AFFAIRES GÉNÉRALES ET POLITIQUE
GENERAL AFFAIRS AND POLICY

Doc. prél. No 18
Prel. Doc. No 18

mars / March 2007

HccH
HAGUE CONFERENCE ON
PRIVATE INTERNATIONAL LAW
CONFÉRENCE DE LA HAYE
DE DROIT INTERNATIONAL PRIVÉ

PROGRAMME PILOTE D'APOSTILLES ÉLECTRONIQUES (*e-APP*)

MÉMOIRE SUR CERTAINS ASPECTS TECHNIQUES FONDANT LE MODÈLE PROPOSÉ POUR L'ÉMISSION D'APOSTILLES ÉLECTRONIQUES (E-APOSTILLES)

établi par
*Christophe Bernasconi (Bureau Permanent) et Rich Hansberger (*National Notary Association*)*

* * *

ELECTRONIC APOSTILLE PILOT PROGRAM (e-APP)

MEMORANDUM ON SOME OF THE TECHNICAL ASPECTS UNDERLYING THE SUGGESTED MODEL FOR THE ISSUANCE OF ELECTRONIC APOSTILLES (E-APOSTILLES)

drawn up by
Christophe Bernasconi (Permanent Bureau) and Rich Hansberger (National Notary Association)

Document préliminaire No 18 de mars 2007
à l'intention du Conseil d'avril 2007
sur les affaires générales et la politique de la Conférence

Preliminary Document No 18 of March 2007
for the attention of the Council of April 2007
on General Affairs and Policy of the Conference

Permanent Bureau | *Bureau Permanent*
6, Scheveningseweg 2517 KT The Hague | *La Haye* The Netherlands | *Pays-Bas*
telephone | *téléphone* +31 (70) 363 3303 fax | *télécopieur* +31 (70) 360 4867
e-mail | *courriel* secretariat@hcch.net website | *site internet* http://www.hcch.net

PROGRAMME PILOTE D'APOSTILLES ÉLECTRONIQUES (*e-APP*)

MÉMOIRE SUR CERTAINS ASPECTS TECHNIQUES FONDANT LE MODÈLE PROPOSÉ POUR L'ÉMISSION D'APOSTILLES ÉLECTRONIQUES (E-APOSTILLES)

établi par
*Christophe Bernasconi (Bureau Permanent) et Rich Hansberger (*National Notary Association*)*

* * *

ELECTRONIC APOSTILLE PILOT PROGRAM (e-APP)

MEMORANDUM ON SOME OF THE TECHNICAL ASPECTS UNDERLYING THE SUGGESTED MODEL FOR THE ISSUANCE OF ELECTRONIC APOSTILLES (E-APOSTILLES)

drawn up by
Christophe Bernasconi (Permanent Bureau) and Rich Hansberger (National Notary Association)

Introduction

1. Under the electronic Apostille Pilot Program (e-APP), the Hague Conference on Private International Law (HCCH) and the National Notary Association (NNA) are, together with any interested State (or any of its internal jurisdictions), developing, promoting and assisting in the implementation of low-cost, operational and secure software models for (i) the issuance of and use of electronic Apostilles (e-Apostilles), and (ii) the operation of electronic Registers of Apostilles (e-Registers). The e-APP was officially launched during the Special Commission on General Affairs and Policy of the HCCH in April 2006. It is designed to illustrate how the Conclusions and Recommendations of the 2003 Special Commission meeting on the practical operation of the Hague Apostille Convention and the 2005 International Forum on e-Notarisation and e-Apostilles can be implemented in practice by relying on existing and widely used technology.[1] The e-APP, it should be emphasised, offers and promotes the adoption of software *models* that are freely configurable by participating States. Additionally, States are welcome to develop their own software solutions and to work collaboratively within the co-operative framework of the e-APP. Although States are not required to share their systems or models in an open-source environment under the e-APP, it is the hope of the e-APP that, at the very least, participating States will use the e-APP to educate each other about their work, shared visions, and – to the extent necessary – legal environments.[2]

