The National eNotary Registry

Ensuring Trustworthy and Reliable Electronic Documents Through Secure eNotarization

August 8, 2007

Published as a public service by the
NATIONAL NOTARY ASSOCIATION

Table of Contents

I. Introduction

A. Public Trust

For centuries, the Notary Public has imparted trust to documentary transactions by attesting to the execution of instruments with a particular sign in the form of a physical and tangible seal of office. The presence of a seal clearly identifies the Notary as a governmentally appointed official witness and, most importantly, provides *prima facie* proof of the underlying document’s authenticity and its lawful execution by a particular willing and aware person.

In a world where documents are now created by directing streams of electrons to register as 0’s or 1’s in a coherent pattern of computer bits and bytes, the Notary’s traditional, tangible seal must be transformed if it is to serve in the electronic realm its evidentiary purpose of conferring authenticity and credibility on documents.

What, then, is the electronic counterpart to the Notary’s paper-compatible inking or embossing seal?

It is the Electronic Notary Seal, a trustworthy and cost-effective credential-based method for electronically verifying a Notary’s identity and official status, thereby lending the same trust to notarized electronic documents as exists in the paper world. In addition, this electronic authentication credential may simultaneously serve as the Notary’s electronic signature.

For the electronically capable Notary, the Electronic Notary Seal functions as an identity credential, as a signature, and proof of official status.

B. Concept for a National eNotary Registry

This paper describes the functions, specifications, processes, and benefits of a National eNotary Registry, the centerpiece of an electronic credential management system for Notaries Public that issues, administers and validates Electronic Notary Seals.

The Registry is premised on three fundamental concepts:

- A Notary Public must use an electronic authentication credential when performing an electronic notarization. (See Section II, “The Need for Electronic Notary Authentication Credentials,” pages 4–6.)

- A Notary’s electronic authentication credential must be trustworthy. (See Section III, “Trustworthy Electronic Authentication Credentials,” pages 7–9.)

- For electronically notarized documents to be reliable, interested third parties must quickly and independently be able to verify the status of the Notary and validate the Notary’s electronic credential. (See Section IV, “The National eNotary Registry,” pages 10–14.)

II. The Need for Electronic Notary Authentication Credentials

A. The Requirement for an Official Seal

What public need justifies the use of credentials by Notaries and the maintenance of a National eNotary Registry to enroll, manage and validate those credentials?

The answer can be found by analyzing the challenges present in both the current paper-based notarial system and the emerging electronic environment.

In authenticating a notarial act today in the United States, Notaries in virtually every state, territory and the District of Columbia must possess and use an official physical seal[1] — the Notary's credential in the paper world. Courts take judicial notice of the Notary's seal[2] because notarized documents serve as *prima facie* proof of the document's authenticity and lawful execution.

In order to protect the physical seal credential from acts of fraud, states have enacted laws to securely issue and associate a seal with a particular Notary.[3] Yet, despite these rules, seals can be obtained with relative ease by an unauthorized person — even, in one case, by placing the highest bid in an online auction on eBay.[4] Furthermore, with the help of feature-rich photo editing software, any savvy amateur can manipulate an image of a Notary seal, making the resulting graphic presentation virtually indistinguishable from a hand-stamped seal impression.

Many government officials, technologists, attorneys and even Notaries themselves have long been concerned that these abuses must be addressed in the electronic realm before the day when Notaries begin to perform eNotarizations.[5]

That day has arrived.

The 1999 Uniform Electronic Transactions Act (UETA) that has been adopted in virtually every state and the 2000 federal Electronic Signatures in Global and National Commerce Act ("E-SIGN") recognize electronic transactions, signatures and notarizations.

Implementations of electronic signatures compliant with the UETA and E-SIGN laws can be designed simply to accept a Notary's typed name as a signature or to incorporate a "Sign Here" button[6] that the Notary clicks. Clearly, much more security is needed.

