA. CODE § 50-4-2a. In the federal courts, *see* 18a U.S.C. Rule 5 for initial appearances upon arrest and 18a U.S.C. Rule 10 for arraignments.)

A fundamental difference between use of audio-video communication by a judge as opposed to by a notary public should be kept in mind. In a criminal judicial proceeding, principals generally are in the custody of law enforcement and their personal identities are typically not issues yet to be resolved; in a notarization, the principal may "walk in off the street" as a complete stranger and personal identity remains very much an unresolved issue to be determined by the notary. In addition, the notary typically does not have access to fingerprint and DNA databases that law enforcement might use to identify a person in custody. Therefore, there generally is more risk attendant a remotely-performed notarial act than in a teleconferenced judicial proceeding.

The items chronicled above compelled the drafters to recognize that advances in teleconferencing technology, as well as identification processes, had satisfied many legislators and public regulators that reliable "remote" screenings of a principal by a notary are possible. The governing rules need to be carefully conceived and dutifully enforced. Therefore, brackets were added to Subparagraph 2-1(b) to recognize that an appearance before a notary public by means of "audio-video communication" in the eyes of some legislators may constitute an additional reliable means of achieving personal appearance and invoking the notary public's powers. Here, as elsewhere in the Act, references to audio-video communication are bracketed to reflect that this new form of personal appearance is an option that legislators in some jurisdictions may decide not to adopt. (*See, e.g.,* Section 6-2(b).)]

§ 2-2 Credential.

"Credential" means a record evidencing an individual's identity.

Comment

The drafters introduced a new definition of "credential" because increasingly the term is used synonymously with "identification document" and also in current usage it may refer either to a tangible or paper identification document (*see* N.J. STAT. ANN. § 5:12-101h.(e)) or an identifying electronic device or process (*e.g.,* the federal Transportation Worker Identification Credential which utilizes biometrics contained in an integrated computer chip housed within the card to identify the bearer). In the Act, it is used for paper credentials (*see* Section 8-2). [It also is used for electronic credentials (*see* Section 5A-1(4).]

§ 2-3 Electronic.

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

Comment

Section 2-3 defines "electronic" consistent with the Uniform Electronic Transactions Act. (*See* UETA § 2(5).) The drafters employed terms that are compatible with the UETA because that act has been adopted by virtually all jurisdictions (*see, e.g.*, GA. CODE ANN. §§ 10-12-1 to 10-12-20; KAN. STAT. ANN. §§ 16-1601 to 16-1620; NEB. REV. STAT. §§ 86-612 to 86-643; UTAH CODE ANN. §§ 46-4-101 to 46-4-503; and ME. REV. STAT. ANN. tit. 10 ch. 1051 §§ 9401 to 9419) or served as the starting point for other legislation enacted throughout the country (*see, e.g.*, CAL. CIV. CODE §§ 1633.1 to 1633.17; ARIZ. REV. STAT. ANN. §§ 44-7001 *et seq.*; MD. CODE ANN. (COM. LAW) §§ 21-101 to 21-1-120; and OHIO REV. CODE ANN. §§ 1306.01 to 1306.23).

The term "electronic" is to be liberally construed to embrace not only computer-generated signatures and records, but also those created by other technologies that may currently be in use or developed in the future.

§ 2-4 Electronic Journal.

"Electronic journal" means a chronological record of notarizations maintained by a notary public in an electronic format in compliance with Chapter 9 of this [Act].

Comment

Section 2-4 has been adopted largely intact from the 2010 version of the Model Notary Act. As with the 2010 Act, the drafters decided to enumerate the specifications for an electronic notarial journal in a separate chapter (*see* Chapter 9), instead of including them in the definition itself.

For the purposes of this section, "record" is used in its ordinary, everyday meaning, and not as it is defined in the UETA or in Section 2-14 of this Act.

§ 2-5 Electronic Notarial Act and Electronic Notarization.

"Electronic notarial act" and "electronic notarization" mean a notarial act or notarization as specified in Section 5-1 of this [Act] that involves an electronic record and that is performed by a notary public as a security procedure in compliance with this [Act].

Comment

Section 2-5 declares that every electronic notarization is itself a "security procedure," whose definition in Section 2-16 is closely based on the definition of the same term in the UETA (*see* UETA § 2(14)). The UETA definition spells out that a security procedure is "employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the information in an electronic record." One of the clear standards that has arisen in the new field of electronic notarization is that an electronic notarial act must qualify as a "security procedure" with the important capabilities of establishing who signed and notarized an electronic record and rendering a notarized electronic record as tamper-evident.

According to George L. Paul *et al.*, FOUNDATIONS OF DIGITAL EVIDENCE, p. 212 (ABA, 2008): "Concerning electronically notarized documents, an international and national e-document authenticity standard has emerged that reflects the evidentiary need for electronic documents to have the capability of authenticity testing. This standard requires that any relying party be able to verify the origin and integrity of the notarized electronic document. Establishing the authenticity of a notarized document thus requires the capability, in perpetuity, of independently authenticating the notary, and verifying whether the content of the electronic document is complete and unaltered." (*See* also NASS NAT'L ELEC. NOT. STAND. § 5-9; ABA SUBCOMMITTEE ON ETRUST: ENOTARY WORKGROUP WHITEPAPER ON ENOTARIZATION at 3.3 (ABA, 2006), stating, "(T)he document being proffered must contain or be accompanied by evidence that it has not changed since it was first generated in its final form"; and Daniel J. Greenwood, ELECTRONIC NOTARIZATION: WHY IT'S NEEDED, HOW IT WORKS, AND HOW IT CAN BE IMPLEMENTED TO ENABLE GREATER TRANSACTIONAL SECURITY at 10 (Nat'l Notary Ass'n, 2006).)

In this Act, at the core of each electronic notarization is the assurance that the notarized electronic record was signed by a particular real individual and that the record will prominently display evidence of any subsequent alteration. In that way, all electronic notarizations are themselves security procedures.

§ 2-6 Electronic Notarial Certificate.

"Electronic notarial certificate" means the part of, or attachment to, an electronic record that is completed by the notary public, bears that notary's electronic signature and seal, and states the facts attested to by the notary in an electronic notarization.

Comment

Section 2-6 recognizes that every notarization, whether paper-based or electronic, requires a notarial certificate. The certificate may be either an integral part of the paper or electronic record or attached to it. The definition of "electronic notarial certificate" reflects the definition of the same term adopted by the National Association of Secretaries of State in 2006, and reaffirmed in 2011 and 2016. (*See* NASS NAT'L ELEC. NOT. STAND., "Definitions" at 7.) An "electronic notarial certificate" is not to be confused with a "public key certificate," which is a component of a technology widely used to create digital signatures.

§ 2-7 Electronic Notarization System.

"Electronic notarization system" means a set of applications, programs, hardware, software, or technologies designed to enable a notary public to perform electronic notarizations.

Comment

The term "electronic notarization system," borrowed from a Florida administrative rule (*see* FLA. ADMIN. CODE § 1N-5.001(4)), is new to the Act. An electronic notarization system is the analogue to the notary's traditional inked

seal and pen. It is the *tool* by which a principal executes an electronic signature and the notary performs the electronic notarial act. An electronic notarization system may be a dedicated, end-to-end solution comprising hardware (for example, a signature pad or public key certificate installed on a physical token or device) and software. Or, it may be software installed in the online environment (a "web application") that is used to perform electronic notarial acts. (*See* Chapter 4 for standards governing electronic notarization systems.)

§ 2-8 Electronic Record.

"Electronic record" means a record created, generated, sent, communicated, received, or stored by electronic means.

Comment

Section 2-8 essentially borrows the definition of "electronic record" from the UETA. (*See* UETA § 2(7).) In the 2002 and 2010 Model Notary Acts, the term "electronic document" was used instead of "electronic record" to strengthen the connection of electronic notarizations to paper-based official acts. In this Act, the drafters adopted "electronic record" to align with the prevailing terms used both in the UETA and the federal E-SIGN Act.

§ 2-9 Electronic Signature.

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

Comment

Section 2-9 essentially borrows the definition of "electronic signature" from the UETA. (*See* UETA § 2(8).) The definition describes the different possible forms of an electronic signature, and is intended to be as inclusive as possible. No doubt, technologies not yet developed will create new ways to produce electronic signatures that would satisfy the definition.

It is important to note that this section only defines what an electronic signature is. Rules that apply to a notary's use of an electronic signature are detailed in Section 7-2. New to this Act is the requirement that an electronic signature produced by a notary be created using an "electronic notarization system." (*See* Section 2-7 and Comment for the definition of "electronic notarization system".)

§ 2-10 Enrollment.

"Enrollment" means a process for registering a notary public to access and use an electronic notarization system.

Comment

Some electronic notarization systems require a notary to set up an account with the system prior to using the system. Typically, these are online systems in which a notary will log onto a website to perform the electronic

notarial act. The enrollment process will assist the notary in creating a profile within the system and assign login credentials to be used by the notary for gaining access to the system. When a notary is requested to perform an electronic act, the notary will present the credentials in order to access the system.

§ 2-11 Personal Knowledge and Personally Knows.

"Personal knowledge" and "personally knows" mean familiarity with an individual resulting from interactions with that individual over a period of time sufficient to dispel any reasonable uncertainty that the individual has the identity claimed.

Comment

Section 2-11 provides a definition of the critical concept of personal knowledge of identity. Although most notarizations will be based upon identification through evidentiary means (*see* Section[s 5A-5 and] 8-2), sometimes it may be necessary to base identity on a notary's personal familiarity with another individual. Personal knowledge is a necessary element of the chain of proof when a sole credible witness is used. (*See* Subparagraph 8-2(a)(2).) The Act provides a rule of reason for determining personal knowledge. (*See Anderson v. Aronsohn*, 63 CAL. APP. 737, 740 (1923), which deals with the nature of personal knowledge of identity, stating that "the degree of acquaintance which would authorize a notary to certify that he had personal knowledge involves something more than mere casual meetings, and must be based upon a chain of circumstances surrounding the person tending to show that he is the party he purports to be.")

The definition does not quantify the number of interactions nor the duration of a time of acquaintance sufficient to convince a notary that an individual has a claimed identity. This is left to the notary's best judgment. The drafters, however, firmly believed that any reasonable doubt on the part of the notary about whether a signer is "personally known" must instead result in reliance on acceptable identification credentials or on at least one credible witness.

Amendments to a California law (CAL. CIV. CODE § 1185) in 2007 removed the authorization for notaries to rely on personal knowledge to identify principals or credible witnesses in the performance of notarial acts. These changes were enacted at the behest of the California law enforcement community, which perceived an overly liberal interpretation of "personal knowledge" as the basis for too many false identifications by notaries. The result, prosecutors complained, was a lack of recorded evidence in notary journals (*e.g.*, identification credential serial numbers) that might be useful in investigating criminal acts of forgery. The drafters decided not to take away from notaries the valuable option of using personal knowledge as the basis for an identification. Instead, they encourage notaries to supplement any journal notation that a signer was "personally known" with information from an identification credential of the signer that might later be useful to law enforcement.

§ 2-12 Principal.

"Principal" means:

(1) an individual whose electronic signature is notarized in an electronic

notarization; or

(2) an individual taking an oath or affirmation from the notary public, but not in the capacity of a credible or other witness for the electronic notarial act.

Comment

Section 2-12 defines a term used throughout the Act — principal. The drafters determined that it made sense to identify the person using the services of a notary as a principal. It simplifies the statute and ends ambiguities with respect to witnesses or other parties who may have dealings with a notary, but are not seeking the performance of a notarial act for themselves (*e.g.*, an individual asking a notary to serve a bedridden elderly parent).

§ 2-13 Provider.

"Provider" means an individual or entity that offers the services of an electronic notarization system.

Comment

The "provider" may be a live person or a legal entity (*e.g.*, corporation, partnership, LLC) owning, offering, or operating an electronic notarization system.

§ 2-14 Record.

"Record" means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

Comment

The definition of "record" is borrowed from the UETA. (*See* UETA § 2(13).) It encompasses "tangible" (*e.g.*, paper) and electronic records. As is done in the UETA, in this Act the term "electronic record" is chosen when the context refers explicitly to a record kept in electronic form. There are instances in this Act when a "record" is clearly "tangible." (*See* the definition of "credential" in Section 2-2 and Section 8-2 where "tangible" identification credentials are presented.)

§ 2-15 Satisfactory Evidence of Identity.

"Satisfactory evidence of identity" means evidence authorized under Chapter[s 5A and] 8 of this [Act] to verify that an individual has the identity claimed.

Comment

In Section 2-15, "satisfactory evidence of identity" is any evidence that is expressly authorized for a notary public to use in verifying the identity of a principal for an electronic notarial act. Chapter 8 provides rules for satisfactory evidence of identity when used in electronic notarizations performed in the physical presence of the notary. [Chapter 5A provides rules for satisfactory evidence of

identity in electronic notarizations when the principal is appearing before the notary by means of audio-video communication.]

§ 2-16 Security Procedure.

"Security procedure" means a procedure employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the information in an electronic record. The term includes a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, or callback, or other acknowledgment procedures.

Comment

Section 2-16 adopts the definition of "security procedure" provided in the UETA (*see* UETA § 2(14)).

One of the prime innovations of this Act is applying the function of a security procedure as defined in the UETA to electronic notarization. (*See* Section 2-5 and Comment.) There is congruence in the two processes. Indeed, the Comment for UETA § 2(14) states: "A security procedure may be applied to verify an electronic signature, verify the identity of the sender, or assure the informational integrity of an electronic record." Verification of an electronic signature and the identity of the signer arguably are two key components to any electronic notarization. In addition, the drafters believe that the phrase "acknowledgment procedures" in the definition can relate to the notarial act of an "acknowledgment."

§ 2-17 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.

Comment

Section 2-17 adopts in substance the corresponding definitions in the administrative rules of Florida and North Carolina. (FLA. ADMIN. CODE § 1N-5.001(8); and 18 N.C. ADMIN. CODE §§ 07C.0102(9) and (10).) A notary may affix an electronic signature using a physical token or an electronic notarization system that is accessed through standard login credentials (user name and password). Thus, the notary could be required to maintain "direct physical control" of the token that is used to create the electronic signature or simply ensure that the login credentials to any system not under the notary's direct physical control are not compromised. "Other secure means of authentication" could include existing technologies such as biometrics (*e.g.*, fingerprint, retinal or facial scans) or ones developed in the future.

§ 2-18 State.

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

Comment

The definition of "state" is borrowed from the Uniform Law Commission's definition that appears in many of its acts. (*See, for example,* REV. UNIF. LAW ON NOT. ACTS § 2(14) and UNIF. POWER OF ATTY. ACT § 102(13).) In this Act, "state" usually is bracketed as a referent to the enacting state or other jurisdiction. "State" does not include a federally recognized tribal government. (*See* Section 8-2 where "tribal government" is defined for use in that Section.)

§ 2-19 Tamper-Evident.

"Tamper-evident" means that any change to a record shall provide evidence of the change.

Comment

"Tamper-evident" has been adopted in the electronic signature and transactions industry as well as in law as a term of art. (For an example of the latter, *see* REV. UNIF. LAW ON NOT. ACTS § 20(a).) The term is more all-inclusive than the narrower negative connotations that the word "tamper" suggests. Certainly, "tamper-evident" refers to any illegal attempt by an individual to make unauthorized changes to a record, but the term may also be used to refer to "any" changes to a record — authorized or not. The changes, which may include amendments to the text of the record, addition of one or more principals' electronic signatures, or the notary public's electronic signature and seal, may be catalogued and time-stamped at the moment of occurrence in an audit trail comprising all actions taken with respect to the record. Thus, all changes are "evident" but it is ultimately up to the transacting parties relying upon the record, or a court, to determine whether a given action or change is authorized or unauthorized.

Tamper-evident does not mean "tamper-proof." A tamper-proof technology would prevent any changes from being made to the record once applied. In a notarization context, this would be highly undesirable. If a record required multiple principals to sign the record at different times, a "tamper-proof" technology applied after the first signature would prevent the other principals from signing the record later.

§ 2-20 Venue.

"Venue" means the jurisdiction where the notary public is physically located while performing an electronic notarial act.

Comment

In keeping with customary usage in law, in this Act "venue" refers to the jurisdiction where a notary performs an electronic notarial act. (*See* FLA. STAT. ANN. § 117.05(4)(a).) It is usually indicated by the words "State of _____, County of _____" appearing at the top of a notarial certificate.

[§ 2-21 Verification of Fact.

"Verification of fact" means a notarial act in which a notary reviews public

or vital records, or other legally accessible data, to ascertain or confirm any of the following facts:

(1) date of birth, death, marriage, or divorce;
(2) name of parent, marital partner, offspring, or sibling; and
(3) any matter authorized for verification by a notary by other law or rule of this [State].

