The International Electronic Notarization Assurance Standard

Draft for Discussion at the
4th International Forum
on eNotarization, eApostilles
and Digital Evidence
New Orleans, Louisiana, USA

Comment Period May 30 – June 30, 2008

International Forum

Presented by the National Notary Association

The international representatives at this Forum will discuss and consider the International Electronic Notarization Assurance Standard that has been proposed by Notary societies from around the world. The International Forum provides for a gathering of international Notaries and identification experts to discuss, debate and exchange important ideas and standards proposed by all interested countries.

Table of Contents

Scope and Intent

The challenges before Notary Societies around the world are to preserve and strengthen the national role of the Notary in the rapidly emerging digital economy and to ensure the international cross-border recognition of notarized electronic documents in a global economy. Consequently, Notaries throughout the world must quickly transition to performing electronic notarizations that have the same legal effect and admissibility as currently presumed by their physical-world counterparts.

To achieve these objectives an international assurance Standard for Electronic Notary Certificates, Electronic Notarial Acts, and Notarized Electronic Documents is needed that will accord to the resulting notarized electronic documents the same reliability and presumption of admissibility enjoyed by paper documents notarized with physical seals and handwritten ink signatures. This international Standard establishes a minimum level of assurance for issuing and managing Electronic Notary Certificates, executing Electronic Notarial Acts with Electronic Notary Certificates, and verifying the authenticity of Notarized Electronic Documents.

Accordingly, Notarized Electronic Documents signed with an Advanced Electronic Notary Signature which is based on a Qualified Electronic Notary Certificate and which is created by a Secure Electronic Notary Signature Creation Device:

(a) satisfies the legal requirements of a Electronic Notarial Act in relation to an electronic Original Document in the same manner as a physical Notary seal satisfies those requirements in relation to a paper document; and

(b) is admissible as evidence in legal proceedings.

This standard meets or exceeds the requirements of the following authoritative electronic signature sources:

(a) The UN Model Law[1]

(b) The EU Electronic Signature Directive[2]

(c) The U.S. e-Sign Act[3]

This standard is composed of four Articles. Article 1 defines the roles and responsibility of the Notary Society Issuing Authority; Article 2 presents a standard for Qualified Electronic Notary Certificates; Article 3 presents a standard for performing Notarial Electronic Acts; and Article 4 presents a standard for verifying the authenticity of Notarized Electronic Documents.

[1] UNCITRAL Model Law on Electronic Signatures

[2] European Union Electronic Signature Directive

[3] United States Electronic Signatures in Global and National Commerce Act

Definitions

(a) **Advanced Electronic Notary Signature** means an electronic signature that is uniquely linked to the Notary; capable of identifying the Notary; created using means that the Notary can maintain under the Notary's sole control; and linked to the Original Electronic Document to which it relates in such a manner that any subsequent change of the Original Electronic Document is detectable.

(b) **Digital Certificate** means a computer-based record or electronic file that identifies the Notary Society Issuing Authority issuing such record or file; names or identifies a certificate holder; contains the Identity Key of the certificate holder; identifies the certificate's validity period; is digitally signed by a Certification Authority; and states the intention of its holder to be bound by the terms of the document digitally signed with the certificate's Signing Key in accordance with applicable standards. A certificate includes not only its actual content but also all documents expressly referenced or incorporated within it.

(c) **Electronic Notarial Act** and **Electronic Notarization** mean an official act by an Electronic Notary that involves Electronic Original Documents.

(d) **Electronic Notary** means a Notary with the capability of performing Electronic Notarial Acts in conformance with this Standard.

(e) **Electronic Original Document** means any electronic record or file that can be signed with a Secure Electronic Notary Signature Creation Device.

(f) **Identity Key** means the public key, also referred to as signature verification data contained in the Qualified Electronic Notary Certificate.

(g) **Notarial Act** means an official act that a Notary Public is authorized to perform.

