

4TH INTERNATIONAL FORUM ON E-NOTARIZATION, E-APOSTILLES AND DIGITAL EVIDENCE

*Organized and hosted by the National Notary Association
of the United States of America,
held on 29 – 30 May 2008 in New Orleans, Louisiana, USA*

Conclusions & Recommendations¹

1. Over 110 experts from 25 States, including representatives from the Hague Conference on Private International Law (HCCH) and the International Union of Notaries (UINL), government representatives (including several from Competent Authorities designated under the Hague Apostille Convention²), notaries from civil law, common law and mixed law jurisdictions, and other professionals, convened in New Orleans, Louisiana (USA) to attend the Fourth International Forum on e-Notarization, e-Apostilles and Digital Evidence, organized and hosted by the National Notary Association of the USA (NNA).³ The Forum attendees congratulated the NNA for its efforts to bring leading experts and authorities from around the world together to discuss issues of digital evidence, especially as they relate to e-Notarization and e-Apostilles.

I. The Electronic Apostille Pilot Program (e-APP)

2. The attendees congratulated the Permanent Bureau of the HCCH and the NNA on their continuing efforts related to the e-APP. It was again emphasized that the spirit and letter of the Apostille Convention are not an obstacle to the use of modern technology to further improve the practical operation of the Convention. The Forum further acknowledged that not only Competent Authorities benefit from implementing the e-APP but indeed any user of Apostilles (whether as a requesting person or final recipient), because the overall operation of the Convention is greatly improved, security dramatically enhanced and fraud effectively combated.

¹ These Conclusions & Recommendations were drafted and suggested by Timothy Reiniger, Executive Director, National Notary Association (USA), Christophe Bernasconi, First Secretary, Hague Conference on Private International Law, and Stephen Mason, Barrister. They were then submitted to, amended and endorsed by a Faculty of Forum attendees.

² *Hague Convention of 5 October 1961 Abolishing the Requirement of Legalisation for Foreign Public Documents*. For more details on this Convention, see the “Apostille Section” on the Hague Conference’s website at <<http://www.hcch.net>>.

³ The presentations as well as a full list of participants and the complete program can be found on the website dedicated to the International Forum at <<http://www.nationalnotary.org/forum>>, as well as on the Hague Conference’s website at <<http://www.hcch.net>>. An electronic copy of these Conclusions & Recommendations can also be found on the website dedicated to the e-APP at <<http://www.e-APP.info>>.

3. The Forum congratulated the Murcia Superior Court of Justice, Spain, for its comprehensive endorsement of the e-APP and the work it has accomplished in implementing e-Apostilles as suggested under the e-APP. The implementation of the e-Apostilles component was completed technically, and the first e-Apostille is to be issued in Murcia in the near future. E-Apostilles are to be issued in the first instance for public documents relating to inter-country adoption matters; in the future, they will be extended to include all public documents presented to the Court. Furthermore, the Murcia Superior Court of Justice also plans to implement an e-Register in the first quarter of 2009. The Forum emphasized that the work conducted by the Murcia Superior Court of Justice has the characteristic of a model implementation of the e-APP.

4. The Forum also congratulated the United Kingdom for announcing that it will be ready to test the implementation of both components of the e-APP in March 2009 at the latest. The Forum further congratulated Bermuda for announcing that in the first quarter of 2009 it will have in place an e-Register and the capability of issuing e-Apostilles.⁴

5. The Forum recalled that States should strive to achieve high standards in the issuance and management of digital credentials for Competent Authorities, including personal appearance before a qualified Registration Authority operating on behalf of a Certificate Authority issuing digital certificates used to digitally sign e-Apostilles.

6. Whilst strongly encouraging States to recognize foreign e-Apostilles issued according to the model suggested under the e-APP, the Forum recalled again that the probatory weight of Apostilles, whether issued in paper or electronic form, remains subject to the relevant rules of the jurisdiction where they are produced. Arguably, it is conceivable to require the sending State to contact the receiving State to make sure e-Apostilles will be accepted, but if this approach was taken, then it would, in effect, give the receiving State the opportunity to reject e-Apostilles, which might hinder the development of e-Apostilles altogether, and also provide receiving States with a greater power in the digital world than they have in the physical world.

7. Finally, the Forum recognized that the model of an e-Register suggested under the e-APP is an invaluable tool to enhance the use and consultation of Apostilles-Registers to check the origin of Apostilles.

II. Digital Evidence

A. Admissibility of evidence

8. Provisions relating to the admissibility of evidence have, in general, been passed in many jurisdictions by way of amendments to existing legislation or changes to procedural rules. Whilst some jurisdictions have yet to deal with the changes brought about by digital evidence (such as a number of African countries), others, such as China and India can be considered to be in an intermediate phase, where some changes have been made, but not comprehensively.

⁴ For comprehensive and updated information regarding the e-APP, see the e-APP website at <http://www.e-APP.info>.

B. Authenticity of evidence

9. There is more divergence in respect of the authenticity of evidence in legal proceedings. Some jurisdictions do not require evidence to be authenticated before being admitted into legal proceedings, but the procedural rules in other jurisdictions require evidence to be authenticated before being admitted. Yet other jurisdictions provide for procedural rules whereby parties admit the authenticity of the documents unless otherwise challenged in advance of the proceedings. Further, in jurisdictions where the authenticity of a document must be proven before being admitted, there may be a general practice where if the parties do not take an issue regarding the authenticity of the documents, and the judge agrees, then the documents will be admitted without the need for authentication. Further issues may arise where a jurisdiction classifies evidence, and it may be a matter of debate as to which category the evidence fall into, which in turn will affect its admissibility, how it can be challenged, any presumptions that might apply and what weight will be assigned to the evidence.