2. The purpose of this Memorandum is to offer additional information and explanations on the technical aspects of the model suggested for the issuance of e-Apostilles, particularly on the use of digital signatures (I.), the format of an e-Apostille (II.), as well as on the use and status of a printed version of an e-Apostille (III.). The goal of the e-APP is to facilitate communication and co-operation among participating States, and this Memorandum is written in that continuing spirit of collaboration. This Memorandum, then, is part of an on-going dialogue between States participating in the e-APP and documents numerous questions, reflections, and insightful suggestions made by participating States, interested observers, and potential e-APP participants.

3. Participation in the e-APP does not require a formal agreement between States, nor does it require any kind of binding commitment to the Pilot Program. By participating in the e-APP, we encourage States to share ideas, examples, and resources to as great an extent as they can in order to facilitate the wider adoption of e-Apostilles and e-Registers.

---

[1] The e-APP made a breakthrough in February 2007, when the state of Kansas issued the first test e-Apostille in accordance with the model suggested under the e-APP, and Colombia, the receiving State, officially indicated its acceptance of this test e-Apostille. As a result, the two jurisdictions are now ready to complete authentications of public documents entirely electronically. Furthermore, the state of Rhode Island joined the e-APP by adopting and implementing the Program's free, open-source electronic Register software. Any interested person can now conduct a secure, online search for an Apostille issued by Rhode Island officials (currently in paper form, soon also in electronic form) by entering its number and date and the register will show automatically if a matching entry can be found, thus allowing receiving parties to verify the origin of the Apostille much more quickly and efficiently than can be accomplished currently.

[2] In this context, it may be useful to recall para. 7 of the Conclusions of the Second International Forum on e-Notarisation and e-Apostilles (held in Washington in May 2006), which reads as follows: "Participants also noted that if there are domestic laws, rules, or any regulations relating to the execution of electronic notarial acts, the use and administration of electronic signatures, or the transmission of electronic documents (including notarial acts), these laws, rules, or regulations continue to apply under the suggested models developed for the purposes of the e-APP […]." The First International Forum on e-Notarisation and e-Apostilles (held in Las Vegas in May 2005) had already recognised that "[m]ost countries have now enacted legislation recognising the legal effect of electronic signatures and electronic documents"; the Forum encouraged States "to continue reviewing and enhancing the legal framework for allowing the use of electronic signatures and electronic documents" (para. 2 of the Conclusions). The Conclusions of both the first and second Forum are available on the "Apostille Section" of the Hague Conference's website < www.hcch.net >.

I. Digital Signatures: A Question of Trust

A. Verifying digital signatures in Adobe

4. The model suggested for the issuance of e-Apostilles uses out-of-the-box, PDF technology (see also below under II.), Furthermore, under the suggested model Competent Authorities use digital certificates to digitally sign the e-Apostille they are issuing. In this context, it is important to emphasise that when a person digitally signs an Adobe PDF document, by design Adobe does not "trust" the digital certificate. Adobe designed its PDF software this way as a security check and balance, so to speak. This is in sharp contrast to (and a thinly veiled criticism of) the approach taken so far in the Microsoft Windows operating system (see, however, the comments below in para. 11). The Windows operating system (Windows 2000 and subsequent versions) automatically trusts digital certificates from a number of providers. Most end users do not realise this fact, which has been criticised by some security experts as a potential security flaw. If one receives a digitally signed Word document, for example, from a Certificate Authority that Microsoft has already decided it trusts, one will not receive any alerts as to the possibility or need to review the certificate before deciding to trust it. Adobe, by contrast, requires an end user to deliberately add the certificate to its list of trusted identities to ensure the recipient has the ability to determine who to trust and not trust.