(h) **Notarized Electronic Document** means the Electronic Original Document that has been signed with an Advanced Electronic Notary Signature.

(i) **Notary Applicant** means the Notary Public applying for a Qualified Electronic Notary Certificate.

(j) **Notary Certification of Facts** means the part of an Electronic Notarized Document that is completed by the Notary, bears the Notary's Advanced Electronic Notary Signature, and states the facts attested by the Notary in a particular Electronic Notarization.

(k) **Notary Public** and **Notary** mean any person commissioned to perform Notarial Acts.

(l) **Notary Society Issuing Authority** (NSIA) means a legal entity representing a national association of Notaries responsible for maintaining the Notary Society Issuing Authority Policy governing the operations and compliance of the Qualified Certification Service Provider, Qualified Registration Authority, Verifier, and the Electronic Notary.

(m)**Notary Society Issuing Authority Policy** (NSIAP) means the policy document governing the operations and responsibilities of the Notary Society Issuing Authority involved in the issuance and life cycle management of Qualified Electronic Notary Certificates and Secure Electronic Notary Signature Creation Devices.

(n) **Notary Subscriber Agreement** means the agreement between the Notary and the Notary Society Issuing Authority governing the terms and conditions of use for the Qualified Electronic Notary Certificate.

(o) **Online Certificate Status Protocol** (OCSP) means the real-time method used to receive and respond to a request for the validity status of a Qualified Electronic Notary Certificate.

(p) **Public Key Infrastructure** means a set of policies, processes, personnel, server platforms, software, and workstations used for the purpose of administering Electronic Notary Certificates and key pairs, including the ability to issue, maintain, validate, and revoke Electronic Notary Certificates.

(q) **Qualified Electronic Notary Certificate** (QENC) means a Digital Certificate issued by a Notary Society Issuing Authority that conforms to the requirements of this Standard.

(r) **Qualified Certification Service Provider** (QCSP) means a Certificate Authority issuing Qualified Electronic Notary Certificates according to the Notary Society Issuing Authority Policy and this Standard.

(s) **Qualified Identification and Authentication** (QI&A) means the process of establishing and authenticating the real identity of a Notary Applicant and the authenticity of the Notary Applicant's commission for the issuance of a Qualified Electronic Notary Certificate.

(t) **Qualified Registration Authority** (QRA) means an entity that is responsible for ensuring the proper identification and authentication of Notary Applicants, and receiving and distributing the Qualified Electronic Notary Certificates. The QRA receives the requests from the Verifier and securely communicates the requests to the QCSP in a way that can be verified for authenticity.

(u) **Secure Electronic Notary Signature Creation Device** means configured

software or hardware mechanisms used to create the Advanced Electronic Notary Signature.

(v) **Signing Key** means a private cryptographic key, also referred to as signature creation data, cryptographically bound to the Qualified Electronic Notary Certificate.

(w) **Standard** means The International Electronic Notarial Act Assurance Standard.

(x) **Verifier** means the person authorized by the Notary Society Issuing Authority to perform the QI&A of Notary Applicants, entering the Notary Applicant information and verifying its completeness and correctness, and securely communicating the requests to the QRA in a way that can be verified for authenticity. While the Verifier performs similar functions to the QRA, the Verifier is authorized to serve a limited population of Notary Applicants based on geographical proximity.

Article 1: Notary Society Issuing Authority

The Notary Society Issuing Authority:

(a) shall employ personnel who possess the expert knowledge, experience, and qualifications necessary for the services provided, in particular competence at managerial level, expertise in electronic signature technology, and familiarity with proper security procedures; they shall also apply administrative and management procedures which are adequate and correspond to recognized standards;

(b) shall use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them;

(c) shall use trustworthy systems to store Qualified Electronic Notary Certificates in a verifiable form so that:

(i) only authorized persons can make entries and changes,

(ii) information can be checked for authenticity,

(iii) Qualified Electronic Notary Certificates are publicly available for retrieval only in those cases in which the Notary's consent has been obtained, and

(iv) any technical changes compromising these security requirements are apparent to the operator.

