Standards for Electronic and Remote Notarizations and Requirements for Remote/Electronic Notarization Platform Approval

A. Standards for notaries conducting electronic or remote notarizations

(1) Electronic or remote notarizations must occur with the use of an electronic or remote notarization system, which has two-way live audio and video conference technology that has been approved by the Michigan Department of State. No other vendor may be used.

(2) Prior to conducting an electronic or remote notarization, the notary public shall determine that the individual appearing before the notary public is the individual whose signature appears on the record through one of the following:
   (a) The notary public has personal knowledge of the individual;
   (b) The individual is identified by a sworn oath or affirmation of a credible witness personally known by the notary public and the individual signing;
   (c) The individual has been identified by their current license, personal identification card, or other government-issued identification document containing both a picture and signature.

(3) For remote notarizations, in addition to being verified through one of the methods outlined in section 2, the individual appearing before the notary must also be verified through a credential analysis process that is contained within the notarization platform. The credential analysis must utilize public or private data sources to confirm the validity of an identification credential and must, at a minimum:
   (a) Use automated software processes to aid the online notary public in verifying the identity of a remotely located individual;
   (b) Ensure that the identification credential passes an authenticity test, consistent with sound commercial practices that:
      (i) Use appropriate technologies to confirm the integrity of visual, physical, or cryptographic security features;
      (ii) Use appropriate technologies to confirm that the identification credential is not fraudulent or inappropriately modified;

(iii) Use information held or published by the issuing source or an authoritative source, as available, to confirm the validity of identification credential details; and
(iv) Provide output of the authenticity test to the online notary public;

(c) Enable the online notary public to visually compare for consistency:
(i) The information and photograph on the presented credential, and
(ii) The remotely located individual as viewed by the online notary public in real time through communication technology;

(d) Require a government-issued identification credential that:
(i) Is an unexpired government-issued identification credential that contains the photograph and signature of the individual; and
(ii) May be imaged, photographed, and video recorded under applicable state and federal law; and
(iii) Can be subjected to credential analysis.

(e) Include an image capture procedure that confirms that:
(i) The remotely located individual is in possession of the credential at the time of the notarial act;
(ii) Credential images submitted for credential analysis have not been manipulated; and
(iii) Credential images match the credential in the possession of the remotely located individual; and

(f) Require the captured image of the identification credential to:
(i) Be of sufficient image resolution to perform credential analysis in accordance with the requirements of this subsection;
(ii) Be of sufficient image resolution to enable visual inspection of the credential by the notary public; and
(iii) Include all images necessary to perform visual inspection and credential analysis in accordance with the requirements of this subsection, including the identity page of any passport and the front and back images of any identification card.

(4) A notary public is required to maintain a journal for all notarial acts performed using a remote notary platform.

(a) The journal must be maintained as a physical copy or in a permanent, tamper-evidence electronic version for at least 10 years after the performance of the last notarial act contained in it.

(b) The journal must contain at least all of the following:
(i) The date, time, and type of each notarial act performed

(ii) A description of the record, if any
(iii) The full name and address of the individual for whom the notarial act is performed
(iv) How the notary identified the individual (personal knowledge, etc.)
(v) The fee charged, if any
(vi) The platform by which the notarial act was maintained
(vii) Whether an audio or visual recording exists.

(c) The notary public may designate a custodian to maintain the journal or the audio or visual recording.

(5) A notary public may refuse to conduct a notarial act using a remote electronic notarization platform if the signer objects to an audio or visual recording of the notarial act. If a recording is made, the notary must do all of the following:
(a) Disclose that an audio or visual recording is being made
(b) Explain how the recording will be preserved
(c) Obtain the signer's consent to the recording.

(6) The notary public must refuse to perform an online notarization if:
(a) The notary public is unable to verify the identity of the signer;
(b) The notary public is unable to verify the security of the two-way audio-visual transmission; or
(c) The signature of the principal cannot be attached to the electronic document.

B. Requirements for remote/electronic notarization platform approval by the Department of State

(1) The online notarization system used must meet the following criteria:
(a) The persons communicating must simultaneously see and speak to one another;
(b) The signal transmission must be live, real time;
(c) The signal transmission must be secure from interception or access by anyone other than the persons communicating;
(d) The technology must provide sufficient audio clarity and video resolution to enable the notary to communicate with the signer and utilize the permissible signer identification methods;
(e) The system must provide confirmation that the electronic document presented is the same as the electronic document notarized;

(f) Allow for the affixation of the notarial certificate, signature and seal;
(g) Allow for viewing the notarial certificate, signature and seal;
(h) Provide a method of generating a paper copy of the document including the notarial certificate, signature and seal and any other document associated with the execution of the notarial act;
(i) Maintain an audio or visual recording of the notarial act for 10 years after the performance of the notarial act; and
(j) Make all records available to the Department upon request for investigation or authentication purposes.

