ARTICLE:

THE PROPOSED INTERNATIONAL E-IDENTITY ASSURANCE STANDARD FOR ELECTRONIC NOTARIZATION

By **Timothy S. Reiniger**

Introduction

Of the many important developments that occurred at the 4th International Forum on eNotarization, eApostilles and Digital Evidence in New Orleans, Louisiana,[1] the progress toward a uniform, global standard for trustworthy and reliable electronic notarizations is the most noteworthy. At the Forum, notary representatives and attendees from 25 countries and six continents discussed the Standard.[2] After receiving further public comments, a working group consisting of Forum attendees and notary experts will issue a revised version before the end of the year.

Need for international e-identity assurance standard for notaries

The challenge facing the global move toward e-notarization is establishing a uniform and trustworthy approach for issuing and managing notaries' electronic identity credentials and signatures. The Standard — initially proposed by the National Notary Association of the United States (NNA) — establishes minimum criteria for issuing, managing, and validating notaries' electronic credentials. The purpose of the Standard is to ensure that electronically notarized documents, based on the use of one federated credential by the notary, will be legally acceptable anywhere in the world.

Without a uniform e-identity assurance standard that is aligned to the various national signature laws and emerging industry access control and secure messaging requirements, notaries everywhere face the need to own multiple electronic credentials. For example, the bio-pharmaceutical industry[3] and the aerospace and defense industry,[4] already require the use of different digital certificates to participate in secure network communications. At the same time, every relying party should know that the electronic credential and signature of the notary in one country is as legally valid and reliable as the electronic credential and signature of a notary in any other country.

Elements of proposed Standard

The Standard would aim to establish a trustworthy universal assurance level for binding the identity of a notary to an electronic credential. This is crucially important when taking into account that the integrity of the content of the electronic document and the signatures rests on the capability of identifying the actual signer or sender of the document in a trustworthy manner.[5] Accurate e-identity, in turn, rests on robust procedures to obtain relevant and accurate identifying information during the credential registration and issuance process.[6]

To best secure international approval and implementation, the contents of the Standard have been based expressly on the European Union's electronic signature directive,[7] the Liberty Identity

[1] *The 4th International Forum on e-Notarization, e-Apostilles, and Digital Evidence took place May 29 and 30, 2008 and was hosted by the NNA in conjunction with its annual United States notary conference. Forum presentations and other program details are available at http://www.nationalnotary.org/forum.*

[2] *French and Spanish language versions of the Standard are available at http://www.nationalnotary.org/forum.*

[3] *See the digital certificate requirements of SAFE-Biopharma Association, available at http://www.safe-biopharm.org.*

[4] *See the digital certificate requirements of CertiPath, Inc., available at http://www.certipath.com and the Transglobal Secure Collaboration Program, http://www.tscp.org.*

[5] *Ed Chase, ' Eunomic Solutions in a Commonly Used Application' in George L. Paul, Foundations of Digital Evidence, (American Bar Association, 2008), Appendix A at 162.*

[6] *Patrick McKenna, ' The Probative value of digital certificates: Information Assurance is critical to e-Identity Assurance,' Digital Evidence and Electronic Signature Law Review (previously the e-Signature Law Journal), 1 (2004) 55 - 60.*

[7] *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, OJ L 13, 19.01.2000, p.12. Versions in the other languages of the European Community Member States are available at http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&numdoc=31999L0093&model=guichett&lg=en.*

The UINL has further specified that Notaries should obtain an electronic signature with a high level of security, accredited by a recognized certificate, using a safe signature creation device.

Assurance Framework of the Liberty Alliance Project,[8] and the official policies of the International Union of Latin Notaries (UINL).[9] These sources reflect previously adopted cross-border efforts that touch on the matter of e-identity assurance.

Notary society as issuing authority

Consistent with the policy of the UINL that the notary society or organization in each country must issue the digital certificates,[10] the notaries societies of the European Union member nations and in other continents have already begun establishing procedures for what notaries must do to obtain the digital certificates that permit e-notarizations to occur. These notaries societies are also creating procedures to determine how those credentials will be managed, renewed, and revoked.