(d) shall take measures to prevent forgery of Qualified Electronic Notary Certificates, and in cases where the Notary Society Issuing Authority generates Signing Keys, guarantee confidentiality during the process of generating such data;

(e) shall not store or copy the Signing Key of the Notary to whom the Notary Society Issuing Authority provided key management services;

(f) shall maintain sufficient financial resources to operate in conformity with the requirements laid down in the Notary Society Issuing Authority Certificate Policy, in particular to bear the risk of liability for damages, for example, by obtaining appropriate insurance;

(g) shall inform the Notary in writing and in common understandable language before entering into a contractual relationship with a Notary seeking an Electronic Notary Certificate of the precise terms and conditions regarding the use of the Electronic Notary Certificate, including any limitations on its use, the existence of a voluntary accreditation scheme, and procedures for complaints and dispute settlement. Such information shall be transmitted by a durable means of communication and may be transmitted electronically. Relevant parts of this information shall also be made available on request to third-parties

relying on the Electronic Notary Certificate;

(h) shall ensure that the commission of the Notary is verified and is authentic prior to the issuance of the Qualified Electronic Notary Certificate;

(i) shall be responsible for designating Verifiers to perform the QI&A of Notary Applicants as authorized agents of the QRA. Verifiers shall be required to enter into an agreement that defines their obligation to perform and attest to the fulfillment of QI&A obligations;

(j) shall not be responsible for verifying the status of the Notary's commission at the time an Electronic Notarial Act is performed as it is the responsibility of the Notary to notify the Notary Society Issuing Authority of the Notary's commission suspension, revocation, or expiration;

(k) may subcontract functions to other entities only if the NSIA remains responsible for the performance of these subcontracted services in compliance with the NSIAP, and such entities agree to be bound by the Notary Society Issuing Authority Policy. Subcontracted functions include:

(i) the Qualified Electronic Notary Certificate manufacturing process,

(ii) publication of Qualified Electronic Notary Certificates,

(iii) revocation of Qualified Electronic Notary Certificates, and

(iv) ensuring that all aspects of the NSIA services, operations and infrastructure related to Qualified Electronic Notary Certificates issued under the NSIAP are performed in accordance with the requirements, representations, and warranties of such NSIAP, including notification of Qualified Electronic Notary Certificate issuance and revocation.

Article 2: Qualified Electronic Notary Certificates

2.1 Qualified Electronic Notary Certificate Ownership

(a) A Qualified Electronic Notary Certificate:
  (i) is the private property of the Notary;
  (ii) is governed by the Notary Subscriber Agreement as defined by the Notary Society Issuing Authority Policy; and
  (iii) may incorporate an electronic image of the Notary's official physical seal that may appear on any visual or printed representation.

(b) An Electronic Notary may own two Qualified Electronic Notary Certificates at one time provided the following requirements are met:
  (i) the Signing Key of one Qualified Electronic Notary Certificate is protected on a software-based Secure Electronic Notary Signature Creation Device and the Signing Key of the second Qualified Electronic Notary Certificate is protected on a hardware-based Secure Electronic Notary Signature Creation Device;
  (ii) each Signing Key is linked to a unique Qualified Electronic Notary Certificate that identifies the same Notary and commission identifier; and
  (iii) each Qualified Electronic Notary Certificate meets the same assurance requirements as defined by this Standard.

2.2 Qualified Certification Service Providers

A Qualified Certification Service Provider who issues Qualified Electronic Notary Certificates shall:

(a) demonstrate the reliability necessary for issuing Qualified Electronic Notary Certificates in conformance with this Article;

(b) ensure that the system clock used for Qualified Electronic Notary Certificate issuance and life cycle management operations is sourced from a legally mandated National Timing Authority in an auditable and trusted manner and that the timestamps of Qualified Electronic Notary Certificate issuance, validity status verification (OCSP or other Qualified Certification Service Provider responses), and revocation are resistant to falsification and manipulation, and are verifiable on demand by any independent party.