5. The security process Adobe has established is designed so that the recipient of the document can independently verify the authority and identity of the sender of the document. The recipient can do this by contacting (*e.g.*, calling) either the sender directly or the sender's company or organisation and verifying the sender's title and identity (in the second example, the company or organisation would vouch for the actual sender). Another option is for the recipient to contact the Certificate Authority (*e.g.*, access its public key register on-line) and verify the origin of the certificate. Once satisfied with the verification process, the recipient then follows the steps described below to recognise and trust the digital certificate in the document signed by that sender. This process of recognising and trusting the digital certificate need only be completed once, as any future documents digitally signed by that sender's certificate will automatically be recognised and trusted by the receiver's Adobe software. The recipient may also choose not to verify the authority and identity of the sender's digital certificate, and instead choose to immediately follow the steps described below to trust the sender's digital certificate in the first and subsequent documents.

6. To configure Adobe 7.0 Reader/Standard/Professional to trust a digital Certificate Authority, the following steps must be taken:

1. Click on the trusted digital signature.
2. Click on the Signature Properties button in the Signature Validation Status dialog box.
3. Click on the Show Certificate button on the Summary tab in the Signature Properties dialog box.
4. Click on the Trust tab.
5. Click on the Add to Trusted Identities button.
6. Click on the OK button.
7. In the Import Contact Settings dialog box, check the appropriate Trust Settings checkboxes to trust the digital certificate.
8. We recommend that the user select only the first checkbox for "Signatures and as a trusted root".

7. It is important to point out that this process of trusting a digital certificate from a particular sender (such as a Competent Authority) can essentially be reversed. In other words, a recipient can decide *not* to trust a sender's digital certificate. To configure Adobe 7.0 Reader/Standard/Professional to "untrust" a digital Certificate Authority, one has to take the following steps:

1. Click on the digital signature one wants to "untrust".
2. Click on the Signature Properties button in the Signature Validation Status dialog box.
3. Click on the Show Certificate button on the Summary tab in the Signature Properties dialog box.
4. Click on the Trust tab.
5. Click on the Add to Trusted Identities button.
6. Click on the OK button.
7. In the Import Contact Settings dialog box, de-select the appropriate Trust Settings checkboxes to "untrust" the digital certificate.
8. Example: If the first checkbox for "Signatures and as a trusted root" is checked, simply de-select this checkbox.

8. For additional information regarding digital signature trust in Adobe, one may search the Adobe Help files for the entry titled "Determining the trust level of a certificate" or simply "Digital certificates".

9. In addition to the processes described above, recipients of an e-Apostille issued under the suggested model may be able to use other verification methods. In Kansas, for example (see the comments in footnote 1), the State of Kansas Root Certificate Authority maintains a Certificate Revocation List (CRL) that can be accessed using a standard Web browser by navigating to the internet location (URI) of the CRL. Under a second – and much simpler method – verification of a Kansas Certificate is possible simply by accessing a website < https://digitalid.verisign.com/services/client/index.html >. On this web site, any recipient of a digitally signed document from a Kansas State government official can enter the certificate holder's email address to verify a) the current status of the digital certificate in question (whether it is current and in good standing, revoked, expired, etc.), and b) the serial number of the digital certificate. The two verification methods described are made available at no cost and provide a simple means to determine the current validity of a digital certificate.

10. Though we realise that PDF is not truly an open source technology, we would like to reiterate that the use of PDF technology under the model for e-Apostilles is a *suggested* model only. In other words, and as already noted, we encourage Competent Authorities to develop alternative models and to share these developments with the e-APP participant community. Competent Authorities may choose to offer the alternative models for use by other Competent Authorities under the auspices of the e-APP (as long as the models are freely licensed), but even if the models are not offered for use by other Competent Authorities our hope is that information about the models will be made freely available to the e-APP community.