Comment

Section 2-21 defines a notarial power that may be considered beyond the notary's traditional ministerial role. For that reason, this section is bracketed. Locating, reading, and interpreting legal records is generally regarded as being in the bailiwick of attorneys. Yet, the extraction of certain basic information from public, vital, or other records — *e.g.*, date of birth or death, date of marriage or divorce — does not require legal training. Such information, as certified by a notary, is often requested by foreign agencies in the context of adoption of a child. Thus, in part to lessen the bureaucratic hardships imposed on couples attempting to adopt foreign children, this section gives lawmakers the option of allowing notaries to perform a verification of fact function. The statutory list of verifiable facts may be tailored to a particular jurisdiction.

In performing a verification of fact, notaries may visit a pertinent office that houses public, vital, or other records to ascertain the needed facts, or accept a record from an individual. Clearly, the former option is preferred, but notaries are given discretion in the latter case to assess the trustworthiness of any record presented. The notary is well-advised to positively identify the presenter, and to inspect the proffered record for evidence of tampering or counterfeiting, much like a notary inspects identification credentials presented by principals.]

Chapter 3 — Registration to Perform Electronic Notarial Acts

Comment

General: Chapter 3 delineates the process for registering to perform electronic notarial acts. The drafters firmly believed that requiring a notary to obtain an additional commission in order to operate electronically would impose an impediment in violation of the UETA and E-SIGN's position that *any* notary can perform electronic notarizations, not to mention an administrative hardship on the commissioning body. The drafters, however, also believed it to be in the public interest and a reasonable accommodation to have some governmental oversight over notaries performing electronic notarizations. Such oversight would at the very least enable the commissioning body to authenticate a notary's electronic acts and to investigate a notary's conduct in disciplinary matters. Thus, this Act requires interested notaries to register with the commissioning official their intent to notarize electronically before performing such acts. (*See* Section 3-1.) A notary who is not interested in performing electronic notarizations is not required to register.

As a reasonable protection for the public, registrants are required to prove their electronic competence by passing a course of instruction and examination on electronic notarization. (*See* Section 3-2.) The registration is valid as long as the notary's underlying commission remains in effect (*see* Section 3-3).

Requirements for the electronic registration application are provided in Section 3-4, and Section 3-5 mandates the commissioning official to approve the registration of a notary who meets the requirements, and deny any applicant who does not qualify. Section 3-6 relates to the confidentiality of information disclosed by registrants. Finally, Section 3-7 requires the commissioning official to establish and maintain a database of notaries public. The database would identify those notaries approved to perform electronic notarial acts.

§ 3-1 Registration with [Commissioning Official].

(a) A notary public shall register to perform electronic notarial acts with the name that appears on the notary's commission.

(b) A notary public shall register with the [commissioning official] for each commission term before performing electronic notarial acts.

(c) An individual may apply for a notary public commission and register to perform electronic notarial acts at the same time.

(d) An individual may elect not to perform electronic notarial acts.

Comment

Section 3-1 requires the notary to register with the commissioning official. (*See* N.C. GEN. STAT. § 10B-106.)

Registration serves a number of purposes. First, it notifies the commissioning official of the notary's intent to perform electronic notarial acts. Second, it allows the commissioning official to maintain oversight of notaries who notarize electronic records. Third, it enables the official to verify and authenticate the electronic acts of the notary.

Subsection (a) clarifies that a notary public must use the same name that

appears on the notary's commission when registering to perform electronic notarial acts.

Under Subsection (b), an interested notary must apply for registration for each commission term. Registration does not automatically renew.

Subsection (c) clarifies that a person may seek to be registered to perform electronic notarial acts at the same time the person submits an application for a notary commission — even an initial one.

Subsection (d) simply provides that holding a commission as a notary public does not obligate the notary to register to perform electronic acts.

§ 3-2 Course of Instruction and Examination.

(a) Before each registration to perform electronic notarial acts, an individual shall complete a course of instruction of [_____] hours approved by the [commissioning official] 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 this [Act] or in any other law or official guideline of this [State].

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

Comment

Section 3-2 mandates that all notaries applying for registration to perform electronic acts first satisfactorily complete an education and testing requirement. This is in addition to and not a substitute for the general education and testing requirement for basic notary commissioning, if the jurisdiction has one. The Act adopts the position that, in order to protect the public, any notary public who wants to perform electronic notarizations must prove the capability to do so. This section sets forth the mechanism for providing that protection.

The recommended number of hours for the education requirement in Subsection (a) has been left up to the enacting jurisdiction, a change from the 2010 Model Notary Act which mandated four hours of instruction. The length of the course of instruction should ensure that the notary is at a minimum proficient in performing certain electronic tasks and prepared to pass the required examination. It is anticipated that the course and exam may be taken online or in a more traditional classroom setting. Administrative matters may be handled in the same manner as the basic notary education requirements. Nothing in the Act precludes the notary from taking additional courses to maintain or improve skills. Indeed, continuing education that keeps the notary apprised of technological advances is encouraged. (*See*, *THE NOTARY PUBLIC CODE OF PROFESSIONAL RESPONSIBILITY*, Guiding Principle X and Standard XA-4 (www.nationalnotary.org/knowledge-center/reference-library/notary-public-code-of-professional-responsibility.))

Subsection (b) expands the provisions of the 2010 Act. The course would be required to address any rules, procedures, and ethical obligations in this Act, or in any other law or official guidelines of the commissioning official. This would include pertinent statutes, administrative rules, or case law decisions, as well as any relevant directives of the commissioning official that may appear

in the official's website, notary public handbook, newsletters, or other written communications.

Subsection (c) gives the option of taking the instruction on electronic notarization at the same time as any course used to fulfill basic notary commission qualification requirements. For example, the material on electronic notarization could be presented in a classroom course on the same day as the regular notary course or in a separate unit of an online course covering the basic notary public material.

§ 3-3 Term of Registration.

Unless terminated pursuant to Section 12-2 of this [Act], the term of registration to perform electronic notarial acts shall begin on the registration starting date set by the [commissioning official] and shall continue as long as the notary public's current commission remains valid.

Comment

Section 3-3 sets the effective dates of the registration period during which a notary public is authorized by the commissioning official to perform electronic notarial acts. Approval to perform electronic notarial acts is prospective, and not retrospective. Whereas the registration starting date may not correspond with the underlying notary commission, the expiration date of both the commission and registration always will be the same.

§ 3-4 Registration Application.

An individual registering to perform electronic notarial acts shall submit to the [commissioning official] an application in a format prescribed by the [commissioning official] which includes:

(1) proof of successful completion of the course and examination required under Section 3-2 of this [Act];
(2) disclosure of any and all license or commission revocations or other disciplinary actions against the registrant; [and]
(3) any other information, evidence, or declaration required by the [commissioning official][.][; and
(4) evidence that the surety bond prescribed by Section 5A-3 for performance of electronic notarial acts by audio-video communication has been issued.]

Comment

Section 3-4 has been considerably shortened from its original form in the 2010 Model Notary Act. One requirement eliminated was the provision requiring a notary public to notify the commissioning official of each separate technology the notary intends to use in performing electronic notarial acts (*see* 2010 MODEL NOTARY ACT § 16-4(2)). At the time of registration an applicant might not know of all the electronic notarization systems the applicant might use in the future. Furthermore, it is conceivable the notary might be presented with the opportunity to use a system not previously considered for

use. As a result, the drafters decided that this reporting requirement was overly restrictive. Note however, that in Sections 4-1(d) and (e) an electronic notarization system provider or the notary public must apprise the commissioning official of this information after enrollment in, or initial use of, any electronic notarization system by the notary. The policy of reporting each technology and system remains, but the notary need not report it at the time of registration.

This Chapter prescribes three requirements for the registration application. The first is proof that the applicant has completed the educational course and examination required under Section 3-2. The second is disclosure of any revocations of and disciplinary actions taken against a professional license or commission of the applicant, including any sanctions imposed related to an existing or prior notary commission and actions that had occurred after the notary had been issued the current commission. The third is any additional requirement that may be deemed appropriate by the commissioning official.

[The fourth requirement (evidence that a surety bond has been issued) is bracketed and applies only to those registrants who intend to perform electronic notarial acts using audio-video communication. (*See* Section 5A-3.)]

§ 3-5 Approval or Rejection of Registration Application.

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

(b) The [commissioning official] may reject a registration application if the applicant fails to comply with any section of this [Act].

Comment

Upon an approval of a registration to perform electronic notarizations, the commissioning official shall issue a unique registration number to the notary. This number is separate and distinct from the commission number the registrant was issued for being commissioned as a notary public. The unique registration number is a required element of the notary public's electronic seal under Section 7-3(a).

Subsection (b) authorizes the commissioning official to reject a registration application under two general circumstances: when the applicant fails to meet the requirements for registration under Chapter 3, and when the applicant fails to comply with any section of the Act in performing electronic notarial acts during a previous or current registration term. Any prior or pending disciplinary action taken against the notary's current commission also is a cause for rejecting the application.

§ 3-6 Confidentiality.

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

Comment

Section 3-6 mandates that the confidentiality standards that apply to an

application for commissioning as a notary public must be applied to a registration application. If a jurisdiction has a particular provision, the bracketed clause may be used to reference the applicable statute. (*See* MD. CODE ANN. (GEN. PROV.) § 4-332, which relates to inspection of a public record that contains information about the application and commissioning of a notary public.)

§ 3-7 Database of Notaries Public.

The [commissioning official] shall maintain a database of notaries public on a publicly-accessible website which:

(1) any interested person may use to verify the authority and good standing of a listed individual to perform notarial acts;
(2) indicates whether a notary is registered to perform electronic notarial acts; and
(3) describes any administrative or disciplinary action taken against the notary.

Comment

This Section mandates that the commissioning official maintain a database of notaries public searchable by the public. (*See* REV. UNIF. LAW ON NOT. ACTS § 24, for a similar requirement, though it does not require the posting of disciplinary actions against notaries, as Section 3-7 provides.) Currently, approximately one-half of the notary-commissioning jurisdictions have such a publicly accessible database. While the databases mainly provide information about a notary public's availability to perform paper-based notarial acts, Section 3-7 requires the database also to indicate whether a notary is registered to perform electronic notarial acts. (*See* the West Virginia Secretary of State's database at apps.sos.wv.gov/business/notary for an example of such a register.)

Chapter 4 — Electronic Notarization Systems

Comment

General: This Chapter provides rules for electronic notarization systems and providers. An electronic notarization system is the means by which a notary performs an electronic notarial act. A system may be a hardware device such as a cryptographic token that is used to create a notary public's electronic signature. It may be a software program that runs on a mobile device and uses the device's touchscreen to enable a notary to sign, or a web application that requires a notary to click a button to sign. A system may incorporate both hardware and software, as in a solution that requires a signature pad to interface with software to create the notary's electronic signature.

There are three different general approaches in regulating electronic notarization systems. The first is to provide a single solution and require all notaries to use it. (KAN. ADMIN. REG. § 7-43-2(c).) The second is to qualify and approve all solution providers and require notaries to use only them. (18 N.C. ADMIN. CODE §§ 07C.0501 and 07C.0502.) The third is to establish performance standards and require any system that a notary uses to comply with these standards. (FLA. STAT. ANN. § 117.021(2); and FLA. ADMIN. CODE § 1N 5.002.) Of these three approaches, this Act adopts the third. The performance standards specified in Section 4-1 are the heart of the Chapter.

§ 4-1 Requirements for Systems and Providers.

(a) An electronic notarization system shall comply with this [Act] and any rules adopted by the [commissioning official] pursuant to Section 15-1 [and Section 15-2] of this [Act].

(b) An electronic notarization system requiring enrollment shall enroll only notaries public who have registered with the [commissioning official] to perform such acts pursuant to Chapter 3 of this [Act].

(c) An electronic notarization system provider shall take reasonable steps to ensure that a notary public who has enrolled to use the system has the knowledge to use it to perform electronic notarial acts in compliance with this [Act].

(d) A provider of an electronic notarization system requiring enrollment shall notify the [commissioning official] of the name of each notary public who enrolls in the system within five days after enrollment by means prescribed by the [commissioning official].

(e) A notary public who uses an electronic notarization system not requiring enrollment shall notify the [commissioning official] of the date of initial use of the system within five days after the initial use by means prescribed by the [commissioning official].

(f) An electronic notarization system shall require access to the system by a password or other secure means of authentication.

(g) An electronic notarization system shall enable a notary public to affix the notary's electronic signature in a manner that attributes such signature to the notary.

(h) An electronic notarization system shall render every electronic notarial act tamper-evident.

Comment

The standards to which electronic notarization systems and providers must conform are specified in Section 4-1. Subsection (a) requires systems to meet the performance standards in the Act and any related rules adopted by the commissioning official, including ones to enable remote electronic notarization (*see* Section [15-2]). For example, a system must be capable of producing a notary's electronic seal with the elements specified in Section 7-3.

Subsection (b) pertains to systems that enroll notaries. (*See* Section 2-10 and Comment.) System providers that require enrollment must enroll only notaries who have registered with the commissioning official to perform electronic notarial acts. Providers might achieve this by requiring a notary to upload a copy of the notary's commission and notice of registration to perform electronic notarial acts, or the system might "ping" a commissioning official's online database of notaries public automatically to verify whether a notary has in fact registered.

Subsection (c) requires providers to reasonably ensure that notaries enrolled in the system know how to use it. The system provider might provide training when a notary is given access to the system, create a user manual as a reference guide, or provide answers to frequently-asked questions on its website. Subsection (c) does not require the provider to ensure that a notary has performed a particular electronic notarization in conformity with the law, only that the notary knows how to use the system to do so.

Subsection (d) requires a provider requiring enrollment to notify the commissioning official of the identity of the notary within five days of enrollment. (*See* Comment on Section 3-4.) A commissioning official will need to know which systems the notary is using for the purpose of oversight and issuing authentications of electronically-notarized records.

Subsection (e) applies to systems not requiring enrollment. An example might be a generic software program installed on a notary's computer or mobile device. The program may not be designed specifically to perform electronic notarial acts, but nonetheless has the capability to be used for this purpose, along with other functions. A notary who employs such a system must inform the commissioning official of this fact within 5 days of its initial use. The commissioning official may prescribe the means for this notification (*e.g.*, completion of a registration form, sending an email, updating the notary's profile on the commissioning official's website, or some other preferred method).

All systems — those requiring enrollment and those that do not — must authenticate the notary to the system prior to use. Subsection (f) means that at a minimum the system must require a username and password. Since many mobile devices now have biometric identification capabilities, a thumb- or fingerprint, or facial scan also could be used. The overarching concern is to prevent individuals from performing electronic acts without proper authentication. It should be noted that the authentication required under this Section is in addition to any authentication to use the computer or mobile device. That is, the notary must first log on to gain access to the computer or mobile device before then accessing the

software program to perform the electronic notarization.

Subsection (g) raises the important issue of attribution. Under the UETA, "an electronic record or electronic signature is attributable to a person if it was the act of the person" (*see* UETA § 9(a)). An electronic notarization system must be able to show that production of the notary's signature was the notary's act. (*See* MINN. STAT. ANN. § 358.47(a); and VA. CODE ANN. § 47.1-16A.)

Finally, Subsection (h) requires an electronic notarization system to render every electronic notarial act tamper-evident. (*See* Section 2-19 and Comment; IOWA CODE ANN. § 9B.20.1; N.D. CENT. CODE § 44.06.1-18.1; MONT. CODE ANN. § 1-5-615(1)(a); OR. REV. STAT. § 194.305(1); PA. CONS. STAT. ANN. § 57-320(a); and W. VA. CODE § 39-4-19(a).)

§ 4-2 Notary Not Liable for System Failure.

A notary public who exercised reasonable care enrolling in and using an electronic notarization system shall not be liable for any damages resulting from the system's failure to comply with the requirements of this [Act]. 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.

Comment

In notarizing paper documents, notaries generally are not concerned with whether a pen they use to sign or a rubber stamp with which they affix an impression of their notary seal are working. There is little risk of damage if these tools were to malfunction. With electronic notarization systems, there is the possibility that a "bug" in software or hardware could result in the production of an electronic notarization that does not comply with the law. For example, a malfunctioning signature pad could capture the signature of the signer and notary, but fail to save the data. Alternatively, a problem with software could result in the system's failure to accurately produce the required elements of the notary's electronic seal. (*See* Section 7-3.)

Thus, the drafters concluded that an exculpatory clause relieving the notary from liability for such failures was needed. Section 4-2 provides protection against liability if the notary used reasonable care in enrolling in and using the system. The Section also explicitly renders unenforceable any provision in an electronic notarization system licensing agreement which attempts to waive a notary's immunity to liability for the system's failure. This provision is designed to prevent a culpable system provider or manufacturer from shifting liability to an innocent notary.

§ 4-3 Refusal of Requests to Use System.

A notary public shall refuse a request to:

(1) use an electronic notarization system that the notary does not know how to operate;

(2) perform an electronic notarial act if the notary does not possess or have access to an appropriate electronic notarization system; and

(3) perform an electronic notarial act if the notary has a reasonable belief that an electronic notarization system does not meet the requirements set forth in this [Act].