(c) be audited by an independent and qualified external third party to demonstrate compliance with all governing regulatory and Notary Society Issuing Authority Policy requirements; and

(d) retain records designed to be archived as evidence and that are time stamped at the time they are created or received by the Qualified Certification Service Provider, Qualified Registration Authority, or Verifier.

2.3 Qualified Electronic Notary Certificate Issuance

2.3.1 Notary Identity and Commission Verification

(a) The Notary Society Issuing Authority shall verify, by appropriate means in accordance with national law, the identity and commission of the Notary to whom a Qualified Electronic Notary Certificate is issued.

(b) The Notary Society Issuing Authority shall record and retain all relevant information concerning Qualified Electronic Notary Certificates for at least ten (10) years after the Qualified Electronic Notary Certificate expires or is revoked in order to provide evidence of certification for the purposes of legal proceedings. The recording and retention of information required by this subsection may be performed by electronic means.

(c) The Verifier shall be an authorized individual designated and certified by the Notary Society Issuing Authority who has contractually agreed to abide by the governing Notary Society Issuing Authority Policy.

(d) The Verifier shall identify and authenticate the true identity of the Notary Applicant through presentation of one form of national government-issued picture identification or two forms of non-national government identification, one of which shall contain a picture.

(e) The Verifier shall ensure that the any national government-issued picture ID presented by a Notary Applicant:

(i) appears to be a genuine document properly issued by the claimed issuing authority and valid at the time of application; and

(ii) bears a photographic image of the holder that matches that of the Notary Applicant;

(f) The Verifier shall ensure that any non-national government-issued picture ID presented meets the requirements of subparagraphs (i) and (ii) of subsection (e) of this section and states an address at which the Notary Applicant can be contacted.

(g) The Verifier shall establish the Notary Applicant's identity no earlier than thirty (30) days before issuance of the initial Qualified Electronic Notary Certificate.

(h) The Verifier shall confirm the status and authenticity of the Notary Applicant's current commission as a Notary Public through presentation of the Notary's current original [name of commissioning document] or a certified copy of the same, and the information shall be verified to ensure legitimacy.

(i) The following information shall be obtained and electronically notarized by the Verifier and transmitted to the Qualified Registration Authority in a secure and verifiably authentic manner:

(i) satisfactory evidence of the Notary Applicant's identity, including the name of the credentials verified, the corresponding credential identifiers, and notarized copies;

(ii) the Notary Applicant's Notary commission information and a notarized copy of the commission;

(iii) a declaration of truthful assertions sworn to or affirmed by the Notary Applicant and subscribed using a handwritten signature in the presence of the Verifier, which may be obtained by electronic means; and

(iv) the name of the Verifier, the Verifier's unique identifying number, the date and time of the QI&A transaction, and the Verifier's handwritten signature, which may be obtained by electronic means.

2.3.2 Identity and Signing Key Pair Generation

(a) Cryptographic keying material for Signing Keys shall be generated according to the appropriate security assurance standard for cryptographic modules, such as ISO/IEC 19790: 2006[4] or U.S. NIST FIPS 140-2 Level 3 for Qualified Certification Service Providers, and Level 2 for the Qualified Registration Authorities and Electronic Notaries.

(b) Identity and Signing Key sizes and signing algorithms shall be as defined by a Qualified Certification Service Provider medium level assurance standard.

2.3.3 Secure Electronic Notary Signature Creation Devices

(a) A Secure Electronic Notary Signature Creation Device shall, by appropriate technical and procedural means, ensure at the least that the Signing Key used for Advanced Electronic Notary Signature generation:

(i) can practically occur only once, and that its secrecy is reasonably assured;

(ii) cannot, with reasonable assurance, be derived; and

(iii) can be reliably protected by the Electronic Notary against the use of others.