11. We would also like to point to some interesting developments by Microsoft in their upcoming release of Microsoft Office 2007. This new version will include built-in support for digital signatures almost identical to Adobe's. Thus, a Competent Authority could presumably digitally sign an e-Apostille in Microsoft Word 2007 with the same security and assurances provided currently in Adobe PDF. We feel that this development signals an important trend in support of the technology recommended under the e-APP. The fact

that Microsoft supports the technology recommended under the e-APP (however inadvertent that support is) reflects a positive development that, very soon, will enable any Competent Authority with a copy of Microsoft Word 2007 to execute e-Apostilles safely and securely, thus supporting an even broader use and distribution of e-Apostilles. The new version of Microsoft Word 2007 also includes free, built-in conversion support for PDF. In short, the Competent Authority will be able to choose to distribute the e-Apostille electronically in Word *or* PDF with just the click of a button.

B. Basics of a Public Key Infrastructure (PKI)

12. The Adobe PDF digital signature trust model is premised on the operational guidelines of a Public Key Infrastructure (PKI). Although we only have space here to discuss the basic tenets of PKI,[3] it is important to note that a PKI involves certain key actors, including a Certificate Authority (CA) and a Registration Authority (RA). A CA is an independent third-party to any transaction that occurs within a PKI. The CA issues the digital certificate that is used to digitally sign the PDF. The CA is an audited organisation that must adhere to strict operating procedures in order to maintain trust in the digital certificates that it issues. The RA is a party contracted to the CA that is solely responsible for proofing the identity and establishing the related rights and duties of a person requesting a digital certificate. Again citing the first test e-Apostille, the State of Kansas in the United States acted as an RA by issuing a digital certificate to an employee within the Kansas Secretary of State's office. Trust within a PKI relies on the CA and RA acting responsibly and subjecting themselves to independent audits and oversight. However, trust within a PKI is also in the hands of the transacting parties, which typically includes a document signer and the document recipient. As explained above, if the document recipient *trusts* that the CA and RA are credible actors, then the document recipient can in turn trust that the document signer is who he/she claims to be and is acting within the scope of his/her authority. The document recipient, in other words, has complete authority to trust or not trust transactions within a PKI.

13. In addition to the PKI trust model, other important features are included or can be included within a given PKI infrastructure.

(1) One important feature that participants in a PKI infrastructure can rely upon is the Certification Practice Statement (CPS). The CPS contains the statement of roles, responsibilities, and requirements that govern the issuance, use, and management of digital certificates within a particular PKI, among other things. Thus, a CPS, as one example, might state that all digital certificates issued under the CPS require the applicant for a digital certificate to be identified in person by an appropriately contracted RA. In many cases, a CPS is written to comply with the Internet Engineering Task Force (IETF) Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. Under the e-APP, the state of Kansas in the United States has issued the following CPS that governs its management of digital certificates.

(2) In addition, a governmental or private entity might be subject to local laws, rules, and / or regulations that govern the issuance and use of digital certificates. For example, with respect to the first test e-Apostille issued by the Competent Authority of Kansas, local state regulations govern the issuance and management of digital certificates by the Kansas Root CA. An important

[3] Readers interested in a more thorough explanation of PKI may wish to start here: < http://en.wikipedia.org/wiki/Public_key_infrastructure > (as per 19 March 2007). Special and general reference resources are abundant, and Wikipedia provides an excellent introduction to these resources.

feature of these regulations is that all applicants are required by law to appear in person before an authorised government official and present at least one government-issued picture identification document to a Local Registration Authority to request and receive a digital certificate from the state of Kansas CA. At this time, Kansas allows Chief Election Officers to serve as Local Registration Authorities.

(3) To facilitate more rapid and reliable verification of revocation, a CA might enable a feature known as Online Certificate Status Protocol (OCSP). OCSP enables more rapid and reliable checks of the revocation status of a digital certificate issued by a particular CA. Thus, OCSP, although not required in a PKI, can provide a more efficient and faster means of verifying whether or not a given digital certificate has been revoked or is still valid. Although the state of Kansas CA does not yet offer OCSP revocation checking, it may do so in the future.