In the United States, a comparable effort has been launched by the NNA through the Electronic Notary Signature (ENS) program. The federal ESIGN law and state electronic signature laws prohibit states and local notary commissioning officials from enacting laws and rulemaking that would proscribe specific authentication or electronic signature technologies.[11] However, the states are permitted to set technology neutral performance standards to assure record integrity.[12] The result is that both the government and the private sector need the NNA to perform the electronic credentialing issuance and management role in the United States.

Digital certificate required

In view of the fact the signature laws in common law countries emphasize function over form in contrast to the civil law tradition of emphasizing form over function,[13] it is necessary to consider why the proposed Standard is entirely based on the use of one electronic signature technology – the digital signature contained in the digital certificate.

The proposed Standard's emphasis on the digital certificate reflects the Conclusions of the XXIV UINL Congress: ‘Whereas digital signatures are a technical tool which can serve the notarial function, we request that member notariats be equipped with the necessary means for encouraging the introduction of the new technologies, the training of notaries and the use of digital signatures.’[14] The UINL has further specified that ‘Notaries should obtain an electronic signature with a high level of security, accredited by a recognized certificate, using a safe signature creation device. To do so, it will be advisable to proceed to generate the signature verification and creation data, by the certification authority, and its delivery to the notary under the control of the competent notarial authority.’ Indeed, the Standard mirrors the practices currently used by Notary Societies in many nations, including Italy, Germany, Argentina, Spain, Estonia, Brazil, Mexico, and Austria. Notaries Societies in the United Kingdom, Australia, and Turkey plan to implement similar electronic notarial practices next year.

The use by notaries of the digital certificate has three purposes, two of which go beyond the signature function: access, authentication, and adoption. First, a digital certificate can be used as, in effect, a key to allow authorized individuals to electronically obtain *access* to secure networks such as public registries. Second, a digital certificate *authenticates* the origin of a message so that the recipient can infer the identity of

[8] *http://www.projectliberty.org.*

[9] *Collected at http://www.nationalnotary.org/forum.*

[10] *See ‘ Certification Policy for the Notarial Electronic Signature of Member States of the International Union of Latin Notaries (U.I.N.L)’ from the 2004 Congress held in Mexico City and available at http://www.nationalnotary.org/forum. The notarial electronic signature ‘ should be protected by a certificate issued under the control and responsibility of the notarial authority in each member state of the U.I.N.L.’*

[11] *Electronic Signatures in Global and National Commerce Act (E-Sign) 15 USC §§ 7002(a)(2)(A) and 7004 (b)(2)(C). For a fuller discussion of the technology neutrality aspects of United States' federal and state electronic signature laws, see Stephen Mason Electronic Signatures in Law (Tottel, 2nd edn, 2007) §§ 8.2 and 8.3 and Jane K. Winn and Benjamin Wright, Law of Electronic Commerce, (Aspen Law & Business, 4th edition, 2000) § 5.04[A].*

[12] *E-Sign 15 USC § 7004 (b)(3)(A). United States performance standards for e-notarization are contained in NATIONAL E-NOTARIZATION STANDARDS (Nat' l Ass' n of Secretaries of State 2006) available at http://www.nationalnotary.org/commission.*

[13] *See Stephen Mason, Electronic Signatures in Practice, 6 J. High Tech L. 149, at 152 (2006) and Electronic Signatures in Law (Tottel, 2nd edn, 2007) Chapter 9 for a discussion of authentication of electronic documents generally in common law countries.*

[14] *XXIV International Congress of Latin Notaries, Conclusions of the Working Group for Theme II ‘ The Notary and electronic contracts’ (2004), available at http://www.uinl.org.*

the sender. This is associated with, for example, the secure filing of deeds with public land registry systems. Third, a digital certificate provides a means for a signer to *adopt* the contents of a document with the intent to render a legal signature — the function that would be used for electronic notarizations.

Because of the additional security measures associated with digital certificates and certificate management policies, such as unique number identifiers, hashing capabilities, and public revocation lists, relying parties anywhere in the world can have a much higher degree of confidence that the signature on an electronic notarial certificate belongs to the notary and not an imposter. Also, the digital certificate adds a layer of protection against forgery for the content of the document by means of encryption.