(b) In most cases, Signing Keys shall be generated and remain within the cryptographic boundary of the Secure Electronic Notary Signature Creation Device. If the key is generated elsewhere, then the Secure Electronic Notary Signature Creation Device shall be delivered to the Notary by the Notary Society Issuing Authority. The Notary Society Issuing Authority shall maintain accountability for the location and state of the Secure Electronic Notary Signature Creation Device until the Notary accepts possession of it. The Notary shall acknowledge receipt of the Secure Electronic Notary Signature Creation Device. The Signing Key shall be protected from activation, compromise, or modification during the delivery process. Under no circumstances shall anyone other than the Notary have substantive knowledge of or control over the Signing Key after generation of the key.

[4] International Standards Organization/International Electrotechnical Commission: ISO/IEC 19790:2006 *Security requirements for cryptographic modules* issued on 1 March 2006.

(c) When keyed hardware tokens are delivered to Notaries, the delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct Notaries.

(d) The Qualified Certification Service Provider shall maintain a record of validation for receipt of the token by the Notary.

2.3.4 Notary Signing Key Protection

(a) A Secure Electronic Notary Signature Creation Device shall, by appropriate technical and procedural means, ensure at the least that the Signing Key used for Notary Electronic Signature generation can be reliably protected by the legitimate Notary against the use of others.

(b) The Qualified Certification Service Provider shall specify to the Notary that the Signing Key must be held in the strictest confidence and protected in accordance with the terms of the Notary Subscriber Agreement.

(c) The Signing Key of a medium assurance software-based Secure Electronic Notary Signature Creation Device may be backed up as long as it remains under the Notary's control and meets all the protection and usage requirements for the Notary's Signing Key.

(d) The Signing Key of a medium assurance hardware-based Secure Electronic Notary Signature Creation Device shall not be backed up.

2.3.5 Qualified Electronic Notary Certificate Attributes

A Qualified Electronic Notary Certificate shall contain:

(a) an indication that the certificate is issued as a Qualified Electronic Notary Certificate;

(b) the identification of the Notary Society Issuing Authority and the jurisdiction in which it is established;

(c) the name of the Notary Applicant;

(d) the Identity Key which corresponds to the Signing Key that is under the sole control of the Notary;

(e) an indication of the beginning and end of the Qualified Electronic Notary Certificate period of validity;

(f) the Advanced Electronic Signature of the Notary Society Issuing Authority issuing the Qualified Electronic Notary Certificate; and

(g) limitations on the scope of use of the Qualified Electronic Notary Certificate to execution of Electronic Notarial Acts and access to systems to perform Electronic Notarial Acts.

2.3.6 Secure Electronic Notary Signature Creation Device Acceptance and Custody

(a) The Notary Society Issuing Authority shall specify in the Notary Subscriber Agreement:
  (i) the terms and conditions for use of the Electronic Notary Certificate;
  (ii) the obligation to protect the Signing Key and maintain control over the Secure Electronic Notary Signature Creation Device; and
  (iii) the procedure which constitutes acceptance and agreement by a Notary. The process of notification, acceptance, and issuance, and the mechanisms used, may depend on factors such as the software- or hardware-based form of the Secure Electronic Notary Signature Creation Device and how it is made available to the Notary.

(b) By accepting an Qualified Electronic Notary Certificate, the Notary:
  (i) warrants that all information provided by the Notary and included in the Qualified Electronic Notary Certificate, and all representations made by the Notary as part of the application and QI&A process, are true; and
  (ii) formally agrees to the terms and conditions of the Notary Subscriber Agreement as a pre-condition to the Notary's use of the Qualified Electronic Notary Certificate.

(c) The Notary shall be required to sign the Notary Subscriber Agreement containing the requirements the Notary must follow to use the Qualified Electronic Notary Certificate.

(d) Failure by a Notary to object to the issuance of an Electronic Notary Certificate or its contents shall constitute acceptance of the Notary Subscriber Agreement.