Comment

In Section 4-1(c) a provider of an electronic notarization system has a duty to ensure that a notary public with access to the system knows how to use the system. Section 4-3(1) places equal responsibility on notaries for knowing how to operate any system that they employ, and mandates that they refuse to operate an unfamiliar system.

In many instances, a notary will be able to enroll in and use an electronic notarization system at a moment's notice, provided the notary knows how to operate the system. Subparagraph (2) covers situations in which a notary may not have sufficient time or opportunity to procure or enroll in a given system for the purpose of satisfying a request to perform an electronic notarial act. For example, a notary may be asked to perform an electronic notarization using a digital certificate that the notary does not have or cannot be expected to obtain quickly enough to fulfill the request. In such cases, the notary must refuse to perform the requested act.

Subparagraph (3) requires a notary to refuse to perform an act if the notary has a reasonable belief that the system will not allow compliance with applicable law. For example, if the system does not allow the notary to create an electronic signature or journal entry in conformance with the Act, the notary may refuse the request to perform the act using that system.

Chapter 5 — Electronic Notarial Acts

Comment

General: Chapter 5 identifies paper-based notarial acts that may be performed electronically, and makes clear that certain fundamental requirements for notarial acts also apply in the electronic realm.

Section 5-2 is an omnibus provision allowing legislators to apply any existing notary statutes for notarial acts to electronic notarizations.

Section 5-3 specifies three basic requirements for electronic notarial acts and one bracketed requirement applying in the context of a remote electronic notarization. Among these requirements is the need for the principal to appear in the physical presence of the notary for any notarization of an electronic signature. A new requirement particular to electronic notarial acts clarifies that both the principal and signer must sign the electronic record using an electronic signature. The bracketed provision allows notaries to administer oaths and affirmations by means of audio-video communication.

§ 5-1 Authorized Electronic Notarial Acts.

A notary public of this [State] who has registered to perform electronic notarial acts may perform the following notarial acts electronically:

(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)] [[other notarial act] as set forth in Section [____] of [_____][.][; and]]
[(6)] [noting a protest of a negotiable instrument[.][; and]]
[(7)] [executing a verification of fact.]

Comment

Section 5-1 identifies the six types of notarizations that may be performed electronically. All but noting a protest are identified in the 2010 Model Notary Act. (*See* 2010 MNA Section 5-1 and Comment.)

[Noting a protest and performing a verification of fact are in brackets. This offers legislators the choice of allowing notaries of their jurisdiction to perform them. In recent years, some states have amended their statutes to allow only certain notaries to perform a protest. (CAL. GOV'T CODE § 8205(a)(1); NEV. REV. STAT. ANN. § 240.075.10; and OR. REV. STAT. § 194.375.) On the other hand, states that have enacted the Revised Uniform Law on Notarial Acts included protests as an authorized notarial act, although only two states limited who could perform them. (*See* MONT. CODE ANN. § 1-5-604(c)(4); and OR. REV. STAT. § 194.375.)

Since the 2002 Model Notary Act introduced the new notarial act of "verification of fact" (2002 Model Notary Act, Section 2-20 and Comment), two states have enacted it into law. (VA. CODE ANN. § 47.1-2; and WYO. STAT. ANN. § 34-26-101(b)(xx).)]

As in the 2010 Model Notary Act, oaths and affirmations are not mentioned

in the list of authorized electronic notarial acts in that, being largely oral and gestural acts that require a face-to-face meeting of oath-taker and notary, they are not performed differently in an electronic context than in a paper environment. [(*See* Section 5-3(c) that permits oaths and affirmations to be administered using audio-video communication.)]

Nothing in this or any other section of Chapter 5 derogates from the notary's authority to perform any of the notarial acts that may be authorized by other applicable law in a non-electronic setting. [(*See* Subparagraph 5-1(5).)] For example, one state allows notaries to verify vehicle identification numbers. (FLA. STAT. ANN. § 319.23(3)(a).)

§ 5-2 Applicability of Other Laws and Rules.

In performing an electronic notarial act, the notary public shall adhere to all applicable laws, rules, and official guidelines of this [State] that apply to notarial acts, including but not limited to:

(1) definitions as set forth in [Section [____] of [_____]];
(2) identification of principals as set forth in [Section [____] of [_____]] OR [Chapter 8 of this [Act]];
(3) maintenance of a journal of notarial acts as set forth in [Section [____] of [_____]] OR [Chapter 9 of this [Act]];
(4) completion and form of a notarial certificate as set forth in Section [____] of [_____];
(5) disqualifications for a notary's financial, beneficial, or personal interest as set forth in Section [____] of [_____];
(6) prohibitions for notaries as set forth in Section [____] of [_____];
(7) prescriptions for notaries as set forth in Section [____] of [_____];
(8) penalties and sanctions for notary misconduct as set forth in Section [____] of [_____]; and
(9) prohibitions and prescriptions regarding the payment, waiving, discriminatory assessment, prior notice, and journal recording of fees for non-electronic acts, as set forth in Section [____] of [_____].

(NOTE TO LEGISLATORS: If law in your jurisdiction does not provide rules for subparagraphs (1) through (9) above, you may choose to adopt provisions from the National Notary Association's Model Notary Act of 2010. The MNA is a state-of-the-art collection of best practice rules that have been widely adopted in the United States and its territories through legislative enactment, administrative rule-making, or gubernatorial executive order.)

Comment

Section 5-2 is an omnibus provision designed to facilitate enactment of the MENA as a "plug-in" to a state's existing notary public code. Instead of enacting new sections duplicating these provisions, Section 5-2 earmarks pertinent

existing statutes to apply to electronic notarizations as they do to paper-based ones. (For a different approach, *see* ARIZ. REV. STAT. ANN. §§ 41-351 *et seq.*, which largely duplicates §§ 41-311 *et seq.*)

Subparagraphs (2) and (3) give lawmakers the option of either plugging in to existing statute or adopting two later chapters in this Act — Chapters 8 (Identification of Principals) and 9 (Journal of Notarial Acts). They were added to the Act because the drafters believed they were important to the integrity and fraud-deterrent function of all notarial acts, electronic and non-electronic.

§ 5-3 Requirements for Electronic Notarial Acts.

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

(b) If an electronic notarial act requires a record to be signed:

(1) the principal shall appear in person before the notary public; and

(2) the principal and the notary public shall sign the record with an electronic signature.

[(c) If a notarial or electronic notarial act requires administration of an oath or affirmation to a principal or a witness, the notary public may administer that oath or affirmation by means of audio-video communication.]

Comment

Section 5-3 mandates basic requirements for electronic notarial acts. Subsection (a) applies the rule adopted in virtually every state that a notary public must be within state borders when performing an electronic notarial act. (*See* FLA. STAT. ANN. § 117.021(1); and § 117.01(1), where the jurisdiction of a notary public who performs electronic notarial acts is the same as for paper-based acts.) By contrast, Virginia law allows electronic notaries to notarize anywhere in the world just as its paper-based notaries may do. (VA. CODE ANN. § 47.1-13B.) The drafters believe the public's interest is best served by a policy requiring electronic acts to be performed by notaries in the state or jurisdiction where they are commissioned. Traditionally, each state has had the authority to appoint and regulate notaries public operating within its boundaries and the statutes specifically designate the individuals authorized to perform notarial acts within each state. (ALA. CODE § 35-4-24; DEL. CODE ANN. tit. 29, § 4323; IDAHO CODE § 55-701; MISS. CODE ANN. § 89-3-3; and UTAH CODE ANN. § 57-2a-3(1).) These laws typically do not authorize notaries public of other jurisdictions to notarize within the state, though they often allow commuting residents of bordering states to apply for a notary commission in the state where they work. (*But see* MONT. CODE ANN. § 1-5-605(4), where, through an interstate reciprocity agreement, Montana notaries are expressly authorized to perform notarial acts in a bordering state that recognizes the notary's authority within that state.)

Subparagraph (b)(1) requires the principal signing an electronic record to appear in person before the notary public for an acknowledgment or verification upon oath or affirmation, or for a signature witnessing. (*See* Section 2-1 and Comment.) Notaries may certify a

copy of an electronic record, note a protest of a negotiable instrument, and perform a verification of fact without requiring the individual requesting the electronic notarial act to appear personally.

Subparagraph (b)(2) emphasizes that an electronic notarial act involving notarization of a signature requires both the principal and notary public to sign the electronic record with an electronic signature. The clarification is important because the definition of "electronic notarial act" (*see* Section 2-5 and Comment) has been broadly construed to apply to acts involving electronic *records* that may or may not require a signature. (*See, e.g.,* Subparagraph 5-1(4).) The drafters were concerned that without Subparagraph (b)(2) a principal could sign a paper document with a handwritten ink signature, convert the document into an electronic record, and then present it to a notary public for notarization in person or through audio-video communication, raising doubts about the authenticity of the signature.

[Subsection (c) gives any jurisdiction that enacts the bracketed Chapter 5A the option of allowing notaries to administer oaths and affirmations by means of audio-video communication. One state now authorizes law enforcement officers, correctional officers, correction probation officers, traffic accident investigative officers, and traffic infraction enforcement officers who have the power to administer oaths to administer oaths using reliable electronic means without requiring the individual making the oath to be physically present before the officer. (*See* FLA. STAT. ANN. § 117.10.) This bracketed provision allows a notary public to administer an oath or affirmation to an affiant who is the subject of the electronic notarial act, or to any witness required for the electronic notarization (*e.g.*, a credible witness who identifies the principal).]

[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.

Chapter 7 — Electronic Signature and Seal of Notary Public

Comment

General: To evidence an electronic notarial act, an electronic notarial certificate must be properly signed and sealed by the notary public. This Act replaces the 2010 Model Notary Act concepts of "registered electronic notary seal" and "registered electronic signature" with the provisions of this Chapter. (*See* MODEL NOTARY ACT of 2010 Chapter 19.) In the 2010 Act, a notary public was required to register the notary's electronic signature and seal with the commissioning official. In this Act, a notary or electronic notarization system provider must notify the commissioning official of each electronic notarization system the notary uses to create electronic signatures and seals.

Section 7-1 emphasizes that an electronic notarial certificate must be signed by the notary and authenticated with the notary's electronic seal. Section 7-2 provides basic performance and security standards for a notary's electronic signature. Section 7-3 provides specifications for the notary's electronic seal.

§ 7-1 Certification of Electronic Notarial Act.

A notary public shall sign each electronic notarial certificate with an electronic signature that complies with Section 7-2 of this [Act] and authenticate the electronic notarization with an electronic seal that complies with Section 7-3 of this [Act].

Comment

Section 7-1 requires that an electronic notarial certificate be signed with the notary's electronic signature and authenticated with the notary's electronic seal. This provision generally corresponds with the laws governing traditional paper notarial certificates. (ALA. CODE § 36-20-72; ARIZ. REV. STAT. ANN. § 41-313E and § 41-355G; CAL. GOV'T CODE § 8205 and § 8207; IOWA CODE ANN. § 9B.15; OKLA. STAT. ANN. tit. 49, § 5; KAN. STAT. ANN. § 53-105; and UTAH CODE ANN. § 46-1-16.

§ 7-2 Electronic Signature of Notary.

(a) A notary public shall use an electronic notarization system that complies with Chapter 4 of this [Act] 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 an electronic notarization system 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 an electronic notarization system 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] that a notary public who signed an

electronic record in an official capacity had authority at that time to perform electronic notarial acts.

Comment

Subsection (a) requires a notary's electronic signature to comply with Chapter 4 (related to electronic notarization systems) and additionally requires the notary's electronic signature to be "capable of independent verification," which is defined in Subsection (d). It takes the position that any party relying on an electronic notarization should be able to verify the status of the notary's commission and registration to perform electronic notarial acts. The public can verify the status of a notary by checking the database required to be maintained by the commissioning official under Section 3-7, or making inquiry to the commissioning official.

Subsection (b) is intended to prevent misuse of the notary's electronic signature. Such misuse might be undetected if an impostor obtained the notary's access credentials to an electronic notarization system and signed an electronic notarial certificate in the notary's name. Therefore, the notary has a duty to protect access to or otherwise prevent another's use of any electronic notarization system that the notary employs to perform electronic acts. (*See, for example*, N.M. ADMIN. CODE § 12.9.11.C and E; N.C. GEN. STAT. § 10B-126(a) and (b); and VA. CODE ANN. § 47.1-14E.)

Subsection (c) requires the notary to keep in the notary's sole possession or control the knowledge or physical access needed to produce the notary's electronic signature. (*See* Section 2-17 and Comment.)

Subsection (d) defines the phrase "capable of independent verification" as introduced in the 2010 Model Notary Act. There, the term was defined to include verification of both the notary's authority and the validity of the notarial act. (MODEL NOTARY ACT OF 2010, Section 15-1 and Comment.) Now, only the aspect of verification of the notary's authority is required. Verification of the notary's authority can be ascertained online through the commissioning official's database (*see* Section 3-7 and Comment) or through other contact with the official's office.

§ 7-3 Electronic Seal of Notary.

(a) The electronic seal of a notary public shall contain:
  (1) the name of the notary exactly as it is spelled on the notary's commission;
  (2) the title "Notary Public";
  (3) the words "[State] of [name of [State]]";
  (4) the commission number of the notary;
  (5) the registration number indicating that the notary may perform electronic notarial acts; and
  (6) the commission expiration date of the notary.

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

(c) The electronic seal of a notary public shall not be used for any purpose

other than performing electronic notarizations under this [Act].

(d) Only the notary public whose name and registration number appear on an electronic seal shall generate that seal.

Comment

Section 7-3 provides rules for the notary public's electronic seal. Essentially all states and jurisdictions regulating notaries public require them to have and use an official seal to authenticate their official acts (*see, for example,* ARK. CODE ANN. § 21-14-107(b); and MO. ANN. STAT. § 486.285), or to add commission information typically included in an official seal to a notarial certificate under the notary's signature (*see* MICH. COMP. LAWS § 55.282(2); and N.Y. EXEC. LAW § 137).

Subsection (a) specifies the informational elements that must be included in the notary's electronic seal. These elements generally correspond to information included in notary seals used on paper documents.

The Act does not prescribe the form in which the electronic seal is produced. The jurisdictions that have enacted the Uniform Real Property Electronic Recording Act included its provision clarifying that an image of a physical seal need not be reproduced on an electronically-notarized real property record. (*See* IDAHO CODE § 31-2903(3); and WIS. STAT. ANN. § 706.25(2)(c)). While Subsection (b) allows the seal to be affixed in the form of a digital image that appears in the representation of a traditional physical notary public seal (*see* TEX. GOV'T CODE § 406.013(d); ADMIN. RULES OF MONT. § 44.15.107), the seal also may simply constitute information added to the electronic record (*see* CAL. GOV'T CODE § 27391(e); and OR. ADMIN. RULES § 160-100-0100(3)).

Subsection (c) replicates a provision limiting the use of traditional notary seals for notarial purposes only. (*See* CAL. GOV'T CODE § 8207). By contrast, the notary is not prohibited from using the electronic signature adopted for use in electronic notarial acts for non-notarial purposes as well — just as a paper-based notary uses an inked signature for both notarial and non-notarial purposes.

Subsection (d) disallows anyone but the notary public himself or herself from using the notary's electronic seal of office.

Chapter 8 — Identification of Principals

Comment

General: The drafters determined to include a chapter in this Act on identification of principals because there still are jurisdictions that do not have adequate or meaningful identification rules for notaries public. In some cases, the rules may not be particularly useful. Jurisdictions with more modern laws on identification may choose to have their existing statutes for paper-based notarial acts apply to electronic acts as well — *see* Subparagraph 5-2(2).

§ 8-1 Identification of Principal Required.

[(a)] A notary public shall determine from personal knowledge as defined in Section 2-11 or satisfactory evidence of identity as prescribed in Section 8-2 that the principal appearing before the notary is the individual that he or she purports to be.

[(b) In performing an electronic notarial act by means of audio-video communication, a notary public shall determine from personal knowledge as defined in Section 2-11 or satisfactory evidence of identity as prescribed in Section 5A-5 that the principal is the individual that he or she purports to be.]

Comment

Section 8-1 makes clear that properly identifying a principal is a pro-active obligation imposed upon the notary for every notarial act. Any electronic notarial act involving notarization, whether it be an authentication of an electronic signature, or administration of an oath or affirmation, requires the principal signing the electronic record or taking the oath or affirmation to be identified by the notary. (*See* the definition of "principal in Section 2-12.) Although some jurisdictions do not specifically address this requirement, it is essential to any notarization, electronic or non-electronic.

Subsection (a) provides the standard for identification of principals for those electronic notarizations which require the principal to appear physically before the notary public. (*See* the definitions of "'personal knowledge' and 'personally knows'" and "satisfactory evidence of identity" in Sections 2-12 and 2-15, respectively.) Section 8-2 further defines satisfactory evidence of identity.