If a third party had reason to investigate a transaction years later and needed to verify and prove that a particular Notary signed the document, it would be extremely difficult to track a typed-name or click-wrap signature back to the Notary. The Notary's signature could have been executed or adopted by the actual Notary or by *any* person in cyberspace — hiding behind a shroud of anonymity — who typed a few words taken from the imprint of a Notary's physical seal as gleaned from a paper document. Alarmingly, persons relying on the document would be none the wiser.

For electronically notarized documents to be truly dependable, the Notary's electronic credential — the secure replacement for the fraud-vulnerable physical seal — must be securely attached to or associated with the Notary's electronic signature. Only then can all who rely on an electronically notarized document, especially those whose legal rights or financial assets are on the line, have confidence that the document bears a trustworthy electronic credential identifying the person purporting to act as a Notary Public and hasn't been altered.

B. Wedding Robust Technology with a Trusted Witness

Relying on developments that are time-tested and have been proven in online commercial models for years, a robust technology has emerged that binds an individual to an electronic signature and to the electronic document: digital certificates in a Public Key Infrastructure (PKI).

A digital certificate is issued by a trusted third party[7] after identifying the individual in person. The digital certificate contains a "private" and "public" key pair. The credential holder uses the private key to "sign" documents, the so-called "digital signature." Any member of the public may then use the attached corresponding "public" key that is cryptographically bound with the signer's identity to verify the signature made with the private key.

When adopted by a Notary Public, the digital signature performs exactly the same function as a tangible Notary seal; it is the Notary's *electronic* credential.

Early PKI vendors confidently claimed that digital signatures would replace the Notary's human witnessing ministrations and several states followed suit by enacting laws that equated the affixing of a digital signature without a Notary present to that of a Notary personally taking the acknowledgment of a signer.[8]

This confidence was unfounded. For good reason Utah recently repealed such an ill-conceived statute, which stipulated that "a certificate issued by a licensed certificate authority is an acknowledgment of a digital signature."[9]

The only way to know for sure that a person signed a document — paper or electronic — is to have a trusted impartial witness, such as a Notary, present. By contrast, a person who uses a public key to verify a digital signature can only establish that a person's private key was used to create the signature. It cannot conclusively prove that the rightful owner of the private key actually used it.

A digital signature can never replace the socially interactive confirmation that is the true basis of trust. It can never replace the witnessing of a handwritten or electronic signature made voluntarily and knowingly in the physical presence of a Notary by a principal for the considerations and purposes expressed in the document.

The good news is that we can do much better than to rely on potentially exploitable physical seals and on digital certificates whose aim is to replace the Notary. Electronic commerce can be enhanced by wedding the time-tested official witnessing function of a Notary together with a trustworthy process for issuing secure electronic credentials to Notaries.

The National eNotary Registry does just that. It provides for the first time a nationally accredited system for the management of standards-based Electronic Notary Seals that are issued in a secure and reliable manner, capable of validation instantaneously over the Internet, usable with any electronic document that exists currently (or that might be created by technologies yet to be developed) and offered cost-effectively.

III. Trustworthy Electronic Authentication Credentials

A. Accreditation and Liability Framework

A Notary's electronic credential must be trustworthy. To establish this trust, the Electronic Notary Seal and National eNotary Registry have been vetted through a universally respected third party — the Secure Identity Services Accreditation Corporation (SISAC)[10] — in order to meet the stringent standards for digital certificate issuance and management in the mortgage finance industry.

The SISAC vision is to provide the many disparate service providers[11] in a mortgage finance transaction with a common SISAC-accredited digital certificate issued by approved "Accredited Issuing Authorities" (AIA) and by an approved "Registration Authority" (RA)[12], so that the service providers can reliably know with whom they are dealing. The RA is a person or entity acting as an agent of a "Certification Authority," the manufacturer of the credential, and verifying the identity and authority of the Notaries to whom the digital certificate credential is issued.

At the heart of SISAC compliance are its governing documents which bind the parties, assign liability and present the requirements for accreditation.

Accreditation includes submission of an application containing information on the applying organization and its digital certificate issuance practices. Of particular significance are three requirements: an organizational audit, proof of sufficient financial resources, and maintenance of records. These requirements are briefly summarized below.