(e) A mechanism shall be used to authenticate the correct Notary to that Notary's assigned Secure Electronic Notary Signature Creation Device before the activation of any Signing Key. Acceptable means of authentication include, but are not limited to, confidential passphrases and PINs or biometrics.

(f) A hardware-based Secure Electronic Notary Signature Creation Device shall be delivered to a Notary in a manner that ensures that the correct Secure Electronic Notary Signature Creation Device and corresponding activation data are provided securely to that Notary;

(g) A software-based Secure Electronic Notary Signature Creation Device shall be activated to ensure that the Secure Electronic Notary Signature Creation Device is accessible and that the corresponding activation data is provided to the correct Notary.

(h) The Signing Key shall be generated and remain within the cryptographic boundary of the Secure Electronic Notary Signature Creation Device cryptographic module.

(i) If the Signing Key is generated outside of the cryptographic boundary of the cryptographic module, the Electronic Notary Signature Creation Device shall be delivered to an authenticated Notary in a secure and auditable manner. The Signing Key shall be protected from activation, compromise, or modification during the delivery process.

(j) Under no circumstances shall anyone other than the Notary have substantive knowledge

of or control over the Signing Key or generate a copy of the Signing Key.

(k) The Notary shall acknowledge receipt of the Secure Electronic Notary Signature Creation Device. The Notary Society Issuing Authority shall maintain a record of receipt of the Secure Electronic Notary Signature Creation Device by the Notary.

(l) A Secure Electronic Notary Signature Creation Device shall not be left unattended or otherwise available to unauthorized access. At the end of the validity period of a Qualified Electronic Notary Certificate, the Secure Electronic Notary Signature Creation Device shall be deactivated.

2.4 Qualified Electronic Notary Certificate Life Cycle Management

2.4.1. Qualified Electronic Notary Certificate Validity

(a) A Qualified Certification Service Provider shall ensure the operation of a real-time, reliable, and secure:

(i) Qualified Electronic Notary Certificate directory, which shall contain a published list of all OCSP responders;

(ii) OCSP responder(s) for responding to validity status requests in accordance with RFC 2560; and

(iii) revocation service to revoke Qualified Electronic Notary Certificates that have become invalid or have been compromised according to section 2.4.3.

(b) A Qualified Electronic Notary Certificate shall have a maximum validity period of three (3) years.

2.4.2 Qualified Electronic Notary Certificate Renewal and Re-Keying

(a) Renewal consists of issuing a new Qualified Electronic Notary Certificate with a new validity period and serial number while retaining all other information in the original Qualified Electronic Notary Certificate, including the Identity Key.

(i) A Qualified Electronic Notary Certificate may be renewed if the Identity Key has not reached the end of its validity period, the associated Signing Key has not been compromised, and the Notary name and attributes are unchanged. In addition, the validity period of the certificate shall not exceed the remaining lifetime of the Signing Key.

(ii) The Electronic Notary and Verifier may request a renewal and the Qualified Registration Authority shall approve renewal.

(iii) Qualified Electronic Notary Certificate renewal may be performed using the initial or a new QI&A.

(b) Re-keying consists of creating a new Qualified Electronic Notary Certificate with a different Identity Key and serial number while retaining the other Notary information from the old certificate. The new certificate may be assigned a different validity period and/or signed using a different QCSP Signing Key.

2.4.3 Qualified Electronic Notary Certificate Revocation

(a) A Qualified Certification Service Provider shall:

(i) provide a secure and immediate revocation service that includes a secure directory of all revoked Qualified Electronic Notary Certificates in real time; and

(ii) ensure that the date and time when a Qualified Electronic Notary Certificate is revoked can be determined precisely and verified for authenticity.