[Subsection (b) is bracketed and should be enacted by states choosing to adopt Chapter 5A. It provides the specific standard for identification of principals which applies to electronic acts performed by audio-video communication. A jurisdiction that opts not to enact Chapter 5A should not adopt Subsection (b), remove "(a)", and retain the first sentence.]

§ 8-2 Identification of Principal by Satisfactory Evidence.

(a) A notary public has satisfactory evidence of identity if the notary can identify the individual who appears in person before the notary based on:

(1) at least one unexpired credential issued by a federal, state, or

tribal government bearing the photographic image of the individual's face and signature and a physical description of the individual, or a properly stamped passport without a physical description; or

(2) the oath or affirmation of one credible witness disinterested in the record or transaction who is personally known to the notary public and who personally knows the individual, or of two credible witnesses disinterested in the record or transaction who personally know the individual and provide for the notary's examination credentials as described in Subparagraph (1) of this Section.

(b) For the purposes of this Section:
   (1) "federal" means the United States; and
   (2) "tribal government" means a tribal government recognized by the United States.

Comment

Section 8-2 buttresses the tenet that positive proof of identity is integral to every proper electronic notarization of a signature. A detailed definition of "satisfactory evidence of identity" was deemed essential to this Act. Many statutes refer to "satisfactory evidence," but not all define it precisely. The section allows a principal to prove identity in one of two ways. The first involves self-proof through the use of reliable identification credentials. The second employs credible witnesses.

Subparagraph (a)(1) describes the attributes of credentials found in most self-proving provisions. (*See, e.g.,* CAL. CIV. CODE § 1185(b)(4). *But see* GA. CODE ANN. § 45-17-8(e), which allows the notary some discretion in determining what constitutes acceptable proof.) In response to a recurring inquiry, the Act specifically states that identification issued by a tribal government may be acceptable, and defines the term in Subparagraph (b)(2). The Act also makes any valid passport acceptable identification. This will ensure that visitors from foreign lands have the requisite proof of identity to access notarial services while they are in the United States. Of course, a passport is excellent proof of identity for a United States citizen, as well. The Act requires the principal to produce only one identification credential. (*Accord,* FLA. STAT. ANN. § 117.05(5)(b)(2).) Nothing prohibits a notary from asking for additional proof of identity if any credential presented by the principal raises questions as to its authenticity or is otherwise suspect. Indeed, notaries are obligated to satisfy themselves that the evidence presented positively proves the principal's identity.

Subparagraph (a)(1) requires an identification credential to be unexpired. States that have enacted the Revised Uniform Law on Notarial Acts allow credentials to be expired by not more than three years. (*See* IOWA CODE ANN. § 9B.7; and W.VA. CODE § 39-4-7.)

Subparagraph (a)(2) provides a second avenue for proving identity. It is designed for those principals who do not have identification credentials. Primary beneficiaries of this rule are the elderly, especially those in nursing homes, who may no longer have valid driver's licenses or other current forms of government identification. Following

the lead of California (*see* CAL. CIV. CODE § 1185(b)(2)) and Florida (*see* FLA. STAT. ANN. § 117.05(5)(b)(1)), the Act allows credible witnesses of two types to prove the identity of the principal. Any credible witness must personally know the principal. (*See* Section 2-11 for a definition of "personal knowledge.") To prevent fraud and add to the integrity of the notarization, only persons disinterested in the record or related transaction may serve as credible witnesses.

Only one credible witness is needed if that witness is personally known to the notary. Otherwise two witnesses are required. The Act takes the view that the notary's personal knowledge of the identity of one credible witness is preferred over reliance on two witnesses, who must prove their own identities under the rules of Subparagraph (a)(1). Note that a credible witness cannot have his or her identity proven by another credible witness. The credible witness must either be known to the notary or self-prove identity through acceptable identification credentials.

Subsection (b) defines "federal" and "tribal government." The drafters included a definition of the former because of the confusion that has arisen over whether the term "federal" can apply to foreign governments that issue identification credentials. The Act takes the position that it refers solely to the United States government. Subsection (b) also clarifies that only federally recognized tribal governments may issue ID credentials that are regarded as trustworthy for notaries.

Proper identification lies at the heart of reliable notarizations, Consequently, the drafters contemplated that the rules of this section will be narrowly construed and strictly enforced.

Chapter 9 — Journal of Notarial Acts

Comment

General: The drafters included a separate chapter on the notary public journal in the Act because of the proven evidentiary value of notary journals and the fact that over half of the notary-commissioning jurisdictions in the United States do not have laws requiring notaries to keep journals.

Notary journals have proven to be a somewhat controversial subject. First, there is the threshold issue of whether or not a notary needs to maintain a journal under the law. Some jurisdictions require a notary journal (*see* ARIZ. REV. STAT. ANN. § 41-319; CAL. GOV'T CODE § 8206(a)(1); MO. ANN. STAT. § 486.260; NEV. REV. STAT. ANN. § 240.120; MISS. CODE ANN. § 25-33-5; and 57 PA. CONS. STAT. ANN. § 319), but many do not. Some laws may mention notary records or journals without imposing a specific requirement to maintain them. (*See* ME. STAT. ANN. tit. 4 § 955-B; and UTAH CODE ANN. §§ 46-1-13 and § 46-1-14.) No jurisdiction outlaws the practice. Second, if a journal is maintained, what entries are appropriate? Finally, who should have access to a journal? Most jurisdictions do not address this issue, even though their notaries may be required or allowed to maintain a journal of notarial acts.

The drafters have adopted the view that journals are essential to good notarial practice and decidedly in the public interest. Entry requirements serve to help ensure that the notary records critical information about each notarial act. Such data can be extremely useful in answering any future questions that may arise concerning the document or its signer.

The Act nonetheless recognizes that there is a tension between principals' privacy rights and the right of the public to access information. Consequently, whereas journals of notarial acts should not be considered public records *per se*, their public utility should be recognized and limited access granted in certain situations.

§ 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 this Chapter.

(b) A notary public may maintain more than one journal to record notarial acts.

(c) 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.

(d) For the purposes of this Chapter, "notarial acts" includes any act that a notary public may perform under this [Act] or other law of this [State].

Comment

Subsection (a) mandates that every notary maintain an official journal of all notarizations performed. The notary is required to record notarial acts in chronological order. It mandates that the journal entry be made at the time of notarization. The Act does not specify whether the recording must be made

before or after the notarial act is completed. Although completing the journal entry at the end might seem a logical choice, there is merit in completing the entry before the rest of the notarization is performed. The latter option prevents time-pressed principals from leaving with the notarized document before the journal entry is completed. Additionally, it allows the notary to refuse to act for those who will not provide a signature or any other required entry component. Finally, the journal entries detail the essential elements of a proper notarization. Consequently, by making the journal entry first, the notary is reminded of the steps that should be followed for each notarial act.

Subsection (b) reflects a change in policy from the 2010 Model Notary Act that permitted the notary to keep only one active journal at a time. (*See* OR. REV. STAT. § 194.300(1), allowing a notary to use more than one journal.) The drafters observed that electronic notarization systems currently in the marketplace today often incorporate a separate and distinct electronic journal in their systems, and envisioned the scenario of a notary using one or more electronic notarization systems on a regular basis. In addition, a notary may want to keep one journal for paper-based notarizations and additional journals for electronic notarizations, and, for those jurisdictions that enact Chapter [5A], even keep a separate journal for all electronic notarizations performed by means of audio-video communication. Maintaining one active journal was deemed to be overly restrictive.

Subsection (c) notes that a notary is required to keep a journal even if the notary's employer or contractor keeps records of notarial acts. (*But see* COLO. REV. STAT. 12-55-111(3) which exempts notaries from keeping a journal if their employer retains documents or electronic records containing all of the information required to be entered in the journal.)

Subsection (d) clarifies that in Chapter 9 "notarial acts" refers both to paper-based and electronic notarizations. States enacting Chapter 9 as a broader journal requirement should ensure this definition is retained.

§ 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 [State]; 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.

Comment

Section 9-2 prescribes the format for the journal of notarial acts. Subsection (a) provides three possible formats: a bound book with numbered pages, a format that complies with other applicable law or custom describing the journal's format, or an electronic format. It is particularly important that any book with numbered pages serving as a notary journal be "bound." Loose or separated pages kept in office filing cabinets may easily be misplaced and do not constitute a proper notary journal. Use of electronic journals is an increasingly common practice, whether sanctioned by statute (*see, e.g.,* TEX. GOV'T CODE § 406.014(e))

or permitted without express statutory authority.

Subsection (b) clarifies that all requirements in Chapter 9 pertaining to the journal of notarial acts apply equally to bound-book and electronic journals. For example, an entry in both a paper and an electronic journal must contain all of the requirements prescribed in Section 9-4. Similarly, a notary has a duty to keep an electronic journal under the notary's sole control (*see* Subsection 9-5(b)), and notify the commissioning official when an electronic journal is lost or stolen, or its security compromised (*see* Subsection 9-5(e)).

§ 9-3 Requirements of Electronic Journal.

[(a)] 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;

(4) be capable of capturing and saving an electronic signature [or a recognized biometric identifier or the data related thereto]; and

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

[(b) For purposes of this Chapter, "biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.]

Comment

Just as paper journals have certain operational attributes, under Subsection 9-2(b) electronic journals must have these same characteristics. Paper journals are kept under the physical control of the notary. When a paper journal is to be used, the notary takes it out of a locked safe, desk drawer, or attaché. Correspondingly, with an electronic journal, a notary must access it with a username and password known only to the notary (*see* Subparagraph (a)(1)). Paper journals are to be tamper-resistant; hence the requirement that they have bound bindings and numbered pages to deter alterations (*see* Subparagraph 9-2(a)(1)). Similarly, Subparagraph (a)(2) requires an electronic journal to employ technology to make it tamper-evident. (*See* Section 2-19 and Comment.) An electronic journal must be capable of capturing and saving an electronic signature (Subparagraph (a)(4)), and provide tangible or electronic copies of specific entries (Subparagraph (a)(5)) just like a paper journal.

Unlike paper journals, Subparagraph (a)(3) requires an electronic journal to be capable of creating a back-up record of all entries. This will preserve a record of the notary's official acts in the event the original is lost or compromised. Ideally, such a back-up electronic record would be maintained "off-site" to prevent flood, fire, or other disaster from claiming both original and backup records.

Subparagraph (a)(4) requires an electronic journal to have the capability of capturing and storing the electronic signature of the principal or other individual for whom an electronic notarial act is performed. [If a biometric identifier is permitted, it too must be capable of being captured and saved.] This parallels

the existing requirement for a bound journal to have space for a handwritten signature. (*See e.g.*, CAL. CIV. CODE § 8206(a)(2)(D); and MO. ANN. STAT. § 486.260.) [The concept of "biometric identifier" is borrowed from Illinois and Texas statutes. (*See* 740 ILCS § 14/10; and TEX. BUS. AND COM. CODE § 503.001(a).) Jurisdictions enacting this provision should also enact the corresponding provision in Subparagraph 9-4(a)(4).]

§ 9-4 Journal Entries.

(a) For every notarial act, the notary public shall record the following information in the journal:
  (1) the date and time of the notarial act;
  (2) the type of notarial act;
  (3) the title or a description of the record being notarized, if any;
  (4) the signature or, if an electronic journal is used, the electronic signature [or a recognized biometric identifier or the data related thereto] of each principal;
  (5) the printed full name [and][,] address[, and, in the case of a record affecting real property, the thumbprint] of each principal;
  (6) if identification of the principal is based on personal knowledge, a statement to that effect;
  (7) if identification of the principal is based on satisfactory evidence of identity pursuant to Section[s 5A-5 and] 8-2, a description of the evidence relied upon, including the date of issuance or expiration of any identification credential presented, and the name of any credible witness or witnesses;
  (8) the address where the notarization was performed, if not the notary's business address;
  (9) if the notarial act is performed electronically, a description of the electronic notarization system used; [and]
  (10) the fee, if any, charged by the notary[.][; and
  (11) if the notarial act is performed by means of audio-video communication pursuant to Chapter 5A of this [Act], the name of the jurisdiction in which the principal was located at the time of the electronic notarial act and any other information required by the [commissioning official] by rule pursuant to Section 15-2.]

(b) A notary shall not record a Social Security number in the journal.

Comment

Section 9-4 both mandates a notary journal entry for every notarial act performed and specifies the proper components of each entry. Most of the separate items enumerated are currently required or allowed by jurisdictions legislating the use of notary journals. (*See generally* ARIZ. REV. STAT. ANN. § 41-319; CAL. GOV'T CODE § 8206(a)(2); 57 PA. CONS. STAT. ANN. § 319(c) and TEX. GOV'T CODE § 406.014.) There are, however, some innovations.

[For electronic journals, Subparagraph (4) allows any other recognized

biometric identifier (*e.g.*, a retinal scan) to be captured in lieu of an electronic signature if the notary's journal technology so allows. No doubt, future technical advancements will make it easier for notaries who maintain an electronic journal to use biometric identifiers, which a host of electronic products now can capture and store. Also, for audio-video notarizations wherein the principal is not in the notary's physical presence (*see* Chapter 5A), the drafters determined that there must be a process whereby the absent principal's electronic signature or other biometric identifier is electronically captured at the remote site by the journal. The drafters recognize it is possible some jurisdictions may opt to do away with the traditional requirement of "signing the notary's journal" in the case of audio-video communication, believing that an electronic recording of a principal signing or acknowledging a record is more than sufficient proof that that individual intended to sign the record.]

Subparagraph (a)(5) accommodates journal entries for copy certification and verification of fact notarizations (*see* Section 5-1 and Comment), for which only the name and address of the requester of fact need be recorded. Subparagraphs (a)(4), (a)(6), and (a)(7) require only principals to sign a journal record[, affix a thumbprint,] and provide identification information. If certification of a copy or verification of certain other facts is the matter at issue (*e.g.*, whether two separate documents are congruent), there is no need for identity-related information to be recorded in the journal for a requester of fact. Indeed, it is not even necessary for the requester to be in the notary's physical presence. The drafters contemplated that copy certifications and verifications of fact might be requested by mail or electronic communication. If the requester of fact is present, the notary would not be prohibited from asking the person to sign the journal as evidence that the copy certification or verification of fact certificate was delivered.

[Subparagraph (a)(5) requires capture of principals' and witnesses' thumbprints for all real property documents. The provision is optional because some legislators might deem the requirement as too intrusive or controversial. This represents a slight policy shift from the 2010 Model Notary Act, which required a thumbprint for all notarizations. Proponents of the rule assert that modern technology has made fingerprinting clean, easy, and inexpensive. They posit that many impostors will be deterred from committing forgery because they will not want to leave a thumbprint behind in the notary's journal as proof of their attempted crime. Also, it was asserted, prosecutors will be aided by the journal evidence in bringing forgers to justice.]

Subparagraphs (a)(6) and (a)(7) compel the notary to record how the identity of the principal was established, including a description of any identification credentials or credible witnesses that were relied upon. The requirement pertains to electronic notarizations performed in the physical presence of a notary, since Section 8-2 authorizes the presentation of identification credentials. Additionally, the entry serves to memorialize proper performance of the act.

Subparagraph (a)(8) directs the notary to enter the location at which the notarization was performed, if not at the notary's normal business address. The purpose is to help protect the notary if the act is questioned in the future. Should the notary be called as a witness, this information can serve to refresh the notary's recollection regarding the transaction.

Subparagraph (a)(9) provides an additional requirement for electronic notarial acts. It directs the principal to provide information about the electronic

notarization system used to perform the electronic notarization.

Subparagraph (a)(10) requires the fee for the notarial act to be recorded in the journal. If a fee is not charged, good practice suggests that should be so noted in the journal.

[Subparagraph (a)(11) applies to Chapter 5A. A notary must keep a journal entry and a recording of the audio-video session. The notary must enter the jurisdiction where the principal was located (*e.g.*, California, France, Guam). If the commissioning official adopts rules specifying other information to be recorded, the notary must record that information in the journal.]

Subsection (b) responds to privacy concerns by precluding a notary from entering a Social Security number in a journal. (*See, e.g.*, TEX. ADMIN. CODE § 87.40, prohibiting notaries from recording any number from an identification credential that could be used to identify the signer, grantor, or maker of the record; MASS. GEN. LAWS ANN. ch. 222 §§ 22(c)(v)(1) and (d); and MISS. ADMIN. CODE tit. 1 pt. 5 Rule 5.16C.) Sophisticated criminals can exploit this information for illegal purposes. The drafters believe that this proscription is a prudent and necessary step toward protecting principals from identity theft and the concomitant hardships it can cause.

§ 9-5 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 official].

(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.

(e) If a notary public's journal is lost, stolen, or compromised, the notary shall notify the [commissioning official] on discovery of the loss, theft, or breach of security.