(2) Vendors must establish identity proofing by means of knowledge-based authentication or biometric verification as described below.
(a) A knowledge-based authentication must meet the following requirements:
(i) Each remotely located individual must answer a quiz consisting of a minimum of five questions related to the remotely located individual's personal history or identity, formulated from public or private data sources;
(ii) Each question must have a minimum of five possible answer choices;
(iii) At least 80% of the questions must be answered correctly;
(iv) All questions must be answered within two minutes;
(v) If the remotely located individual fails the first attempt, the individual may retake the quiz two times within 48 hours;
(vi) During a retake of the quiz, a minimum of 40% of the prior questions must be replaced;
(vii) If the remotely located individual fails the second attempt, the individual is not permitted to retry with the same notary or the same third person providing the identity proofing service within 24 hours of the second failed attempt; and
(viii) The online notary public must not be able to see or record the questions or answers.
(b) A biometric verification must meet the following requirements:
(i) The system must allow a remotely located individual to provide a live biometric sample which is then automatically compared against a biometric feature on a government-issued identification credential provided by the remotely located individual;

(ii) The comparison process must conform to applicable National Institute of Standards and Technology (NIST) standards, or their equivalent, for accuracy;
(iii) The biometric system must attempt to verify the validity of the government-issued identification document as part of the biometric verification process;
(iv) The biometric system must not allow more than five consecutive failed authentication attempts. After three failed attempts, the biometric system must impose a delay of at least one minute before the next attempt, increasing by one minute with each unsuccessful attempt up to five attempts;
(v) After five failed attempts, the biometric system must be disabled as a user authentication, and the system must offer another method of identity verification.

(3) The system must provide an audit trail and be able to determine whether the document has been altered after the electronic notarial seal has been affixed to the record.
(a) Vendors must provide a method for determining if the electronic document has been altered after the electronic notarial seal has been affixed and the electronic notarial act has been completed.
(b) The audit log must contain a detailed list of actions taken related to the document explaining the user, date, time, and action taken.
(c) The document must be tamper-evidence after notarization so that any subsequent alterations to the document itself, or electronic notarization are either prevented altogether or detectable.

(4) The system must be able to place a notarial bloc on each document.
(a) The signature of a public notary must appear electronically in the same manner and format as it appears on file with the Department. The signature must either be a digital replica of the signature on the notary application or an exact image of the signature.
(b) The following statement must appear in the seal of the notary public: This notarial act was performed using electronic or remote technology by" immediately followed by the name of the vendor.
(c) The seal must be unique to the notary public and capable of independent verification by the Department.
(d) The notary bloc must appear exactly as identified in MCL 55.287.

(5) Vendors must go through an application process with the Department to be approved.

(a) To become approved, vendors must do all of the following:
    (i) Submit an application to the Department that demonstrates compliance with the Department's standards and the Act's requirements;
    (ii) Provide a demonstration to the Department upon request;
    (iii) Make any changes to come into compliance with the Department's standards or the Act's requirement; and
    (iv) Enable the notary public to comply with the standards outlined above.
(b) Vendors must notify the Department through the Office of the Great Seal when a notary public has been onboarded within five business days. Vendors shall not allow a notarial act to be performed prior to an updated application being approved by the Department of State.
(c) If a notary public's commission has been suspended or revoked by the Department, the Department must notify the vendor of the suspension, and the vendor must immediately suspend or revoke the notary public's access to their system.

(6) The vendor's system must ensure the security and privacy of all personally identifiable information and other data collected during the credential analysis and identity proofing processes. At a minimum, the system must:
(a) Ensure that all sensitive data, including images of identification credentials and biometric data, is securely stored, protected from unauthorized access, and encrypted in transit and at rest;
(b) Limit the use of this data strictly to the purposes of verifying an individual's identity and for maintaining the security and integrity of transaction records. Such data must not be used, sold, or transferred for any other commercial purpose;
(c) Prevent the notary public from having access to, or the ability to retain, raw biometric data or copies of the identification credential after the session, outside of the live viewing of the credential during the notarial act as necessary for identity verification;
(d) Establish and make available to the Department a data retention policy specifying default deletion timeframes;
(e) Conform to and follow applicable security standards, such as NIST, Federal Risk and Authorization Management Program (FedRAMP), or their equivalent; and
(f) Comply with Michigan data breach statutes.