Investigation and Audit. The AIA and RA must undergo a third-party audit by a qualified auditor at their own expense to demonstrate compliance with the SISAC Certificate Policy Requirements Document[13] within the six-month period prior to the date of application for accreditation. An additional annual audit is required to maintain accreditation.

Financial Responsibility and Liability. An AIA and RA must have adequate financial resources to perform their duties, and errors and omissions insurance to remedy the risk to subscribers and relying parties who use their certificates.

SISAC accreditation is distinguished from other PKI systems in the assignment of liability. An AIA and RA are liable for claims presented by parties relying on a certificate when a misidentification results due to a failure to follow the identification and authentication procedures specified in the approved Certificate Policy of the AIA. Liability will not result when fraudulent ID documents were presented during a digital certificate application.[14]

Records of Compliance. AIAs and RAs must maintain all records of application and compliance with the SISAC Certificate Policy Requirements Document for a period of at least 7.5 years following the end of the operational validity of any certificate issued. These records must be safeguarded in a trustworthy manner and made available to SISAC upon request in any investigation or dispute resolution.

B. Credential Specifications

The credential specifications of the Electronic Notary Seal and National eNotary Registry are designed to engender trust in the electronic credential and in the means for validating that credential.

The Electronic Notary Seal is an ANSI X.509 Version 3 digital certificate that contains attributes which uniquely identify the Notary but are part of an electronic credential common in every state. For the first time ever, a Notary's credential holds out the promise of being unique, but common, in all 50 U.S. states, thus reducing, and in many cases, simply eliminating the frequent rejections of properly notarized paper documents that travel across state borders.

The Electronic Notary Seal is installed over a secure Internet connection to the FIPS-compliant Windows Certificate Store on a personal computer and can be stored on a USB-enabled storage device (a smart card[15] for example) or accessed for signing from a server to enable a Notary to perform an electronic notarization using a Web browser.[16] In the SISAC model, the Electronic Notary Seal can be issued as either a BASIC- or MEDIUM-level[17] digital certificate. The Electronic Notary Seal will conform to the following specifications:

Risk Assessment: Risk and consequences of data compromise or access to private information with the likelihood of malicious intent range from minimal for BASIC-level certificates to moderate for MEDIUM-level certificates.

Identity Proofing: An individual must be identified in person with one federal or one state government-issued photo ID.

Revocation Processing: The issuing authority must issue and publish the revocation of a certificate to a publicly accessible Certificate Revocation List (CRL) within at least 24 hours of notification for a BASIC-level certificate and at least 12 hours for a MEDIUM-level certificate.

Financial Liability: AIAs assume liability for ensuring that applicable identification and authentication procedures are stringently followed and must carry errors and omissions insurance in the annual amount of at least $1 and $5 million for BASIC-level and MEDIUM-level certificates, respectively.

The Electronic Notary Seal is valid for one year except in Arizona, where state law allows a maximum validity period of two years.[18] Upon certificate expiration, a new Electronic Notary Seal must be obtained subject to the identification and authentication procedures required for first-time applicants.

IV. The National eNotary Registry

A. The Registry's Three Functions

The National eNotary Registry is a database of all Notaries Public in the United States who have been issued an electronic authentication credential in the form of the Electronic Notary Seal. There are three primary functions of the Registry:

Enrollment. Notaries are qualified to receive an electronic credential through a Registration Authority — a person or entity[19] acting as an agent of a Certification Authority, the manufacturer of the credential — which is accredited to verify the identity and authority of the Notary.

Management. The Registration Authority enrolls and manages the electronic credential in the Registry throughout the credential's life cycle, including processing any premature terminations,[20] and ensures that the Registry reflects the current status of all electronic credentials registered in the system.

Validation. Any interested person, if not the party(ies) directly relying on an electronic document notarized with an Electronic Notary Seal, may consult the Registry to verify that a Notary Public possessed a valid credential at the time the document was notarized.