Comment

Section 9-5 lays down rules for safeguarding the notary journal as a valuable and sensitive record of official acts. Subsection (a) instructs the notary to protect not only the journal, but also any correlative notarial records. This might include the notary's commission or copies of communications from the commissioning official. The notary's journal and records may be surrendered only pursuant to a statute, court order, or directive of the commissioning official. Note, although law enforcement officials are permitted to access journals, they are not entitled to take physical custody of the journal absent a court order.

Subsection (b) requires the notary to safeguard the journal at all times. The drafters recognize that journals often contain sensitive, confidential information that merits protection. The requirement that the journal be kept in a secure area lends itself to reasonable interpretation. The objective is to shield the information in the journal from unauthorized use. Clearly, keeping the journal locked in a

desk under the notary's exclusive control meets the test. Other less secure measures might also be acceptable. Notaries who keep their journals at home must implement similar security measures. The drafters also believe that an electronic journal under the notary's sole control could be stored online on a server with appropriate authentication controlling access to the electronic journal.

Subsection (c) reinforces the rule that the journal is the notary's property. No other notary has a greater right than any member of the general public to inspect the journal, nor may another notary use it. Consequently, a notary who performs a notarial act but does not have the journal available may not record that act in the journal of another notary. Also, in some instances a person may become a notary at the behest of an employer who may presume that the notary's services will be exclusively for the employer's benefit. The Act, however, does not recognize a "notary private" and considers every notary to owe obligations to the general public, notwithstanding the fact that an employer may have absorbed the notary's commissioning costs. Consistent with this view, the Act declares that the notary's journal belongs exclusively to the notary and not the employer. The employer has inspection and copying rights similar to those of other members of the public. Nothing prohibits the employer from exercising these rights to create a separate photocopied log of employer-related notarizations. (*See, e.g.*, CAL. GOV'T CODE § 8206(d).) Consistent with this position, Subsection (c) states that the notary owns the duty of ensuring the journal goes with the notary when the employment relationship terminates, while Subsection (d) clarifies that an employer may not retain the journal of a departing employee.

Subsection (e) requires the notary to inform the commissioning official if, for any reason, the notary cannot continue to use the journal to record notarizations. Imposing this reporting requirement reinforces the view that the journal has official significance and must be handled with due care.

§ 9-6 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 official].

Comment

Section 9-6 addresses another controversial issue concerning the notary journal — whether or not it is a public record — and prescribes procedures for proper handling of the journal. Although a number of jurisdictions require notaries to maintain journals, not all consider the journal to be an accessible public record. (The statute of one such state provides that "a notary public shall keep confidential all documents and information contained in any documents reviewed by the notary public while performing his or her duties…and may release the documents or the information to a 3rd person only with the written consent of the person who requested the services of the notary public" (WIS. STAT. ANN. § 137.01(5m)). Another state requires the notary to keep confidential the address of a principal or witness to the notarization. (MASS. GEN. LAWS ANN. ch. 222§ 11(c)(iv).) The Act rejects the view that the journal is a true public record. Instead, it takes the position that the journal is quasi-public in nature. The Act controls and limits access to the journal by having it remain in the complete control of the notary, and by sensibly restricting its inspection by the general public.

Subparagraph (a)(1) establishes the principle that access to the journal is a privilege, not an absolute right. Thus, a person seeking to inspect the journal must provide basic information about a particular notarial act to qualify to inspect or receive a copy of an entry. The production of the signed, written request required by Subparagraph (a)(1) preserves the privacy rights of principals and eliminates "fishing expeditions." Subparagraph (a)(3) further promotes principals' privacy protection by limiting the inspection to only the specified entries. The Act requires the notary to exercise due care when making copies to ensure that other journal entries, or parts thereof, are neither revealed nor included as part of the copied material.

In seeking to balance the public's rights against unwarranted invasions of privacy, the Act adopts the position that all specific inspection requests must be granted, unless the notary believes either a criminal or harmful purpose will be served by allowing the inspection. (*See* Subsection (b).) The notary must have a "reasonable and explainable belief" that the person requesting the inspection bears a wrongful motive. The drafters recognized that this standard is neither easily defined nor applied. Additionally, there was concern over how the notary would make such a determination. The drafters' intent was to allow a notary to deny or limit access in those situations where the notary has prior knowledge or is able to formulate a compelling opinion regarding the request. As to the former, the notary may have been informed by a principal that he or she is being stalked or is the target of identity theft. Regarding the latter, when asked by the notary why the journal information is needed, the person might not be able to give a plausible response. In these situations, the notary is alerted to potential misuse of the information and should proceed with caution. To protect the personal safety and the private interests of persons named in the journal, Subsection (b) gives the notary discretion to deny access to the journal to any person the notary reasonably believes has a criminal or harmful intent. Notaries should be protected from becoming accessories to criminal or other wrongful acts. The subsection affords them this opportunity.

Subsection (c) makes it clear that, notwithstanding the protections provided by Subsection (b), notary journals are always subject to lawful inspection by appropriate authorities.

§ 9-7 Disposition of Journal.

(a) Upon resignation or expiration without renewal of a notary public commission, the notary shall retain the journal of notarial acts for ten years after performance of the last notarial act recorded in the journal, and the notary shall inform the [commissioning official] where the journal is located during this period.

(b) Upon revocation of a notary public commission, the notary shall transmit the journal to the [commissioning official] or to a repository approved by the [commissioning official].

(c) Upon the death or adjudicated incompetence of a current or former notary public, the notary's personal representative or guardian, or any other person knowingly in possession of the notary's journal, shall transmit the journal to the [commissioning official] or to a repository approved by the [commissioning official].

(d) 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.

Comment

Section 9-7 provides guidance on what to do with the journal and notarial records after the office is vacated or the commission terminated. This ensures that an entry or line item in the journal may be inspected or photocopied at a later date if a dispute or challenge to a notarized document arises.

In general, jurisdictions with journal requirements adopt one of several approaches. First, the notary retains and archives the journal for a period of time. (*See* MASS. GEN. LAWS ANN. ch. 222 § 24.) Second, the notary delivers the journals to the commissioning official. (*See* COLO. REV. STAT. § 12-55-115.) Third, the notary delivers the journals to the clerk of the county of the notary's residence or business address. (*See* CAL. GOV'T CODE § 8209.) Lastly, a notary enters into an agreement with his or her employer under which the journals are retained by the employer upon termination of employment. (*See* OR. REV. STAT. § 194.300(10).)

Subsection (a) implements the first option for notaries who resign or do not renew their commissions. The notary must keep the journal or journals for a period of ten years and inform the commissioning official where the journal or journals are stored.

Subsections (b) and (c) implement the second option for a notary whose commission is revoked, or who dies during the commission term or after having resigned or chosen not to renew the commission. Depositing journals under these circumstances with the commissioning official is preferable to the notary or the notary's representative retaining and archiving the journals as required under Subsection (a). If the notary's commission is revoked, there could be some doubt the notary will comply with a requirement to archive the journals for ten years. If the notary passes away, the drafters felt it was unrealistic to burden the notary's personal representative with this duty.

Subsection (d) requires the notary or the notary's representative to provide access instructions for an electronic journal stored in an online server or electronic notarization system. This is the functional equivalent of a notary physically delivering a bound journal to the commissioning official.

Chapter 10 — Fees for Electronic Notarial Acts

Comment

General: This Chapter addresses a variety of issues concerning the setting and charging of notarial fees for electronic notarial acts. The Act adopts the long recognized position that notaries are entitled to receive a fee for performing a notarization. As a convenience to consumers and to better serve their needs, the Act allows a notary to charge a "travel fee." This permits notaries to recover their costs incident to bringing notarial services to those unable to leave a residence, as well as other customers who expect such conveniences in a competitive marketplace. The Chapter also clarifies that a fee to recover the cost of accessing an electronic notarization system [or audio-video communication session] is included in the fee for the electronic notarization. Fees to recover the notary's expense in providing a copy of an entry in the notary's journal [or a recording of an electronic notarial act performed by audio-video communication] also are authorized in this Chapter.

§ 10-1 Maximum Fees

(a) The maximum fee that may be charged by a notary public for performing an electronic notarial act is:
  (1) for an acknowledgment, [amount in dollars] per signature;
  (2) for a verification on oath or affirmation, [amount in dollars] per signature;
  (3) for a signature witnessing, [amount in dollars] per signature;
  (4) for a copy certification, [amount in dollars] per copy certified; [and]
  [(5)] [for [other notarial act] as set forth in Section [____] in [_____], [amount in dollars] per act[.][; and]]
  [(6)] [for a protest, [amount in dollars] per protest[.][; and]]
  [(7)] [for a verification of fact, [amount in dollars] per fact verified[.]]

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

Comment

Section 10-1 establishes the maximum fee schedule. It identifies all of the different notarial acts, and provides a separate fee for each. The drafters did not include fee amounts. These decisions were deemed best left to the respective jurisdictions. The drafters anticipated that jurisdictions will permit higher fees for electronic notarizations than for their paper-based counterparts because of the costs necessary to perform electronic notarial acts. There also will be ongoing upgrade, maintenance, and security expenses associated with electronic notarizations. Fees for electronic notarizations must reasonably correspond to operating costs, yet be set at a level that does not make electronic notarial acts prohibitively expensive and thus discourage the use of electronic records.

Enumeration of the various notarial acts was not intended to indicate that each should carry a different fee amount. More than one type of electronic notarial act may command the same fee. (For example, the fee for an acknowledgment and a verification on oath or affirmation could be the same.) The list provides the opportunity to set different fee amounts for each of the authorized notarial acts. Some jurisdictions stipulate a single fee for any and all notarial acts (*see*, *e.g.*, 5 ILCS § 312/3-104(a); and IND. CODE ANN. § 33- 42-8-1), while others prescribe a fee for each different type of act (*see*, *e.g.*, HAW. REV. STAT. § 456-17; and N.M. STAT. ANN. § 14-12A-16D).

Subsection (b) clarifies that the reasonable cost of using of an electronic notarization system is included within the maximum fees authorized under Subsection (a). Unlike paper-based notarizations in which the costs for ink pens, notary public seals, and journals are relatively low and usually borne by the notary, electronic notarizations often require a notary to use an electronic notarization system with significant costs associated with its use.

Existing notary fee provisions are based on the model where the consumer or principal directly engages and pays the notary for services. (*See* Section 10-1 which states a *notary* is authorized to charge the stated maximum fees enumerated.) These laws did not envision the new business model that has emerged. Electronic notarization system providers have made significant financial investments to build their systems and market their services. To recover these costs and earn a profit, providers may charge the notary a per-transaction or subscription fee, or collect the maximum fee for the electronic notarization and pay the notary a portion of it. For example, in Virginia, an "electronic notary" may charge a maximum of $25 for an electronic notarial act. (VA. CODE ANN. § 47.1-19B.) Alternatively, the system provider might charge a principal $25 for accessing the system and pay a part of it to the notary as the latter's fee.

The drafters believe that 1) notaries are entitled to recover the reasonable costs of any transaction, subscription, or access fee required to use an electronic notarization system, and 2) there should be one fee for the electronic notarial act that compensates the notary for these reasonable expenses. Policymakers enacting Section 10-1 should specify a maximum fee that adequately anticipates these additional expenses.

§ 10-2 Travel Fee.

In addition to the maximum fee for performing an electronic notarial act, 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 fee set in Section 10-1 and neither specified nor mandated by law].

Comment

Section 10-2 addresses charging a travel fee incident to the performance of an electronic notarial act in the case when the notary and principal physically meet. A few jurisdictions currently permit a notary to charge for travel costs (*see*, *e.g.*, ARIZ. REV. STAT. ANN. § 41- 316B; N.M. STAT. ANN. § 14-12A-16E; and UTAH

CODE ANN. § 46-1-12(2)), and one jurisdiction sets a per-hour fee that varies according to the time of day the travel is performed (NEV. REV. STAT. § 240.100.3 and .4). Most state laws, however, are silent on this point. There are many homebound disabled or elderly persons, as well as individuals in remote areas, who need notarial services. Given the relatively small fees that can be charged for notarial services, it may not be reasonable to expect the notary to personally bear the cost of traveling to accommodate these people. In response, the Act permits the notary to be reimbursed for necessary costs incurred to provide these special services. The Act does not impose rigid guidelines, but there is an expectation that the travel fee will be reasonable. Gouging or otherwise taking advantage of a person needing at-home services may violate public policy and constitute official misconduct.

At a minimum, the travel fee may cover costs such as public transportation fares, or, if a private vehicle is used, gas, parking, and tolls. The drafters contemplated that the travel fee could include other expenses, as well. For example, if the situation necessitates that the notary spend a night away from home, reasonable accommodation and meal costs could be recoverable as part of the travel fee. Indeed, one state currently allows and sets per diem charges for notaries traveling to perform services within the state. (*See* ARIZ. REV. STAT. ANN. § 41-316B.) Additionally, although the term "travel fee" is used, the section was written so as not to preclude a jurisdiction from allowing a notary to include a charge for time spent traveling. Each jurisdiction must balance the potential cost of a "time charge" against the benefit of special-needs principals having a notary come to them. Also, although perhaps not to be encouraged, nothing in the section would preclude a principal from paying a notary solely for the convenience of having the notary come to a home or office, or other location such as an airport, at an odd hour, on a holiday, or in inclement weather.

Section 10-2 references either an existing travel fee provision in the jurisdiction's notary code or the rule provided in this Section. The latter imposes two extremely important limits on the use of travel fees. First and foremost, the notary and the principal or the principal's personal representative must agree upon the travel fee in advance. The drafters contemplated that this agreement will be made at the time the principal or representative asks the notary to travel and before the notary commits to the travel. Also, the agreement will specify the actual dollar amount or an exact method for computing the amount of the fee. Second, the principal must be informed that the travel fee is in addition to any notary fees to be charged for notarial acts, and not required by law but only payable by mutual agreement.

§ 10-3 Copying Fee.

A notary public may charge a reasonable fee pursuant to Section 9-6 of this [Act] to recover any cost of providing a copy of an entry in the journal of notarial acts [or of a recording of an audio-video communication session pursuant to Section 5A-6].

Comment

In Section 10-3, the drafters were particularly challenged by the issue of how properly to charge for copy-certifying an electronic record. Charging per page, as is the rule with copy-certifying a paper original, does not

correspondingly accommodate lengthy "scroll down" electronic pages. Charging by character or word count seemed fairer, although this method is less useful when graphic images are involved. One option is to have "file size" be the determining factor in establishing the fee, but often there will not be direct proportionality between the size of an electronic file and the complexity of the copy-certification task. The drafters decided that charging a fee based on the actual cost of providing the copy was the best approach to take.

Chapter 11 — Authenticity of Electronic Notarial Act

Comment

General: Chapter 11 provides for the authentication of electronically notarized records so that they may be honored in foreign jurisdictions. Section 11-1 dictates that an electronic authenticating certificate be attached to or logically associated with the notarized record in a way that imparts the same level of tamper-evident security as did use of an electronic notarization system by the notary. Section 11-2 prescribes a format and wording for the electronic certificate of authority, and Section 11-3 a maximum fee that may be charged by the commissioning official for issuance of the certificate.

§ 11-1 Evidence of Authenticity.

(a) Electronic evidence of the authenticity of the electronic signature and seal of a notary public of this [State] who is registered to perform electronic notarial acts, 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 notarized electronic record is exchanged between nations that are party to the Convention; or
   (2) an electronic certificate of authority signed by the [commissioning official] 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 tamper-evident manner.

Comment

Section 11-1 describes the electronic version of a certificate of authority used in authenticating a notarized electronic record. As with paper-based authentications, the forms of an electronic authenticating certificate are of two types: an electronic Apostille for electronic records exchanged between countries that are party to the commonly referenced "Hague Apostille Convention," and an electronic certificate of authority for countries not party to that Convention.

Past developments have paved the way for nations party to the Hague Apostille Convention of October 5, 1961, to issue and accept authentications of public documents in electronic form. The Hague Conference on Private International Law's 2003 Special Commission on the Practical Operation of the Hague Apostille, Evidence and Service Conventions concluded that "the spirit and letter of the Conventions do not constitute an obstacle to the usage of modern technology and that their application and operation can be further improved by relying on such technologies" (Conclusions and Recommendations 4). This conclusion guided the participants of the First International Forum on e-Notarization and e-Apostilles, held on May 30-31, 2005, to further affirm that "(it) is the view of the participants that an interpretation of the (Apostille) Convention in the light of the principle of functional equivalence permits competent authorities to both keep

electronic registers and issue electronic Apostilles to further enhance international legal assistance and government services" (Conclusions and Recommendations 1), and that "[c]ompetent authorities are encouraged to issue electronic apostilles" (Conclusions and Recommendations 13).

Therefore, nations party to the Hague Apostille Convention may issue electronic Apostilles. The Convention, however, does not establish specifically whether or not a party to it can issue an electronic Apostille to other non-participating nations. As with an Apostille in paper form, an electronic Apostille must conform to the content and format prescribed by the Convention in order for it to be recognized.