Notary responsible for use and control of the digital signature

To preserve a trustworthy authentication function for the digital certificate, the Standard follows the strict UINL policies that make the notary responsible for the use, protection, and control of the digital signature. Specifically, notaries must use a secure electronic signature creation device.[15] Notaries risk recall or suspension of their certificates upon disclosure of the confidential password that controls use of the digital signature.[16] No one other than the named notary may use the digital signature.[17]

Capability of verifying notary digital signatures

Third parties relying on electronic notarizations must be able to independently verify that the notary's electronic credential, in the form of a digital certificate, is actually being or has been used only by the individual to whom the notary commission was issued by the appropriate jurisdiction.[18] This verification capability should also be quick and simple and permit real-time authentication of the notary's digital signature.[19] The Council of the Notaries of the European Union (CNUE) has already developed and piloted an internet platform that will allow relying parties to verify the digital signatures of European notaries.[20] Similarly, United States' notarial digital signatures may be verified by means of the National eNotary Registry.[21]

The UINL also has taken the position that the notaries societies of each country must give relying parties the ability to verify the notary's digital signature: 'Whereas for the free international circulation of electronic notarial deeds there must be a general method for verifying the signature and the capacity of the presiding notary, we request that the certification of the notary's digital signature remain under the control of the member notariats, whilst observing the principals and methods which are developed for such verification on a global level.'[22]

Conclusion

Ultimately the world's notary organizations — such as UINL, the NNA, and others — will need to lead the effort to develop and implement an e-identity assurance standard for notaries. This is the only way to achieve the aim of ensuring that notaries will require only one federated identity and one electronic credential. Without this, it is likely that notaries will be faced with having to purchase multiple credentials to perform a variety of even the most basic tasks. The world's notary societies, working with the main private industry and governmental users, are in the best position to create such a uniform, global standard that will give eNotarization the necessary degree of security, trust, and reliability.

The Executive Director of the National Notary Association, Timothy S. Reiniger is a licensed attorney in New Hampshire and California, previously practicing law in Manchester, NH serving three terms on the Board of Mayor and Aldermen. He graduated from Georgetown University School of Foreign Service and the University of Michigan Law School.

http://www.nationalnotary.org/

[15] 'Certification Policy for the Notarial Electronic Signature of Member States of the International Union of Latin Notaries (U.I.N.L),' policy number 2, from the 2004 Congress held in Mexico City and available at http://www.nationalnotary.org/forum.

[16] 'Certification Policy for the Notarial Electronic Signature of Member States of the International Union of Latin Notaries (U.I.N.L),' policy number 7.

[17] 'Certification Policy for the Notarial Electronic Signature of Member States of the International Union of Latin Notaries (U.I.N.L),' policy number 7.

[18] See NATIONAL E-NOTARIZATION STANDARDS, Standards 14 and 15 (Nat' l Ass' n of Secretaries of State 2006) available at http://www.nationalnotary.org/commission; FIRST INTERNATIONAL FORUM ON E-NOTARIZATION AND E-APOSTILLES, Conclusions 15 and 18 (Nat' l Notary Ass' n 2005) available at http://www.e-app.info.

[19] Bernard Reynis and Ugo Bechini, 'European Civil Law Notaries Ready to Launch International Digital Deeds,' Digital Evidence and Electronic Signature Law Review (formerly the Digital Evidence Journal), 4 (2007) 14 - 18.

[20] See presentation by Ugo Bechini concerning the European Platform for Digital Signature Verification (IVTF), 'International E-Notarization: European Developments,' delivered at the Third International Forum on e-Apostilles, e-Notarization, and Digital Evidence (2007), available at http://www.nationalnotary.org/forum. Further information concerning the IVTF can be found at http://www.cnue.eu.

[21] Third parties may verify qualified digital certificates used by United States notaries at http://www.ensvalidate.org.

[22] XXIV International Congress of Latin Notaries, 'Conclusions of the Working Group for Theme II' (2004), available at http://www.uinl.org.