B. Real-Time Validation

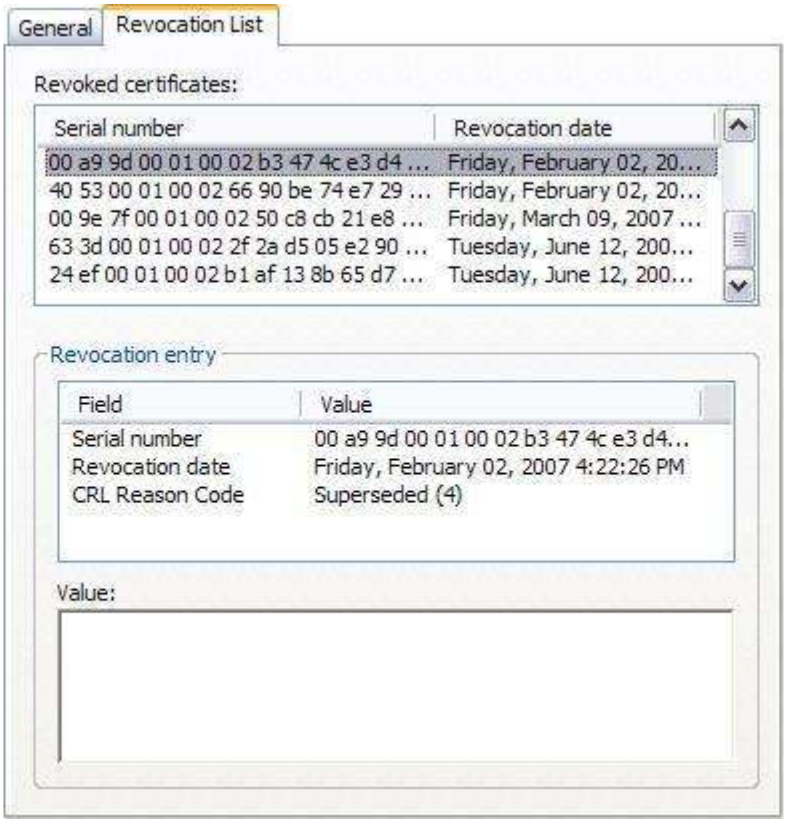
The National eNotary Registry offers any person the advantage of instantaneously validating the electronic credential of a Notary Public to prevent impostors or former Notaries from improperly using credentials undetected. Historical validation services provide relying parties the capability of proving the notarial act in the event of a dispute at some future date.

The Registry is a marked improvement over procedures for validating the Notary's commission. This process typically involves mailing or delivering the actual signed and notarized document to the state Notary regulating official. Upon certifying the legitimacy of the Notary, the official will attach a certificate of authority or *apostille*[21] as proof and forward the document to the receiving party. The process can take weeks to complete.

By contrast, there are multiple ways that the electronic credential of the Notary can be quickly and reliably validated. Each is briefly discussed below.

Certificate Revocation List. Consulting the AIA's certificate revocation list (CRL) is the most basic way to check the status of an Electronic Notary Seal. The CRL will contain the serial numbers of all revoked digital certificates issued by the AIA, the date of revocation and a CRL Reason Code. This list is updated at least every 12 hours for MEDIUM-level SISAC-accredited certificates and 24 hours for BASIC-level certificates.

The CRL can be downloaded and viewed within the Internet Explorer Web browser by typing the Uniform Resource Locator (URL) of the CRL obtained from the digital certificate into the location bar. Once the download commences, the CRL can be viewed by clicking the "Open" button.



Revoked certificates:

Serial number	Revocation date
00 a9 9d 00 01 00 02 b3 47 4c e3 d4 ...	Friday, February 02, 20...
40 53 00 01 00 02 66 90 be 74 e7 29 ...	Friday, February 02, 20...
00 9e 7f 00 01 00 02 50 c8 cb 21 e8 ...	Friday, March 09, 2007 ...
63 3d 00 01 00 02 2f 2a d5 05 e2 90 ...	Tuesday, June 12, 200...
24 ef 00 01 00 02 b1 af 13 8b 65 d7 ...	Tuesday, June 12, 200...