Subsection (b) provides the same security protection for electronic certificates of authority as is given to notarized electronic records themselves. Specifically, the section requires that the means for attaching or logically associating the certificate to the notarized record must produce evidence of any future tampering (*see* Section 2-19) with either the certificate or record. This conforms with the NASS Standards. (*See* NASS NAT'L ELEC. NOT. STAND., "Standards," *Requirements for Issuance of Electronic Apostilles and Certificates of Authentication,* 13 through 15 (2016).) The phrase, "attached to, or logically associated with" is borrowed from the UETA, where it is used to convey the concept that an electronic signature must be linked or connected with the electronic record being signed. (*See* UETA § 2(8) and Comment.) The drafters believed that a certificate from the commissioning authority that speaks to the authenticity of an electronic notary's act should maintain at the very least the same level of security as the underlying notarized record.

§ 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 seal of a notary public of this [State] who is registered to perform electronic notarial acts 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, was registered to perform electronic notarial acts and authorized to act at the time and place the record was electronically notarized.

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__.

(Electronic signature and seal of [commissioning official])

Comment

Section 11-2 prescribes a certificate of authority for issuance by the commissioning official that in a straightforward manner provides the

necessary assurances to third parties relying upon a particular notarized electronic record and confirms an electronic notary's authority to notarize that record. Implicit in this confirmation is the assurance that the record has the security features required by the Act. The certificate of authority states that the notary "was registered to perform electronic notarial acts and authorized to act at the time and place the record was electronically notarized." (*See* Section 2-20, defining venue as "the jurisdiction where the notary public is physically located while performing an electronic notarial act.")

§ 11-3 Fee for Electronic Apostille or Certificate of Authority.

For issuing an electronic Apostille or certificate of authority for an electronic notarial act performed by a notary public of this [State], the [commissioning official] may charge a maximum fee of [amount in dollars].

Comment

Section 11-3 authorizes the commissioning official to charge a fee for issuing an electronic Apostille or certificate of authority for a notarized electronic record. This is consistent with the practice for non-electronic certificates of authority and Apostilles. The specific dollar amount is not set, but instead left to the discretion of the lawmakers of each jurisdiction.

Chapter 12 — Changes of Status of Registered Notary

Comment

General: This chapter provides rules for notaries to follow in reporting pertinent changes in their status to the commissioning official. The provisions correspond to similar rules imposed on traditional "paper-based" notaries (*see* CAL. GOV'T CODE § 8213.5 and § 8213.6; and N.C. GEN. STAT. §§ 10B-50 through 10B-53), but the distinctive nature of the notary's duties in performing electronic notarial acts require that some additional status changes be reported.

§ 12-1 Change of Registration Information.

Any change to the information submitted by a notary public in registering to perform electronic notarial acts in compliance with Section 3-4 of this [Act] shall be reported by the notary within [five] business days to the [commissioning official].

Comment

Section 12-1 requires notaries to report significant changes in information that had been submitted to the commissioning official either at the time of registration or subsequent thereto. This might include any action taken against a notary's professional license (*e.g.*, revocation of a real estate or insurance license). [The same requirements apply if the jurisdiction requires the notary to file a surety bond pursuant to Subsection 3-4(4). (*See* Section 5A-3.)] A reporting deadline of 5 calendar days was adopted because any lengthy delay in reporting these matters could pose a risk to the public if the notary were to continue to perform electronic notarial acts without principals being fully aware of a notary's personal qualifications.

§ 12-2 Termination or Suspension of Registration.

(a) Any revocation, resignation, expiration, or suspension of the commission of a notary public terminates or suspends any registration to notarize electronically.

(b) The [commissioning official] may terminate or suspend the registration to perform electronic notarial acts of a notary public who fails to comply with any section of this [Act].

(c) A notary public may terminate registration to notarize electronically and maintain the underlying notary public commission.

(d) A notary public may terminate registration to notarize electronically by notifying the [commissioning official] of that fact by means approved by the [commissioning official] and disposing of all or any part of an electronic notarization system in the notary's sole control whose exclusive purpose was to perform electronic notarial acts.

Comment

Section 12-2 addresses matters related to termination of registration to perform electronic notarial acts. Subsection (a) states a basic rule: termination or

suspension of the notary's commission, for any reason, concomitantly terminates or suspends the electronic notarization registration. The underlying notary public commission is the foundation upon which the authority to perform any notarial act is founded, whether it be paper-based or electronic.

Subsection (b) follows logically from Section 3-5, where the commissioning official may reject the registration of any notary who fails to comply with any section of the Act. Section 3-5 not only authorizes the commissioning official to reject a registration application for a violation of the Act during a previous registration term, but also to take action for proper cause for a violation during the current registration term. Section 12-2(b) permits a commissioning official to impose sanctions for any violation of the Act.

Subsection (c) makes clear that a notary may voluntarily terminate registration without jeopardizing an otherwise valid notary commission.

Subsection (d) instructs the notary on the steps to be taken for voluntary termination of registration. The phrase "whose exclusive purpose was to perform electronic notarial acts" does not apply to such items as cell phones, laptop computers, and tablet devices that may be used for purposes other than performing electronic notarial acts. The Act does not require disposal of these tools. A cryptographic token containing a public key certificate issued solely to the notary for the purpose of creating the notary's electronic signature is one example of an electronic notarization system subject to disposal. The disposal might entail permanently erasing or expunging software, or physically disabling or destroying hardware. This provision is the analogue to the requirement that a notary destroy the physical notary seal used in paper-based notarizations.

§ 12-3 Disposal of Electronic Notarization System.

(a) Except as provided in Subsection (b), when the commission of a notary public who is registered to notarize electronically expires or is resigned or revoked, or when such notary dies or is adjudicated as incompetent, the notary or the notary's personal representative or guardian within [thirty] days shall dispose of all or any part of an electronic notarization system that had been in the notary's sole control whose exclusive purpose was to perform electronic notarial acts.

(b) A former notary public whose previous commission expired need not comply with Subsection (a) if this individual, within [thirty] days after commission expiration, is recommissioned as a notary and reregistered to perform electronic notarial acts.

Comment

Section 12-3 mandates that the software and other electronic devices used exclusively as an electronic notarization system to create the notary's electronic seal and signature be properly disposed of within 30 days to prevent their misuse by unauthorized parties. This corresponds to the rule for the proper disposal of the tools of office for the paper-based notary, *i.e.*, seal and journal.

Under Subsection (a), an electronic notarization system need not be permanently erased, expunged, or disabled if it were not used "exclusively" to perform electronic acts. Such items could continue to be used on electronic records in the notary's personal and other non-notarial affairs.

Subsection (b) allows a notary "renewing" a commission to avert the disposal procedure set forth in Subsection (a) if the notary intends to be recommissioned and reregistered to perform electronic notarial acts within 30 days after the original commission expires. These two processes may be accomplished at the same time. (*See* Subsection 3-1(c).)

Chapter 13 — Liability, Sanctions, Remedies, and Protections

Comment

General: Chapter 13 makes clear that the basic penalties and remedies for improper performance of electronic notarial acts are the same as those imposed or permitted for improper performance of traditional non-electronic notarizations. Sections 13-1 and 13-2 apply existing misconduct laws for paper-based notarization to the electronic realm. Section 13-3 clarifies that remedies sought against a notary for any electronic act that was purported to be improperly performed must be pursued in courts within the jurisdiction where the notary performed the act and is commissioned.

§ 13-1 Improper Electronic Acts and False Registration.

The liability, sanctions, and remedies for the improper performance of an electronic notarial act, or for providing false or misleading information in registering to perform electronic notarial acts, shall be the same, respectively, as for the improper performance of non-electronic notarial acts, as set forth in Section [____] of [_____], or for providing false or misleading information in applying for a notary public commission, as set forth in Section [____] of [_____].

Comment

Section 13-1 applies the liability, sanctions, and remedies in existing notary statutes to correlative provisions for electronic notarizations under this Act. These statutes assign liability to the notary (*see* 5 ILCS § 312/7-101; MICH. COMP. LAWS § 55.297(1); NEB. REV. STAT. § 64-109; TEX. CIV. PRAC. AND REMEDIES CODE § 121.014; and W.VA. CODE § 39-4-32(a)) and even to the employer of a notary (*see* CONN. GEN. STAT. ANN. § 3-94l(b); 5 ILCS § 312/7-102; MICH. COMP. LAWS § 55.297(1); NEV. REV. STAT. ANN. § 240.150.2; and VA. CODE ANN. § 47.1-27), establish penalties for various offenses (*see* CAL. GOV'T CODE § 8214.1 and § 8214.15; and MICH. COMP. LAWS § 55.300a and § 55.301), and specify other penalties and remedies, such as for engaging in the unauthorized practice of law (*see* MO. ANN. STAT. § 486.390).

Section 13-1 authorizes the commissioning official to suspend or revoke the commission of a notary registered to notarize electronically for 1) a violation of the Act in performing such electronic notarizations, or 2) providing misleading information in registering to perform electronic notarizations. Certain violations, such as a failure to require the principal to appear in person before the notary (*see* Section 5-3(b)) or to verify the identity of a principal (*see* Chapter 8), are sufficiently egregious to warrant both termination of the electronic notarization registration (*see* Section 12-2(b)), and revocation of the underlying notary public commission. The commissioning official will have discretion to determine whether a particular offense merits taking action against a notary's commission.

§ 13-2 Rights of Notice and Appeal.

All of the rights of notice and appeal of any disciplinary action that are

permitted to notaries public performing notarial acts, as set forth in Section [____] of [_____], as well as any action authorized under Section 12-2, shall also apply to notaries performing electronic notarial acts.

Comment

Section 13-2 provides a notary public who is subject to a disciplinary action the right to due process as prescribed under the jurisdiction's notary code or administrative law procedures.

Chapter 14 — Violations by Individual Not a Notary

Comment

General: This chapter provides disciplinary sanctions that can be imposed on non-notaries who wrongfully perform or interfere with official notarial acts.

§ 14-1 Impersonation and Improper Influence.

Any individual impersonating a notary public registered to perform electronic notarial acts, or soliciting, coercing, or influencing a notary to act improperly, is subject, respectively, to the same sanctions applying to impersonation of a notary public as set forth in Section [____] of [_____], and to the improper influence of non-electronic notarial acts as set forth in Section [____] of [_____].

Comment

Section 14-1 addresses acting as a notary without authorization. It makes clear that such action is illegal and subject to criminal penalties. This position is common to many jurisdictions. (*See, e.g.*, COL. REV. STAT. § 12-55-117; VA. CODE ANN. § 47.1- 29; and W. VA. CODE ANN. § 39-4-33(c).). Some jurisdictions also address improperly influencing a notary to perform a notarial act. (CAL. GOV'T CODE § 8225; and NC GEN. STAT. 10B-60(j).)

§ 14-2 Wrongful Destruction or Possession.

Except as provided in Subsections 12-2(d) and 12-3(a) of this [Act], any person who knowingly obtains, conceals, damages, or destroys all or any part of an electronic notarization system whose exclusive purpose was to perform electronic notarial acts is guilty of a _____[class of offense], punishable upon conviction by a fine not exceeding _____[amount in dollars] or imprisonment for not more than _____[term of imprisonment], or both.

Comment

Section 14-2 is analogous to the wrongful possession or destruction of the seal or journal of a paper-based notary. This section imposes the same criminal liability for any person who engages in similar acts with respect to the tools needed to perform an electronic notarial act. The penalty, however, exempts circumstances in which these electronic tools have been lawfully disposed of by the notary (or another person) because the notary has 1) terminated registration to perform electronic notarizations, 2) allowed the commission to expire, 3) died, or 4) been adjudicated as incompetent.

§ 14-3 Additional Sanctions Not Precluded.

Imposition of the sanctions of this Chapter do not preclude other sanctions and remedies provided by law.

Comment

Section 14-3 allows a person victimized by a non-notary public who violates Sections 14-1 or 14-2 to seek any further redress that may be afforded by other applicable law, including a civil action.

Chapter 15 — Rules

Comment

General: Chapter 15 provides the commissioning official rule-making power to implement the Act. Section 15-1 confers broad discretion upon the commissioning official as to the nature and timing of the rules as well as the ability to amend or repeal them. This discretion will enable the commissioning official to provide notaries guidance on how to address technical advancements or other changes in the field. [Section 15-2 requires the commissioning official to establish rules as specified by Section 5A-5 of the Act.]

§ 15-1 Authority to Promulgate Rules.

The [commissioning official] may adopt rules to implement this [Act] prior to or any time after its effective date. The authority includes the right to amend or repeal any rule.

Comment

The drafters recognize that an enacting jurisdiction may opt to give the commissioning official authority to adopt any regulations deemed necessary to ensure that electronic notarizations are properly performed. Section 4-1(a) identifies electronic notarization systems as an area where additional rules may be needed.

[§ 15-2 Chapter 5A Rules.

The [commissioning official] shall adopt rules to implement Section 5A-5 prior to the effective date of this [Act].

Comment

Whereas rules under Section 15-1 are discretionary, Section 15-2 requires that the notary commissioning official of a jurisdiction enacting the bracketed Chapter 5A and other provisions in the Act related to audio-video communication (*see* Sections 2-1, 5-3(c), and 6-2(b)) adopt rules to implement Section 5A-5. For guidance in the formulation of these rules, *see* Appendix II.]

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.

Appendix III — How to Implement the MENA as an Administrative Rule Under the Revised Uniform Law on Notarial Acts

The Model Electronic Notarization Act ("MENA") is intended to be enacted as legislation to supplement or replace existing notary statutes. Nonetheless, its detail and structure lend themselves to adoption as a set of administrative rules. Indeed, the MENA may be adapted as an implementing set of administrative rules for states and jurisdictions which have enacted the Revised Uniform Law on Notarial Acts ("RULONA") published by the Uniform Law Commission.

The RULONA includes provisions allowing notaries to use electronic signatures, requires notaries to notify the commissioning officer or agency of their intent to notarize electronic records, and stipulates that the technology used to create an electronic signature must be "tamper-evident." Most notably, the RULONA authorizes the commissioning officer or agency to publish rules "prescribing the manner of performing notarial acts regarding … electronic records," ensuring "that any change to or tampering with a record bearing a certificate of a notarial act is self-evident," and ensuring "integrity in the creation, transmittal, storage, or authentication of electronic records or signatures." Rules also may be published to "prevent fraud or mistake in the performance of notarial acts" (Section 27). Thus, a jurisdiction that enacts the RULONA may use the MENA as its model for implementing the electronic notarization provisions for its jurisdiction. The MENA also may be adopted as an administrative rule if a jurisdiction has not enacted the RULONA, but already has a statute in place authorizing the commissioning officer or agency to promulgate rules to implement its notary laws.

There are several reasons for adopting the MENA provisions through rule-making. First, adopting a rule through existing authority may be the simplest way to implement standards for electronic notarization. Second, the unusual detail of the MENA makes it well suited to serve as a set of administrative rules. Third, as technology advances, generally it will be easier to amend a rule than a statute.

Appendix III presents a model for implementing the MENA as administrative rules under the RULONA. It takes applicable chapters and sections from the MENA[1] and organizes them in a regulatory format. Instead of utilizing the MENA section conventions, such as "§ 2-4," it uses "Rule 2.4." Where possible, the drafters retained the same chapter and section numbers to facilitate comparison with the corresponding provisions of the MENA.

---

[1] The proposed rules do not include every section or chapter. The provisions on satisfactory evidence of identity in Chapter 8, and the criminal offenses that comprise Chapters 13 and 14 are omitted since they deal with matters typically codified into statute. The drafters determined that they are outside the scope of an administrative rule and best implemented through legislative enactment.

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).

Appendix IV — History of Electronic Notarization Laws

This Appendix chronicles the significant statutory enactments affecting electronic notarization in the United States since 1996, as well as pertinent regulatory adoptions achieved through administrative rule-making.

The Appendix is divided into four sections. The first lists and summarizes the uniform and model acts which inspired most of the cited enactments and adoptions. The second notes the national standards published by the National Association of Secretaries of State. The third covers pertinent U.S. federal legislative and regulatory history. The fourth details the individual state and the District of Columbia legislative and regulatory histories. State enactments and adoptions of the uniform and model laws and national standards presented in the first and fourth sections are noted, as well as other statutes and regulations not based on these uniform or model laws and standards.[1]

Legislative bills are cited, along with the applicable chapter or public act number, where provided. Where available, hyperlinks to bill and rule text are provided.[2] Hyperlinks were accurate at the time of publication.

Uniform and Model Acts

Year	Law or Standard	Summary
1999	UETA (ULC)	Clarifies that a notary or notarial officer may use electronic signatures (Sec. 11).[3]
2002	MNA of 2002 (NNA)	Sets requirements for registering and maintaining status as an e-notary; powers and limitations of e-notaries; rules related to fees; e-signatures and e-seals; and authentication of e-notarizations; and provides sanctions for violations.