14. It is our understanding that the secure electronic signature process as embedded in Adobe technology and described above is in line with the UNCITRAL 2001 Model Law on Electronic Signatures (see, in particular, Art. 6, 7 and 12(3)), as long, of course, as the conduct of the signatory and the certification service provider meet the requirements set out in Articles 8 and 9 of the Model Law. Article 2(a) of the Model Law defines an electronic signature as "data in electronic form in, affixed to or logically associated with, a data message [*i.e.*, the Apostille], which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message." And the test for reliability of an electronic signature, as stated in Article 6 of the UNCITRAL Model Law, "is met in relation to a data message if an electronic signature is used that is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement." Adobe's secure electronic signature process as described above conforms well to this definition of an electronic signature.[4]

15. Further, the standard applied in Article 12(3) of the UNCITRAL Model Law for the recognition of electronic signatures created in another State provides another authoritative basis for the recognition between States Parties to the Convention of e-Apostilles issued in conformity with the model suggested in the e-APP.[5] Again, it is our view that the model suggested under the e-APP offers a very high level of reliability and thus e-Apostilles issued under this model should be recognised between States Parties. This argument is further enhanced by the general principle under the Convention that an Apostille validly produced in one State Party to the Convention must be recognised by another State party to the Convention.[6] Finally, and maybe most importantly, it may be useful to recall that thousands (if not millions) of Apostilles are issued every year by using signature stamps or scanned copies of holographic signatures; although these signing techniques offer significantly lower levels of security than the model suggested

---

[4] See also the definitions of "data message" and "signatory" in Art. 2(c) and 2(d), respectively, of the UNCITRAL Model Law on Electronic Signatures. Art. 2(c): "'Data message'" means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy"; Art. 2(d): "'Signatory' means a person that holds signature creation data and acts either on its own behalf or on behalf of the person it represents".

[5] Art. 12(3) reads as follows: "An electronic signature created or used outside *[the enacting State]* shall have the same legal effect in *[the enacting State]* as an electronic signature created or used in *[the enacting State]* if it offers a substantially equivalent level of reliability."

[6] It is based on this principle that the Permanent Bureau has consistently argued that foreign Apostilles cannot be rejected by a receiving State merely on the grounds that they do not conform to the manner in which Apostilles are issued in the receiving State (for example, with colorful ribbons, wax, and rivets). See Conclusion & Recommendation No 13 of the Special Commission Meeting of 2003.

under the e-APP, they have – to the best of our knowledge – never led to any serious problems of recognition of foreign Apostilles.

C. Long-term Viability of PDF Documents

16. We have received questions regarding the long-term viability of a commercial product such as Adobe PDF, and more specifically how the e-APP might address whether a digitally signed PDF document executed in the year 2007 would be viewable by some recipient – at no cost – in the year 2030 (or beyond). While this is an engaging and actively studied area,[7] the scope of this Memorandum does not extend to a discussion of long-term electronic document archival. The existing PDF specification is partially an open specification that allows anyone – free of royalties or licenses – to develop software that reads and writes to the PDF specification. Significantly, Adobe recently announced that it is releasing the entire PDF document specification to an open and independent international standards body for public use.[8] In brief, allowing the PDF specification to be managed by an independent standards body ensures that software developers can access and view PDF documents using that open standard at theoretically any point in the future without requiring the purchase of an Adobe license.

II. The Format of an e-Apostille: either one continuous PDF file, or a PDF file with an attachment

17. In the e-APP, we contemplated two distinct but ultimately identical formats for e-Apostilles. Both methods protect the underlying document and the e-Apostille Certificate from unauthorised modifications, but each one presents a different interface to the recipient.