Revocation entry

Field	Value
Serial number	00 a9 9d 00 01 00 02 b3 47 4c e3 d4...
Revocation date	Friday, February 02, 2007 4:22:26 PM
CRL Reason Code	Superseded (4)

Value:

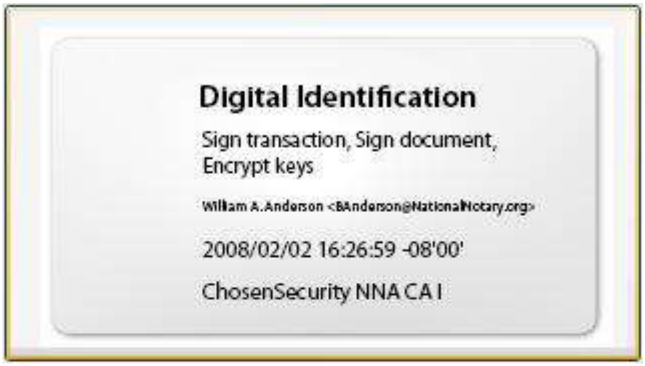
Figure 1. Certificate Revocation List Viewed in Internet Explorer.

The user then must compare the serial number of the revoked certificate from the CRL to the certificate used to sign the document under review.

The disadvantages of using the CRL are that it does not contain any information about the holder of the revoked certificate and is difficult to use. Fortunately, software provides more intuitive methods for checking certificate revocation information and the CRL can be programmatically checked to perform this function automatically.

View Certificate Manually. A second way to determine certificate status is to manually view the certificate in document signing and viewing software. For illustrative purposes, the procedure for viewing a certificate in Adobe Acrobat or Reader Version 8 will be described.

Adobe Acrobat or Reader allows a transacting or relying party to view the certificate of any signing party before or after the signature has been affixed. Clicking on an unsigned signature field embedded within a PDF document in Acrobat or Reader will invoke the Sign Document dialog box. Once the certificate to be used for signing is selected from the drop-down list, a thumbnail of the certificate containing the name of the holder, the holder's email address, the certificate revocation date, the name of the AIA and RA, and the uses of the certificate appears and can be reviewed prior to signing.



Digital Identification

Sign transaction, Sign document,
Encrypt keys

William A.Anderson <BAnderson@NationalNotary.org>

2008/02/02 16:26:59 -08'00'

ChosenSecurity NNA CA I

Figure 2. Certificate Thumbnail Using Adobe Acrobat or Reader.

Clicking on the thumbnail will open the Certificate Viewer, revealing fuller details about the certificate.

In signed PDF documents, clicking on the electronic signature itself will open the Certificate Viewer for convenient viewing of all certificate information for the underlying certificate used to create the signature.

Automatic Checking of the CRL. An even more intuitive way to view the revocation status of an Electronic Notary Seal is to rely on the automatic signature validation feature of document signing and viewing software. Once again, the process utilized in Adobe Acrobat and Reader will be described.

A user must enable the automatic revocation and signature validation features in the system settings within Acrobat or Reader and have a computer connected to the Internet for the validation to succeed. Adobe recommends that users enable this feature.[22]

Once automatic signature validation is set, upon opening a document signed with an Electronic Notary Seal, Acrobat and Reader will obtain the most current information on the certificate from the Certificate Revocation List. One of several icons will appear in the display of the digital signature on the document to depict the status of the certificate, including a green check mark to indicate a valid certificate and a red "X" to indicate an invalid certificate.[23] No manual steps for checking a certificate are required.

Online Validation. A final way to validate an Electronic Notary Seal is through www.ensvalidate.org, a secure Web site hosted by the National Notary Association. When the Notary's last name, the Notary's commission number and state of commissioning are entered into the online form, the Web service application will inform the user if a match of that Notary is found in the system. No additional information about the Notary is provided. This convenient method for checking certificate status is especially useful when a relying party cannot check the Certificate Revocation List directly, does not have access to the electronically notarized document or software programs such as Adobe Acrobat or Reader, and the Notary's name, commission number and state of commissioning are known.