[1] The following abbreviations are used throughout this Appendix: "Admin." for Administrative; "CA" for certificate authority; "DoS" for Department of State; "e-" for electronic; "MENA" for Model Electronic Notarization Act; "MNA" for Model Notary Act; "NASS" for National Association of Secretaries of State; "NES" for National E-Notarization Standards; "NNA" for National Notary Association; "P.A." for Public Act; "P.L." for Public; "Sec." for Section and "SS." for "Sections; "SoC" for Secretary of the Commonwealth; "SoS" for Secretary of State; "Sess." for Session; "RULONA" for Revised Uniform Law on Notarial Acts; "UETA" for Uniform Electronic Transactions Act; "ULC" for Uniform Law Commission; and "URPERA" for Uniform Real Property Electronic Recording Act.

[2] Hyperlinks are applicable only to the MENA published in electronic form.

[3] SECTION 11. NOTARIZATION AND ACKNOWLEDGMENT. If a law requires a signature or record to be notarized, acknowledged, verified, or made under oath, the requirement is satisfied if the electronic signature of the person authorized to perform those acts, together with all other information required to be included by other applicable law, is attached to or logically associated with the signature or record.

Year	Law or Standard	Summary
2004	URPERA (ULC)	Applies UETA Sec. 11 to electronic real property documents, and clarifies that a physical or electronic image of a notary seal is not required when notarizing these records (Sec. 3).[4]
2010	MNA of 2010 (NNA)	Revises and updates the 2002 MNA's Article III provisions on e-notarization.
2010	RULONA (ULC)	Sets rules for notarial acts on paper and electronic records; requires a notary to notify the commissioning official of the notary's intent to perform notarial acts on electronic records; permits a notary to select one or more tamper-evident technologies to notarize e-records and prohibits a person from requiring a notary to use a technology the notary has not selected; clarifies that any technology a notary uses must comply with standards set by the commissioning official; requires the commissioning official to maintain an electronic database of notaries; and authorizes rule-making.
2017	MENA (NNA)	Revises and updates the 2010 MNA's Article III provisions so that they may stand alone from Articles I and II and be enacted alongside any jurisdiction's current notary laws.
	National Standards	
2006 2011 2016	NES (NASS) (Reaffirmed without change) (Reaffirmed without change)	Publishes standards for the registration of e-notaries; the form, manner of performing, and security of e-notarizations; and the authentication of e-notarizations.
	United States	
2000	S.B. 781, P.L. 106-229 (Electronic Signatures in Global and National Commerce Act — "E-SIGN")	Applies the language of UETA Sec. 11 to a transaction in or affecting interstate or foreign commerce.

[4] SECTION 3. VALIDITY OF ELECTRONIC DOCUMENTS. …
(c) A requirement that a document or a signature associated with a document be notarized, acknowledged, verified, witnessed, or made under oath is satisfied if the electronic signature of the person authorized to perform that act, and all other information required to be included, is attached to or logically associated with the document or signature. A physical or electronic image of a stamp, impression, or seal need not accompany an electronic signature.

Year	Law or Standard	Summary
2006	Regulations Adding 26 CFR Part 1 § 1.401(a)-21 to the Treasury Regulations and 5 CFR Part 850 § 850.106(a)-4 to the Admin. Personnel Regulations	Provides that if a participant's signature on a retirement plan is witnessed in the physical presence of a notary, an e-notarization performed in accordance with E-SIGN Sec. 101(g) and state law applicable to notaries will not be denied legal effect. Further allows the Director of the Office of Personnel Management to provide directives that alternate procedures such as audio-video conference technology used by a notary or other official authorized to administer oaths will be deemed to satisfy the physical presence requirement but only if they offer the same safeguards as are provided through physical presence.

U.S. States and Jurisdictions

Alabama		
2001	H.B. 170, Act No. 2001-458	Enacts UETA Sec. 11.
2009	S.B. 90, Act No. 2009-510	Enacts URPERA Sec. 3.
Alaska		
2004	H.B. 285, Ch. 110	Enacts UETA Sec. 11.
2005	H.B. 97, Ch. 60	Authorizes a notary to sign and seal an electronic document by electronic means as authorized by regulation.
Arizona		
2000	H.B. 2242, Ch. 210	Enacts an entire article on e-notarization, with commissioning rules, authorized acts, ethical standards, requirements for electronic documents, and rule-making authorization for e-notarization; allows the performance of e-notarizations, as specified, in the presence of an e-notary, while also prescribing rules for e-notarizations to be performed by a signer without the presence of an e-notary; and defines "electronic acknowledgment."
2000	H.B. 2069, Ch. 268	Adopts an amended version of UETA Sec. 11 and clarifies that an imprint of a notary seal is not required if certain conditions, as specified, apply.
2003	Admin. Rules Adding Article 12 to Ch. 12, Title 2 of the Arizona Admin. Code	Provides rules for e-notary applications, bonds, filing fees, notary journals, e-notary tokens, notary electronic service certificates, time stamp token providers,

Year	Law or Standard	Summary
		and maximum fees, and sets penalties.
2005	S.B. 1354, Ch. 109	Enacts URPERA Sec. 3.
2005	H.B. 2150, Ch. 124	Amends the e-notarization law enacted in 2000 (*see* H.B. 2242, Ch. 210 *above*).
2010	H.B. 2037, Ch. 313	Repeals prior law allowing an e-notary to issue a "notary service electronic certificate" for performing e-notarizations without the e-notary present (*see* H.B. 2242. Ch. 210 *above*).
Arkansas		
1999	S.B. 418, Act No. 718	Defines "electronic signature" and provides that when a person or other entity accepts or agrees to be bound by an electronic record, any rule of law which requires a witness or notary is satisfied by the witness's or notary's e-signature.
2001	S.B. 159, Act No. 905	Enacts UETA Sec. 11.
2007	H.B. 1298, Act No. 734	Enacts URPERA Sec. 3.
2013	Admin. Rules for Electronic Notarial Acts in the State of Arkansas	Provides rules for commissioning a "traditional" notary as an e-notary to perform e-notarizations using public key cryptography, requires an e-notary to perform e-notarizations using public key cryptography, requires an e-notary to complete a training course every 2 years, sets maximum fees, and requires e-notarizations to be performed in the physical presence of the notary.
California		
1999	S.B. 820, Ch. 428	Enacts UETA Sec. 11 in substance.
2004	A.B. 578, Ch. 621	Allows a "digital" reconveyance deed, substitution of trustee and assignment of deed of trust to be e-notarized, and clarifies that a requirement for a notary's seal is satisfied by including certain information, as specified.
2005	A.B. 2805, Ch. 579	Provides that an electronic advance care directive or durable power of attorney for health care is legally sufficient if it is acknowledged before a notary.
2016	A.B. 2143, Ch. 380	Allows any electronic record that is an instrument to be recorded and consistent with Government Code 27201 to be e-notarized and recorded.
Colorado		
2002	H.B. 02-1326, Ch. 229	Enacts UETA Sec. 11.

Year	Law or Standard	Summary
2004	H.B. 1300, Ch. 101	Provides that a notary's e-signature must contain or be accompanied by a document authentication number (DAN) issued by the SoS, stipulates that notaries must maintain a journal for e-notarizations, and sets maximum fees.
2004	Notary Program Rules in 8 CCR 1505-11	Establishes rules for notaries to notify the SoS of the intent to e-notarize, report status changes, and use and secure DANs and e-signatures.
2005	H.B. 1136, Ch. 88	Directs the SoS to adopt rules allowing "pictorial notaries" to transmit encrypted, authenticated photographs of individuals for use by certain agencies, as specified.
2009	S.B. 111, Ch. 180	Repeals Ch. 180 of 2009.
2014	Admin. Rules Amending Notary Program Rules in 8 CCR 1505-11	Recodifies 2004 rules on e-notarization, updates rules related to DANs, and repeals certain prior rules.
Connecticut		
2002	S.B. 561, P.A. No. 02-68	Enacts UETA Sec. 11.
2008	H.B. 5535, P.A. No. 08-56	Enacts URPERA Sec. 3.
2013	Admin. Rule Adding SS. 7-35ee to 7-35ee-10 to the Connecticut Admin. Code	Adopts URPERA rules, requires records containing e-signatures or notarizations to conform to all applicable standards established by the SoS and to all applicable sections of the Connecticut General Statutes.
Delaware		
2000	H.B. 492, Ch. 457	Enacts UETA Sec. 11.
2005	H.B. 79, Ch. 23	Enacts URPERA Sec. 3.
2009	S.B. 246, Ch. 280	Enacts e-notarization provisions based on MNA 2002 for commissioning e-notaries, requiring an educational course, using an e-journal, setting maximum fees, and authorizing the SoS to authenticate e-notarizations.
District of Columbia		
2000	B14-0051, Act No. 14-28	Enacts UETA Sec. 11.
2005	B16-0173, Act No. A16-0134	Enacts URPERA Sec. 3.
Florida		
2000	S.B. 1334, Ch. 2000-164	Enacts UETA Sec. 11, and requires first-time notary commission applicants to take an educational course with a curriculum that includes e-notarization.
2007	S.B. 2038, Ch. 2007-233	Enacts URPERA Sec. 3.

Year	Law or Standard	Summary
2007	H.B. 1305, Ch. 2007-257	Authorizes notaries to perform e-notarizations, applies laws for paper-based notarizations to e-notarizations, prescribes standards for e-signatures based on NASS NES, allows an e-notarization without using the official physical seal of a notary if certain information, as specified, is included, and authorizes rule-making.
2010	Admin. Rules for E-notarization Adding SS. 1N-5.001 and 1N-5.002 to the Florida Admin. Code	Provides that a notary's e-signature may be affixed by an "electronic notary system," as defined, or by a public key certificate, and sets rules for these systems and certificates.
Georgia		
1997	S.B. 103, Act No. 394	Defines "electronic signature."
1999	S.B. 62, Act No. 272	Modifies the definition of "electronic signature" and clarifies that an e-signature is not limited to a "secure electronic signature," as defined, and that any rule of law which requires a notary public signature shall be deemed satisfied by the secure electronic signature of the notary.
2009	H.B. 127, Act No. 140	Enacts URPERA Sec. 3.
2009	H.B. 126, Act No. 141	Repeals Act Nos. 394 of 1997 and 272 of 1999 and enacts UETA Sec. 11.
Hawaii		
2000	H.B. 2585, Act No. 00-282	Enacts UETA Sec. 11.
2009	H.B. 271, Act No. 09-102	Enacts URPERA Sec. 3.
Idaho		
2000	S.B. 1334, Ch. 286	Enacts UETA Sec. 11.
2007	S.B. 1018, Ch. 63	Enacts URPERA Sec. 3.
Illinois		
2007	S.B. 319, P.A. 95-472	Enacts URPERA Sec. 3.
2010	Admin. Rule Adding Sec. 1400.30 to the Illinois Admin. Code	Adopts URPERA rules and provides that an e-signature and e-notarization submitted to a county recorder shall comply with the Illinois Electronic Commerce Security Act and E-SIGN insofar as the Illinois URPERA does not supersede those laws, the Illinois Notary Public Act, and any other laws governing that signature or notarization.

Year	Law or Standard	Summary
Indiana		
2000	H.B. 1395, P.L. 62-2000	Enacts UETA Sec. 11.
Iowa		
2000	H.F. 2205, Ch. 1189	Enacts UETA Sec. 11.
2012	S.F. 2265, Ch. 1050	Enacts the RULONA provisions related to notarization of electronic records; allows the SoS to adopt rules; clarifies that "personal appearance" does not mean appearances which require video, optical, or technology with similar capabilities; and provides that e-notarization of a signature performed in another state will be recognized in Iowa provided that the act is performed in the physical presence of the notarial officer of that state.
2014	Admin. Rules Adding Sec. 721-43.5(9B) to the Iowa Admin. Code	Provides that a notarized document is in compliance with the requirements for a notarial act on an electronic record under Iowa Code Ch. 9B when it is submitted and accepted on the state of Iowa electronic document management system administered by the Iowa judicial branch.
Kansas		
2000	H.B. 2879 (Senate Substitute), Ch. 120	Enacts UETA Sec. 11 and authorizes the SoS to publish rules for e-notarization.
2005	Admin. Regulations Adding SS. 7-43-1 to 7-43-6 to the Kansas Admin. Regulations	Establishes registration procedures for e-notaries; requires e-notaries to complete a course and exam; requires an e-notary to use a digital signature authorized by the SoS and ensure that the digital certificate used to create the e-notary's digital signature is valid and has not expired, been revoked or terminated when the e-notarization is performed; requires the principal to personally appear before the notary for an e-notarization; authorizes the SoS to authenticate the electronic signature and seal of an e-notary; and provides that the statutes applicable to paper-based notarizations apply to e-notarizations.
2006	S.B. 336, Ch. 145	Enacts URPERA Sec. 3.
Kentucky		
2000	H.B. 571, Ch. 301	Enacts UETA Sec. 11.

Year	Law or Standard	Summary
Louisiana		
2001	S.P. 995, L.D. 2557, P.L. No. 762	Enacts UETA Sec. 11.
Maine		
1999	S.P. 995, L.D. 2557, P.L. No. 762	Enacts UETA Sec. 11.
Maryland		
2000	S.B. 3, Ch. 8	Enacts UETA Sec. 11.
Massachusetts		
2003	S.B. 2076, Ch. 133	Enacts UETA Sec. 11.
Michigan		
2000	H.B. 5537, P.A. No. 305	Enacts UETA Sec. 11.
2003	H.B. 4938, P.A. No. 238	Adds UETA definitions of "electronic" and "record," clarifies that "signature" includes an e-signature, and allows notaries to imprint electronically or use an electronic process to add a notary's commission information on a record.
2010	S.B. 791, P.A. No. 123	Enacts URPERA Sec. 3.
Minnesota		
1997	S.F. 173, Ch. 178	Equates use of a digital signature with the notarial act of acknowledgment regardless of whether certificate wording appears with the digital signature or the signer appeared before the CA when the digital signature was created.
2000	H.F. 3109, Ch. 371	Enacts UETA Sec. 11.
2000	S.F. 2783, Ch. 395	Clarifies that a digital signature satisfies the requirement for an acknowledgment under M.S. 358.41, and that if a digital signature is used as an acknowledgment, the CA issuing the certificate is liable to the same extent as a notary, up to any limit of liability stated in the CA's practice statement, for failure to satisfy the requirements of an acknowledgment.
2006	H.F. 2656, Ch. 260	Adds definitions of "electronic record" and "electronic signature" from UETA, authorizes notaries to perform e-notarizations, requires notaries who wish to perform e-notarizations to register, prohibits notaries from notarizing the e-signature of a signer who is not in the

Year	Law or Standard	Summary
		notary's presence, and provides rules for using an electronic seal and completing an electronic notarial certificate.
2008	H.F. 3516, Ch. 238	Enacts URPERA Sec. 3.
Mississippi		
2001	S.B. 2678, Ch. 400	Enacts UETA Sec. 11.
2011	H.B. 599, Ch. 364	Enacts URPERA Sec. 3.
2012	Admin. Rule Amending Title 36, Part 201 of the Mississippi Admin. Code	Adopts URPERA rules and permits chancery clerks to accept electronic real property records with e-notarizations for recordation provided that the state where the electronic real property document has been notarized has enacted e-notarization laws and adopted e-notarization rules to effectuate these laws.
Missouri		
1998	S.B. 680	Equates a digital signature with the notarial act of acknowledgment regardless of whether certificate wording appears with the digital signature or the signer appeared before the CA when the digital signature was created.
2003	H.B. 254	Repeals equating use of a digital signature with an acknowledgment, and enacts UETA Sec. 11.
2016	S.B. 932	Authorizes the SoS to adopt rules for e-notarization.
Montana		
2001	H.B. 234, Ch. 52	Enacts UETA Sec. 11.
2015	S.B. 306, Ch. 391	Enacts the RULONA provisions related to notarization of electronic records and allows a principal to appear before a notary by means of audio-video communication for certain types of transactions.
2015	Admin. Regulations Creating Sec. 44.15.108 of the Admin. Rules of Montana	Sets rules for notarizations performed using audio-video technology.
Nebraska		
2000	L.B. 929	Enacts UETA Sec. 11.
2016	L.B. 465	Establishes rules for registering as an e-notary and for using e-notary signatures and seals, requires signers to be physically present before the e-notary