10. Generally, notarial acts properly executed (by either a common law notary or a civil law notary) will be admitted into evidence and accepted in most courts because of the legal requirements that apply to such acts, but there will be occasions when notarial documents will not be accepted, such as where a State provides that only a digital signature will be recognized unless another form of electronic signature has been agreed between the parties. Where a notarial act is accompanied by a form of electronic signature other than a digital signature, it is conceivable that the notarial act may not be accepted.

III. Electronic Notarial Acts

11. Whilst the electronic notarial act is a legal and practical reality in some common law jurisdictions, there still seem to be some challenges in civil law jurisdictions. The major considerations in civil law jurisdictions relate to the conditions for the establishment of and legal effects of the notarial act, including in particular its authenticity. There are at least five issues of relevance in this regard:

A. The reception and execution of an electronic notarial act

12. This includes the requirement of the simultaneous presence of the parties and the notary (or of a notary in the case of dual or multiple notaries) at all phases of the establishment of the notarial act, independently of whether it is executed in paper or in electronic form. Also, if fraud occurs with respect to the actual content of a notarial act, the question of what was actually the subject of the act will have to be determined by the applicable law designated by the conflict of laws rules of the forum.

B. The conservation of the 'original' (electronic) notarial act

13. Discussion of whether there is an original digital document is fraught with semantic difficulties. It remains an open question as to whether there can be an original act in the digital world. A number of Forum attendees suggested that it is debatable whether there can be a concept of an 'original' document in the digital world, and that the emphasis should be on trustworthiness, integrity and reliability. Conservation is also a significant consideration, as is how to deal with

digital signatures. These are complex matters that are merely highlighted but not elaborated upon in this document.⁵

C. The use and recognition of electronic signatures in a notarial act

14. There are several inter-related issues in respect of electronic signatures. First, some States only recognize the digital signature in particular types of transaction, and give other forms of electronic signature a lesser degree of weight. Secondly, it is suggested that the difference between the signature and the security of the document should be considered separately. In essence, it is necessary to be sure about the process of managing the identity of clients, providing proof of intent and providing for the security of the process.

D. The integrity of the notarial act and issues relating to security

15. The integrity of the notarial act is closely allied to security and is fundamental to the acceptance of the notarial act. In essence, it is probably correct that the authenticity of the underlying document may well be challenged, rather than the actual notarial act itself. This is because, providing notaries continue to carry out their duties in person, the point of attack will have to be considered elsewhere along the chain of control. In all probability, a person will try to get a forged document notarized, rather than attempt to hack into complex systems and change documents and registers.

16. There are advantages and disadvantages to the manuscript signature and the electronic signature (in particular the digital signature). Regardless of the problems associated with electronic signatures, the main concern surrounds the cost of proving a document was properly notarized and signed. Two significant issues arise: interoperability and simplicity. Both are complex areas, and despite the fact that a system might be simple to use, such as digital signatures, nevertheless the simplicity of use disguises the complexity of the physical and virtual infrastructure and the contractual relationships that determine liability. Given the nature of the office of the notary, the liability issues must be at the forefront of the adoption of any infrastructure dealing with electronic notarial acts.

17. Whilst the technology is very complex, nevertheless it is important not to lose sight of where the weakest point of attack is, and it is improbable that a person would take the time and trouble to subvert the system, so much as to attempt to pass off a false document to be notarized. In this respect, the individual notary will already have well tried and tested systems in place to detect most attempts at undermining the notarial act, but consideration must be given to testing electronic documents. Clearly any breach of e-security can be devastating to the integrity of the entire system, but it is important to be realistic in assessing the point at which a person might attack the process of issuing a notarial act.

⁵ For more details, see Stephen Mason, *Electronic Evidence: Disclosure, Discovery & Admissibility*, Chapter 4, (LexisNexis Butterworths, 2007).

E. Issues relating to private international law and the electronic notarial act

18. An additional challenge of using electronic notarial acts is whether computer-generated, electronically signed copies or originals will be recognized as an authentic instrument in other jurisdictions and even if so, whether or not the legal effects attributed to foreign Notarial Acts will be given to them.

IV. Call for International Assurance Standard to Guide Notaries Societies in the Issuance of Trustworthy Electronic Notary Signatures

19. The NNA tabled a proposed “The International Electronic Notarization Assurance Standard” for discussion and adoption by Notaries Societies around the world. The NNA based the proposal on Conclusions 17 through 19 from the Forum held in Las Vegas, Nevada in 2005, UINL policy positions concerning Notaries Societies as Issuing Authorities for member notaries, as well as previous Forum presentations reflecting the implementation of PKI by Notaries Societies in Europe, North America, Central America, South America, Asia, and Australia.

20. Attendees discussed the need for an international assurance standard to provide consistency amongst the various national Notaries Societies in the issuance and authentication of electronic notary signatures. The Standard would be useful in establishing the actions of individual notaries when electronically signing in an official capacity. However, it must be emphasized that such a Standard, if not adopted widely throughout the civil law and common law states, might not have the desired effectiveness for international commerce. The Forum encouraged a continuation of the discussion on possible standards for e-Notarization, beyond the current proposal.

21. The Forum directed the NNA to form an International Working Group that will consider the public comments and to produce a revised proposal. The Forum further directed the NNA to submit this revised version of the International Assurance Standard to the UINL for formal consideration.

* * *