C. Ensuring Document Integrity

Through the National eNotary Registry a Notary's electronic credential can be validated quickly and easily by any relying party. By notarizing an electronic document with this credential, a second ancillary benefit is obtained: any changes made to the document after the Electronic Notary Seal is affixed or attached to the document are immediately detectable.

In technical terms, at the point of signing, the Notary's software applies a mathematical algorithm to the document to produce an original message digest. The same message digest can be replicated by anyone who runs the unchanged document through the same algorithm. The software then encrypts the digest with the private key of the Notary's Electronic Notary Seal to produce a second, signed message digest.

The person proving the content integrity or authenticity of the document applies the same processes, except that the Notary's public key is used instead. The person then compares the original message digest with the digest produced using the Electronic Notary Seal. Comparison of the original message digest to the signed digest reveals either the exact same digests as produced by the Notary or evidence of changes to the original document. Two different digests can mean either that the signature is valid and the document has authorized changes or the signature is invalid because the changes were not authorized.

Encryption is an arms race. Any attempt to encrypt data is theoretically subject to mathematical compromise.[24] Even if it is proven at a later date that the encryption offered by today's digital certificates is no longer considered reliable, the Registry itself will not be compromised. By checking the Registry on a future date, any relying party can be as certain that a Notary possessed a valid credential as on the day it was first issued, because the Registry manages the Notaries who use a credential, not the technology behind the credential itself.

D. Summary of Salient Points

The National eNotary Registry is a tool for the secure issuance, management and validation of Electronic Notary Seals. The following points summarize the salient technological features of the Registry:

Web Accessible. The Registry services are accessible in any standards-compliant Web browser and do not require third parties checking a Registry credential to provide any additional end user software.

Accepted Technology. Digital certificates with a public key infrastructure are used in commercial online activities every day — e.g., to verify a bank's Web site, purchase goods and services online, or secure the transmission of sensitive data to an online vendor. PKI is time-tested and universally adopted.

Interoperability. By conforming to the published ANSI X.509 Version 3 specification for digital certificates, the Registry's credentials are immediately supported in Microsoft® Office, Adobe® Acrobat® and Reader®, and in any alternative electronic document model developed to this common specification.[25]

Control and Oversight. By acquiring SISAC accreditation for its electronic credentials, the Registry must undergo an annual audit to demonstrate SISAC compliance.

V. Conclusion

The legal efficacy of and powerful presumption of authenticity accorded by the courts to a notarized document stands or falls on whether it can be corroborated that 1) a duly commissioned Notary performed the notarial act and 2) the associated instrument has not been altered or forged.

Today, technology has reaffirmed and underscored the importance of the Notary's human witnessing role, while at the same time offering a more reliable solution for identifying the Notary and evidencing changes made to electronic documents.

The Electronic Notary Seal and National eNotary Registry form such a trustworthy and reliable solution. The system is nationally accredited for use in the mortgage finance industry and compliant with established industry standards. Electronic Notary Seals are issued only to Notaries who hold a current Notary commission and whose identities have been carefully verified in person.

Consequently, by utilizing the time-honored and judicially tested official witnessing acts of a Notary Public and along with the National eNotary Registry's capacity to securely issue and validate Electronic Notary Seals, the public can have full confidence that electronic transactions will be not just as secure, but significantly more secure than paper transactions.

VI. End Notes

[1] Notaries in 42 states and the District of Columbia must possess and use an official physical seal. In the remainder of the states, except for one (Vermont), Notaries need only use a private seal without a prescribed image or form in completing the notarial act.

[2] *Pierce v. Indseth*, 106 U.S. 546 (U.S. 1882).

[3] For example, California and Oregon allow only licensed vendors to manufacture Notary seals. Other states require the Notary to present the official commission to procure a seal and forward a sample of the seal image to the commissioning office once it is issued. In order to ensure that the seal is not used by an unauthorized person, 25 states require (and six recommend) the Notary to notify the commissioning official or law enforcement if the seal is lost or stolen, to properly dispose of the seal at the end of a commission term, or expressly prohibit the seal to be unlawfully possessed or used by anyone other than the Notary to whom it belongs.