(b) A Qualified Electronic Notary Certificate shall be immediately revoked when the binding between the Electronic Notary and the Notary's Identity Key is no longer considered valid, including, but not limited to, the following circumstances:

(i) the identifying information or affiliation components of any names in the Qualified Electronic Notary Certificate become invalid;
(ii) the Electronic Notary can be shown to have violated the terms of the Notary Subscriber Agreement;
(iii) the Signing Key contained in the Secure Electronic Notary Signature Creation Device is compromised or is suspected of compromise;
(iv) the Notary Society Issuing Authority determines revocation is in its best interest: and
(v) The Electronic Notary asks for the Qualified Electronic Notary Certificate to be revoked.

(c) Whenever any of the circumstances (i) through (v) of subsection (b) occur, the associated Qualified Electronic Notary Certificate shall be revoked and placed on a certificate revocation list and/or specified as revoked by an OCSP responder.

Article 3: Electronic Notarial Act

3.1 Original Document Rendering

The process for affixing an Advanced Electronic Notary Signature shall ensure that the Electronic Original Document digitally signed was completely and unalterably rendered to the Electronic Notary at the time the Electronic Notarial Act was performed.

3.2 Qualified Electronic Notary Certificate Status Validation

Prior to creating an Advanced Electronic Notary Signature the validity status of the Qualified Electronic Notary Certificate shall be verified to determine whether the Qualified Electronic Notary Certificate has been revoked.

3.3 Electronic Notary's Certification of Facts

The signing formalities and recordation of facts of an Electronic Notarial Act in an Electronic Notary's Certification of Facts shall conform to applicable law in the jurisdiction in which the Notary is commissioned.

3.4 Electronic Notary Signature Creation

(a) The Secure Electronic Notary Signature Creation Device used to create an Advanced Electronic Notary Signature shall not alter the data to be signed or prevent such data from being completely and unalterably rendered to the Electronic Notary prior to the signature being created.

(b) The Advanced Electronic Notary Signature shall provide the capability of demonstrating that the electronic document that was notarized is accurate, authentic, complete, and can detect tampering or alteration.

(c) An electronic image of the Notary's official physical seal may be incorporated into or associated with the Advanced Electronic Notary Signature and may appear on any visual or printed representation of the signature.

Article 4: Notarized Electronic Document

4.1 Qualified Electronic Notary Certificate Reliability

The Qualified Electronic Notary Certificate is reliable if it:

(a) is unique to the Electronic Notary;
(b) is capable of independent verification;
(c) is retained under the Electronic Notary's sole control;
(d) is attached to or logically associated with the electronic document; and
(e) is linked to the data in such a manner that any subsequent alterations to the underlying document are detectable.

4.2 Advanced Electronic Notary Signature Reliability

The verification of an Advanced Electronic Notary Signature shall ensure with reasonable certainty that:

(a) the data used for verifying the Advanced Electronic Notary Signature corresponds to the data displayed to the verifying party;
(b) the Advanced Electronic Notary Signature is reliably verified and the result of that verification is correctly displayed;
(c) the party verifying the Advanced Electronic Notary Signature may, as necessary, reliably establish the contents of the Notarized Electronic Document;
(d) the authenticity and validity of the Electronic Notary Certificate required at the time of the Advanced Electronic Notary Signature verification may be reliably verified;
(e) the result of the verification and the Notary's identity and commission are correctly displayed;
(f) any security-related changes can be detected.

4.3 Reliability of Notarial Certification of Facts

When performing an Electronic Notarial Act, an Electronic Notary shall complete a Notary Certification of Facts which shall be attached to or logically associated with the Electronic Original Document in such a manner that removal or alteration of the Certification of Facts is detectable.

4.4 Original Document Reliability

The Advanced Electronic Notary Signature shall enable a relying party to demonstrate that the Notarized Electronic Document:

(a) accurately reflects the true contents of the Original Electronic Document as it was presented and rendered in final form at the time the Electronic Notarial Act was performed;
(b) is accessible at any time in the future and can be rendered in human readable form accurately and completely; and
(c) can be verified for authenticity independently at any time.