Year	Law or Standard	Summary
		for any e-notarization, and permits the SoS to promulgate rules for e-notarizations and the approval of solution providers.
Nevada		
1999	A.B. 674, Ch. 418	Directs the SoS to adopt rules for use of a digital signature as an acknowledgment.
1999	Admin. Regulations Creating Sec. 720.770 of the Nevada Admin. Code	Provides that a digital signature that is verifiable by the public key set forth in the digital certificate satisfies the requirements for an acknowledgment, as the term is defined in NRS 240.002 under certain conditions.
2001	S.B. 49, Ch. 548	Enacts UETA Sec. 11.
2007	S.B. 88, Ch. 57	Enacts URPERA Sec. 3.
2009	S.B. 92, Ch. 499	Enacts the Electronic Notary Public Authorization Act, adds definitions, establishes procedures for appointment and maintaining status as an e-notary, requires e-notaries to complete a course and examination, sets rules for an e-notary's bond, establishes maximum fees, prescribes rules for e-notary signatures and certificates, requires e-notaries to keep a journal of all e-notarizations, and empowers the SoS to issue authentications of e-notarization and adopt regulations.
New Hampshire		
2001	S.B. 139, Ch. 265	Enacts UETA Sec. 11.
New Jersey		
2001	S.B. 1183, Ch. 116	Enacts UETA Sec. 11.
2014	Admin. Rules Adding SS. 15:3-9.1 to 15.3-9.13 to the New Jersey Admin. Code	Requires that an electronic document submitted for recording in New Jersey be notarized in conformance New Jersey Statutes Annotated 12A:12-11.
New Mexico		
2001	H.B. 232, Ch. 2001-131	Enacts UETA Sec. 11.
2007	S.B. 201, Ch. 2007-261	Enacts URPERA Sec. 3 and permits the SoS to promulgate rules on e-notarization.
2008	E-notarization Admin. Rules Creating SS. 12.9.2.1 through 12.9.2.15 of the New Mexico Admin. Code	Publishes rules for e-notarization based on NASS NES and MNA 2002; requires signers to physically appear before a notary for an e-notarization; sets

Year	Law or Standard	Summary
		registration requirements, including completion of a course on e-notarization offered through a qualified and certified provider, as specified; requires e-notaries to maintain their contact information with the SoS; clarifies that performing an e-notarization without registering is subject to sanctions as described in the NM Notary Handbook; sets rules for the form and manner of performing e-notarizations; sets maximum fees; and clarifies that the liability, sanctions, and remedies as described in the Handbook apply to e-notaries.
New York		
2011	S 2373A, Ch. 549	Provides that the signature requirement for any document that requires acknowledgment or notarization as a condition for recording is satisfied if: (1) the document contains a digitized "wet signature" of the notarizing official and a digitized stamp impression as required by law; or (2) the document contains an e-signature and all other required information, and clarifies that a physical or electronic image of a stamp, impression or seal is not required.
2012	Admin. Rules Implementing S 2373A, Adding Sec. 540.7 to Part 540 of Title 9 of the New York Codes, Rules and Regulations	Requires a notary's e-signature to conform to standards contained in MNA 2010 and NASS NES, and requires notaries to e-notarize only when the signer of the electronic real property document is in the notary's physical presence and can be identified.
North Carolina		
2000	S.B. 1266, Sess. Law 2000-152	Enacts UETA Sec. 11.
2005	S.B. 671, Sess. Law 2005-391	Enacts URPERA Sec. 3; and enacts Article 1A on e-notarization based upon the 2002 MNA, establishes registration rules, requires e-notaries to take a course and examination, authorizes official acts, outlines an e-notary's powers and limitations, sets maximum fees, provides rules for e-notary signatures and seals, permits e-notaries to keep an electronic journal, sets rules for the disposition of software used for e-notarizations upon

Year	Law or Standard	Summary
		resignation or revocation of an e-notary's commission, prescribes certificate forms for e-notarizations, authorizes the SoS to issue electronic apostilles and certifications, and provides sanctions for improper e-notarizations.
2007	Admin. Rules Adding SS. 07C.0101 to 07C.0800 to the North Carolina Admin. Code	Establishes procedures for registering as an e-notary, sets standards for e-notary signatures and seals, requires signers to be physically present before the e-notary for any e-notarization, provides for the approval of e-notary solution providers, and sets rules for employers of e-notaries.
2008	H.B. 545, Sess. Law 2008-194	Recognizes the legal effect of e-documents filed with the Mecklenburg County Register of Deeds if it was e-notarized by a Virginia notary and contains the notary's typed name and commission expiration date.
North Dakota		
2001	H.B. 1106, Ch. 108	Enacts UETA Sec. 11.
2011	H.B. 1136, Ch. 334	Enacts the RULONA provisions related to notarization of electronic records, and authorizes the SoS to adopt rules.
Ohio		
2000	H.B. 488	Enacts UETA Sec. 11.
Oklahoma		
2000	S.B. 1598, Ch. 372	Enacts UETA Sec. 11.
2008	H.B. 2587, Ch. 295	Enacts URPERA Sec. 3.
2007	S.B. 42, Ch. 49	Permits e-signatures and e-notarizations on documents filed with the Oklahoma Office of Admin. Hearings.
Oregon		
1999	H.B. 3041, Ch. 718	Authorizes a person to use, and a notarial officer to accept, an e-signature in the manner prescribed by rule, requires an electronically-signed notarial certificate to be attached electronically by the notarial officer in the manner prescribed by rule and contain the phrase "signed by electronic signature" or similar words, and requires the SoS to adopt rules.
2001	H.B. 2112, Ch. 535	Enacts UETA Sec. 11.
2013	H.B. 2834, Ch. 219	Enacts the RULONA provisions related

Year	Law or Standard	Summary
		to notarization of electronic records, repeals ORS 194.582 enacted by Ch. 718 of 1999 (*see above*), allows notaries to use an electronic journal that complies with rules adopted by the SoS, and authorizes the SoS to adopt rules.
2013	Admin. Rules Implementing the RULONA, Amending Ch. 160, Division 100 of the Oregon Admin. Code	Provides rules for registering a notary's intent to notarize electronic records, requires a notary to include a graphic image of the notary's handwritten signature in performing an e-notarization, requires a notary to logically associate the notary's official stamp with an electronic record, and prescribes the form and rules for electronic journals.
Pennsylvania		
1999	S.B. 555, Act No. 1999-69	Enacts UETA Sec. 11.
2002	H.B. 851, Act No. 2002-151	Requires notary commission applicants to take a course of instruction that includes e-notarization, requires a notary's e-signature to be attributable to the notary identified on the commission, permits counties to allow notaries to register their e-signatures, and provides that a notary is not required to use an electronic seal for an e-notarization if certain specified information is attached to or logically associated with the e-signature or record.
2005	Publication of Notice for Phase I of the E-notarization Initiative in 35 Pa.B. 7068	Allows notaries who have applied with the DoS, purchased an Electronic Notary Seal, and registered their e-signatures in Chester, Lancaster, Philadelphia, or Westmoreland counties to perform e-notarizations.
2010	Publication of Notice for E-notarization Program and Solution Provider Applications in 40 Pa.B. 2065	Announces the availability of and specifications for e-notarization solution provider applications, and requires approval of solution providers.
2012	H.B. 970, Act No. 2012-100	Enacts URPERA Sec. 3.
2013	H.B. 25, Act No. 2013-73	Enacts the RULONA provisions related to notarization of electronic records, and authorizes the SoC to adopt rules.
2014	H.B. 1429, Act No. 2014-95	Clarifies that a power of attorney executed (and notarized) in electronic form may be recorded in the same manner as any other document under URPERA.

Year	Law or Standard	Summary
Rhode Island		
1997	H.B. 6118A, Ch. 320	Allows e-notarizations for filing with state and/or public agencies.
2000	H.B. 7344A, Ch. 259	Enacts UETA Sec. 11.
South Carolina		
2004	H.B. 4720, Act No. 279	Enacts UETA Sec. 11.
2008	H.B. 3451, Act No. 210	Enacts URPERA Sec. 3.
South Dakota		
2000	S.B. 193, Ch. 225	Enacts UETA Sec. 11.
2014	S.B. 68, Ch. 47	Enacts URPERA Sec. 3.
Tennessee		
2001	S.B. 376, Ch. 72	Enacts UETA Sec. 11.
2007	S.B. 317, Ch. 420	Enacts URPERA Sec. 3 and prescribes a certificate for a copy certification of an electronic record.
Texas		
2001	S.B. 393, Ch. 702	Enacts UETA Sec. 11.
2005	S.B. 220, Ch. 103	Permits notaries to record notarial acts electronically in a computer or other storage device.
2005	S.B. 335, Ch. 699	Enacts URPERA Sec. 3.
2009	H.B. 2585, Ch. 461	Authorizes a declarant, witness or notary to sign an advance medical directive or a written revocation of a directive using a digital signature or e-signature meeting certain technical conditions, as specified.
2015	S.B. 1726, Ch. 859	Applies UETA Sec. 11 provision to proceedings filed under Title 5 of the Texas Family Code.
Utah		
1998	S.B. 107, Ch. 63	Provides that an acknowledgment taken by a notary is complete on an electronic document without a notary's seal if certain conditions, as specified, are met, including use of digital signatures by the signer and notary, and verification by the notary of the signer's digital signature against the public key listed in the digital certificate issued to the signer.
2000	S.B. 125, Ch. 74	Enacts UETA Sec. 11.
2000	S.B. 145, Ch. 312	Defines "acknowledgment" to include an admission made by electronic communication that is as reliable as one

Year	Law or Standard	Summary
		made in the presence of a notary, allows "satisfactory evidence of identity" to be based on electronic protocols as reliable as current methods of identification, authorizes notaries to authenticate an electronic or digital signature, provides that if all parties consent, an authenticated electronic or digital signature may be treated as a notarized signature on the record, provides that a notary acting under the supervision and control of a licensed CA that acknowledges and authenticates electronic or digital signatures is protected under the Utah Digital Signature Act, allows a notary to keep an e-journal if the notary performs e-notarizations, and requires all e-notarizations to be signed with a digital signature.
2001	Admin. Rule to Enable Electronic Communication Between a Signer and Notary Using a Digital Signature, Adding Sec. R154-10-502 to the Utah Admin. Code	Sets minimum technical specifications for using live electronic audio-video communication with a digital signature in compliance with U.C.A. Sec. 46-1-2(1) and 46-1-2(11)(c).
2006	S.B. 20, Ch. 21	Repeals the Utah Digital Signature Act of 1996 and the provisions enacted in S.B. 145, Ch. 312 (*see above*).
2008	H.B. 26, Ch. 47	Repeals the requirement that the notary include his or her business or residence address on an acknowledgment e-notarized without an image of the notary's official seal.
2008	File Number 30642 Repealing Sec. R154-10-502 of the Utah Admin. Code	Repeals the 2001 rules setting technical specifications for using live audio-video communication with a digital signature.
2014	S.B. 79, Ch. 89	Enacts URPERA Sec. 3.
Vermont		
2003	H.B. 148, Act No. 44	Enacts UETA Sec. 11.
Virginia		
2000	H.B. 499, Ch. 995	Enacts UETA Sec. 11.
2005	S.B. 992, Ch. 744	Enacts URPERA Sec. 3.
2006	S.B. 448, Ch. 745	Reenacts the URPERA.
2007	H.B. 2058, Ch. 269	Provides rules for commissioning as an e-notary; requires an e-notary to record all e-notarizations in a journal or other

Year	Law or Standard	Summary
		device and establishes rules for these records; prescribes rules and standards, as specified, for the use and security of e-signatures and seals; requires an e-notarization to be evidenced by a notarial certificate signed by and attributable to the e-notary; requires an e-notary to take reasonable steps to ensure the integrity, security, and authenticity of e-notarizations; permits an e-notary to add an electronic notarial certificate to a document at the direction of a principal or lawful authority; sets maximum fees; authorizes the SoC to authenticate an e-notary's e-signature and seal; and authorizes the Secretary to revoke the commission of an e-notary under certain conditions, as specified.
2008	H.B. 218, Ch. 117	Clarifies that the application and commissioning procedures for a notary commission apply to e-notary commissions; requires a notary to obtain a separate e-notary commission; removes the provision that states a failure to affix an e-seal shall not impact the legality or efficacy of a document, and requires an e-notary to keep the electronic journal of e-notarizations for at least 5 years from the transaction date.
2009	S.B. 833, Ch. 160	Authorizes the SoC to adopt standards for e-notarization with the assistance and counsel of the Virginia Information Technologies Agency; requires a notary's e-signature and seal to conform to the standards; requires an applicant registering for an e-notary commission to certify that he or she is in compliance with the e-notarization standards adopted by the Secretary; and clarifies that an e-notarization performed in compliance with UETA and that on its face appears to be properly notarized is presumed to have been properly notarized.
2011	H.B. 2205/S.B. 1247, Ch. 123/177	Authorizes the SoC to accept applications for recommissioning as a notary containing the e-signature of the notary.
2011	H.B. 2318/S.B. 827 Ch. 731/834	Permits an e-notary to perform an e-notarization using video and audio

Year	Law or Standard	Summary
		conference technology; clarifies that the prohibition against notarizing for a signer outside of the presence of the notary does not apply to such e-notarizations; specifies the methods of "satisfactory evidence of identity" an e-notary must use to identify a signer for an e-notarization using video and audio conference technology; provides rules, as specified, for the technology for e-notarizations using video and audio conference; requires an e-notary to keep a copy of the audio and video conference for 5 years; clarifies that any e-notarization performed by an e-notary shall be deemed to be performed within the Commonwealth and governed by Virginia law; stipulates that an e-notary shall exercise a high degree of care in ascertaining the identity of any person who is the subject of an e-notarization; allows a notary to perform a notarial act outside of the Commonwealth if the notarial act is performed in accordance with Virginia law; and amends certain requirements for registering for a commission to perform e-notarizations.
2011	H.B. 1670, Ch. 746	Prohibits a notary from performing a notarial act on a paper or electronic document if the notary is a signatory or is named in the document.
2012	S.B. 270, Ch. 566	Removes the requirement that an e-notary take an oath of office before the clerk of the circuit court.
2013	The Virginia E-notarization Assurance Standard	Provides rules for an e-notary's e-signature and seal based upon the NASS NES and standards for identifying signers appearing by video and audio technology; requires an e-notary to use a digital certificate in performing e-notarizations and requires the digital certificate to conform to X.509 digital certificate standards; establishes standards for the records of e-notarizations required to be kept by e-notaries; clarifies the requirements for the use of an antecedent in-person proofing process to identify a signer in an online e-

Year	Law or Standard	Summary
		notarization; requires an e-notarization to allow relying parties to verify certain information, as specified, about the e-notary's official e-signature and e-seal; defines "e-notarization system;" and provides rules for the use of such systems.
Washington		
1996	S.B. 6423, Ch. 250	Equates the use of a digital certificate to create a digital signature with the notarial act of acknowledgment regardless of whether certificate wording appears with the digital signature or the signer appeared before the CA when the digital signature was created.
2008	H.B. 2459, Ch. 57	Enacts URPERA Sec. 3.
2014	Admin. Rule Amending SS. 434-661-020 and 434-661-030 of the Washington Admin. Code	Adopts URPERA rules and clarifies that execution of an "e-notarization" does not require a special appointment by the Washington Department of Licensing, and requires that an e-notarization of a real property record be performed by a Washington notary or a person authorized by the laws of another jurisdiction outside the state of Washington.
West Virginia		
2001	S.B. 204, Ch. 120	Enacts UETA Sec. 11.
2014	H.B. 4012, Ch. 133	Enacts the RULONA provisions related to notarization of electronic records, and authorizes the SoS to adopt rules.
2014	Emergency Rules Implementing the E-notarization Provisions of the RULONA, Adding Series 153-45 to the West Virginia Code of State Rules	Establishes procedures for registering and maintaining status as an e-notary; authorizes e-notaries to perform certain notarial acts electronically but only if the signer meets certain requirements, as specified; sets rules for the electronic notarial certificate, signature, and seal of a notary based largely on MNA 2010 and NASS NES; allows notaries to keep a journal of e-notarizations and provides rules for journals; authorizes the SoS to authenticate an e-notarization; and provides rules for the SoS denying, suspending or terminating the registration of an e-notary.
2015	S.B. 199, Ch. 162	Finalizes the emergency rules for e-notarization adopted by the SoS in 2014.

Year	Law or Standard	Summary
Wisconsin		
1997	A.B. 811, Act No. 306	Defines "electronic signature."
2003	A.B. 755, Act No. 294	Enacts UETA Sec. 11, amends W.S. 137.01(4)(a) to provide that every official act of a notary shall be attested by the notary's written signature or e-signature as defined in UETA, repeals the prior definition of "electronic signature" (*see* A.B. 811, Act No. 306 *above*), and repeals the prior provision permitting an e-signature to replace a manual signature (*see* A.B. 811, Act No. 306 *above*).
2006	S.B. 616, Act No. 421	Enacts URPERA Sec. 3.
Wyoming		
2001	S.F. 0116, Ch. 58	Enacts UETA Sec. 11.
2016	H.B. 107, Ch. 38	Enacts URPERA Sec. 3.

Since 1957

NATIONAL NOTARY ASSOCIATION
9350 De Soto Ave., P.O. Box 2402
Chatsworth, CA 91313-2402
818-739-4000
www.nationalnotary.org
eMail: nna@nationalnotary.org