[4] On June 27, 2007, an eBay seller auctioned the embosser seal of a Texas Notary obtained at a garage sale.

[5] For an excellent discussion of these concerns, see *Electronic Notarization: Why It's Needed, How It Works, And How It Can Be Implemented To Enable Greater Transactional Security*, by Daniel J. Greenwood, Esq., Director of the E-Commerce Architecture Program at the Massachusetts Institute of Technology. Published by the National Notary Association, this white paper is available on the NNA's Web site at www.nationalnotary.org by clicking on News & Resources/ Library/NNA Position Papers. According to Greenwood: "The reason for paying careful attention to the technology, practices and standards used for eNotarization is that, without care, digital information is subject to the same kinds of fraudulent and exploitive attacks clever criminals launch against paper documents. For that matter, wholly new forms of assault are possible that are unique to digital systems."

[6] The so-called "click-wrap" or "click-through" signature is commonly used in software end user license agreements and in Web applications requiring a signature.

[7] The trusted third party is called a Certification Authority (CA).

[8] See the white paper *Digital Signature Laws and Notarization*, available from the National Notary Association at www.nationalnotary.org.

[9] UCA 46-3-405, which contained this provision, was repealed in 2006 along with the entire Utah Digital Signature Act. The section fully reads: "Unless otherwise provided by law or contract, a certificate issued by a licensed certification authority is an acknowledgment of a digital signature verified by reference to the public key listed in the certificate, regardless of whether words of an express acknowledgment appear with the digital signature or whether the signer physically appeared before the certification authority when the digital signature was created, if that digital signature is: (1) verifiable by that certificate; and (2) affixed when that certificate was valid."

[10] SISAC was created by the Mortgage Bankers Association in consultation with Government Sponsored Entities (GSE) Fannie Mae and Freddie Mac and lenders and technology companies to be the official accrediting organization of identity credentials and identity-issuing authorities for service providers in the mortgage finance industry.

[11] The mortgage finance industry presents an identity management challenge for electronic transactions. The players — originating lenders, mortgage brokers, title insurers, flood and hazard insurers, credit companies, appraisers, tax certifiers, escrow agents, secondary investors, Notaries, etc. — are often unaffiliated and unknown to each other.

[12] The National Notary Association is the Registration Authority (RA) for the National eNotary Registry.

[13] The Certificate Policy Requirements Document contains the minimum baseline requirements for accreditation as a SISAC Accredited Issuing Agency or Certificate Management Services Provider and facilitates interoperability among those parties whose services meet the requirements.

[14] See *SISAC Relying Parties: Guidance and Best Practices for Implementing Use of SISAC Secure Identity Credentials*, available at www.sisac.org.

[15] A smart card is a credit card-size electronic storage device with a computer microchip that can store the private key of a digital certificate.

[16] Referred to as a "roaming ID." The private key of the digital ID is installed on the server and is accessible from any computer that has an Internet connection.

[17] SISAC certificates are issued according to a three-tier security assurance model: BASIC, MEDIUM and HIGH.

[18] See ARS 41-353(C).

[19] See note 12.

[20] Certificates may be revoked for a variety of reasons: e.g., if the private key is compromised, if the Notary Public's commission expires, or if an employee leaves a company in which the certificate had been used to access a private network, etc.

[21] The *apostille* is an authenticating certificate prescribed for use among nations that are party to the 1961 Hague Convention Abolishing the Requirement of Legalization for Foreign Public Documents.

[22] See *Digital Signature User Guide*, published by Adobe Systems, Inc., page 87, available at www.adobe.com.

[23] See Id. at page 86 for a table of applicable icons representing certificate status.

[24] The Electronic Notary Seal uses RSA 1024-bit encryption, meaning that the public key associated with the digital certificate is 1024 bits in length. By today's standards, 1024-bit keys are considered of sufficient length to fend off a "brute force attack"—a trial-and-error method of breaking cryptographic keys by systematically trying every conceivable mathematical solution.

[25] One such model is the cross platform SMARTDOC® format for electronic mortgage documents published by the Mortgage Industry Standards Maintenance Organization.