5TH INTERNATIONAL FORUM ON THE ELECTRONIC APOSTILLE PILOT PROGRAM (E-APP) AND DIGITAL AUTHENTICATION

London, United Kingdom, 13 June 2009

Conclusions & Recommendations

1. Over 120 experts from 41 countries, including several representatives from Competent Authorities designated under the Hague Apostille Convention [1] and other government representatives, notaries from civil law, common law and mixed law jurisdictions, and other professionals, as well as representatives from the Hague Conference on Private International Law (HCCH) and the International Union of Notaries (UINL), convened in London, United Kingdom, to attend the *Fifth International Forum on the electronic Apostille Pilot Program (e-APP) and Digital Authentication* organized by the International Union of Notaries (UINL) and the Hague Conference on Private International Law (HCCH).[2] The aim of the Forum was to bring experts from around the world together to discuss issues relating to the further development of the e-APP and digital authentication more broadly. On the occasion of the first Forum to be held in Europe, the participants recognized the importance and value in considering geographic variety and legal diversity when choosing future venues.

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

2. The Forum congratulated the Permanent Bureau of the HCCH and the National Notary Association of the United States of America (NNA) on their continuing efforts related to the promotion and the development of the e-APP. It was again emphasized that neither the spirit nor the letter of the Apostille Convention are an obstacle to the use of modern technology to further improve the practical operation of the Convention. In particular, the Forum recognized that the issuance of e-Apostilles and the operation of e-Registers greatly improve the effective and secure operation of the Apostille Convention. The Forum acknowledged again that not only Competent

---

1 *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 >.

2 The presentations can be found on the "Apostille Section" of the Hague Conference's website at < http://www.hcch.net > and on the website dedicated to the e-APP at <http://www.e-APP.info>.

Authorities, but indeed any user of Apostilles (whether as a requesting person or final recipient) benefit from the implementation of the e-APP.

3. Echoing the Special Commission held in The Hague in February 2009 which reviewed the practical operation of the Apostille Convention, the Forum noted with great satisfaction that several jurisdictions (Belgium, Bulgaria, Colombia, Spain, Moldova, New Zealand, Kansas, Rhode Island) had already implemented one, or both, of the components of the e-APP. The Forum congratulated in particular the Murcia Superior Court of Justice (Spain) and the Authentication Unit of the Department of Internal Affairs of New Zealand for having fully implemented the e-Apostille component as suggested under the e-APP. This involves the issuance of e-Apostilles by using a digital certificate, and by (partially) inserting the underlying electronic public document into the e-Apostille or attaching it thereto. The Forum emphasized that the work conducted by the Murcia Superior Court of Justice and the Authentication Unit of the Department of Internal Affairs of New Zealand may well represent a model implementation of the e-Apostille component of the e-APP. The Forum further applauded the efforts of several States and jurisdictions (in particular the United Kingdom, Bermuda and Delaware) that are actively pursuing implementation of one or both components of the e-APP. The Forum invites States Parties who have not yet done so to consider actively implementing the e-APP.[3]

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

5. Recalling the fundamental principle of the Convention according to which an Apostille validly issued in one State Party must be accepted in other States Party, mindful that the Convention is silent as to the means of production of Apostilles, be it paper or electronic, and adopting a "functional equivalent approach" based on an analysis of the purposes and functions of the traditional paper-based model of Apostilles with a view to determining how those purposes or functions can be fulfilled through electronic means, the Forum strongly encouraged States Parties to the Apostille Convention to accept and recognise foreign e-Apostilles issued according to the model suggested under the e-APP (see above paragraph 3). The Forum, however, also recalled 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. Finally, the Forum recognized that it is good policy that States Parties inform the other States Parties when they begin to issue e-Apostilles.

6. 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. The Forum recognised in particular the value of e-Registers that also provide information relating to the underlying public document or a copy thereof. Furthermore, the Forum suggested that Competent Authorities operating an e-Register use a SSL Certificate or similar technology to secure the relevant website.[4]

---

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

[4] Typically, a SSL Certificate contains the following information: (i) the domain name for which the certificate was issued; (ii) the owner of the certificate and the domain name; (iii) the physical location of the owner; (iv) the

7. The Forum echoed the determination of the Special Commission 2009, according to which it is for the law of the State of origin to determine the public nature of a document, and that States Parties should give a broad interpretation to the category of public documents.[5]

II. Electronic Notarial Acts

8. Electronic notarial acts are a legal and practical reality in some common law jurisdictions. There seem to be more challenges in this respect in civil law jurisdictions, although it was noted that several civil law jurisdictions have enacted legislation for the execution of electronic notarial acts. In particular, the Forum noted with great interest that the first electronic notarial act was executed in France in October 2008. The major considerations in civil law jurisdictions relate to the conditions for the establishment and the legal effects of the notarial act, including its authenticity. The greatest challenges seem to stem from (i) 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 execution of the notarial act, independently of whether it is executed in paper or in electronic form; (ii) the conservation of the 'original' (electronic) notarial act;[6] (iii) the use and recognition of electronic signatures in a notarial act; and (iv) the integrity of the notarial act, including issues relating to security. 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.[7]

* * *

---

validity dates of the certificate. The certificate is proof that an independent trusted third party has verified that the website belongs to the authority, person or company it claims to belong to. SSL certificates can provide visitors of the website with proof of the website's identity, and confidence in the integrity and security of online communications.

5 See Conclusions & Recommendations Nos 72-77 of the Special Commission 2009, available on the "Apostille Section" of the HCCH website at < http://www.hcch.net >.

6 Recalling the discussion of the fourth Forum held in 2008, it was noted again that the debate of what constitutes an 'original' digital document and what constitutes a copy of an original electronic document is loaded with semantic difficulties. The Forum noted with great interest that centralized registers for the conservation of electronic notarial acts have been established in Belgium and France.

7 Some Forum attendees suggested that the Hague Conference conduct further studies on this topic.