18. Under the first method, a Competent Authority can add the Apostille Certificate as the final page to an existing underlying public document in PDF. Using this first method, then, the recipient would open the PDF document and find the e-Apostille Certificate included as the last page of the same PDF document. If this format is chosen, the underlying public document and the e-Apostille Certificate form one continuous document or, put another way, one single PDF file. One could still choose to print one or more pages of this single file, so that the e-Apostille Certificate could be printed by itself (see point III. below for more information on this topic).

19. Under the second method, the underlying public document is attached as a separate file to the e-Apostille Certificate. This is the method Kansas chose for their test e-Apostille. The recipient still receives a single PDF file, but upon opening the file, the user first views the e-Apostille Certificate, and can then open the attached underlying public document to view it as a separate PDF file. In our view, this method provides a more intuitive interface to the recipient of the apostillised document (incidentally, it is also the one adopted by the United States Department of State for their electronic patent filings and their model of e-Apostilles). By attaching the underlying public document as a file to the e-Apostille Certificate, the intent is to make it very clear to the recipient when he / she first opens the document that he / she is dealing with an Apostille. From there, he / she can then open the underlying public document to view its contents.

20. Under the e-APP, a Competent Authority may select either model, and the e-APP does not suggest that one or the other model is preferable.

---

[7] Readers interested enough to investigate this topic further may wish to review the work of the LTANS (Long-Term Archive and Notary Services) Working Group of the IETF (Internet Engineering Task Force – the IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet; it is open to any interested individual); the LTANS Working Group is developing an Evidence Record Syntax for the long-term storage and retrieval of digitally signed documents over long and possibly undetermined periods of time. See < http://www.ietf.org/html.charters/ltans-charter.html > (as per 19 March 2007) for more information.

[8] Readers can refer to Adobe's press release on the subject here: < http://www.adobe.com/aboutadobe/pressroom/pressreleases/200701/012907OpenPDFAIIM.html > (as per 19 March 2007).

III. Printing the e-Apostille

21. Printing the e-Apostille Certificate (with or without the underlying public document) presents at least two issues that need to be addressed individually: (A) how to prevent fraudulent re-use of the e-Apostille Certificate in the printed medium; and (B) how to ensure that printing an e-Apostille Certificate will accommodate paper-only recordkeeping and evidence requirements.

A. How to Prevent Fraudulent Re-Use of an e-Apostille Certificate

22. The issue of preventing re-use of the printed version of an e-Apostille Certificate is a difficult one to resolve in the age of digital image editing software. Even if we were to exclusively use the first method described above, one could choose to print just the e-Apostille Certificate as a separate page, and we would still be faced with the problem of the fraudulent re-use of that Apostille Certificate for other documents. Indeed, one could simply capture a "printscreen" of the Apostille Certificate (type "Apostille" in Google Image Search…) or spend 30 minutes in Microsoft Word to create a perfectly valid looking impostor Apostille Certificate that could then be easily printed for fraudulent uses. Again, we suggest valuing the e-APP against the safety and anti-fraud levels currently reached in the paper-only environment; keeping in mind not just the e-Apostille, but also the e-Register component of the e-APP, we feel rather strongly that the e-APP by far exceeds current levels of safety and anti-fraud protection.

23. A further challenge lies in the absence of ability (and, for obvious reasons, of will) to build a centralised system for the management of e-Apostilles – at least not for the moment. While it is true that such a centralised system would allow to cost-effectively build security solutions into the system that every Competent Authority could take advantage of, under the e-APP, we neither have the option to create a centralised system (as it would most likely require a new Convention) nor the ability to impose upon a Competent Authority any specific software or hardware requirements (because the Convention is technically neutral).

24. This being said, fraudulent re-use of an electronic or paper Apostille is a problem that needs to be addressed. There are three main solutions in this respect: (a) the e-Register; (b) adding the exact date and moment of the signing of the underlying public document to the information provided under standard item 2 of the Apostille Certificate; and (c) using bar-codes.

25. (a) There is little doubt that the best way to deter fraudulent re-use of any Apostille (be it an electronic or a paper Apostille) is by encouraging, as much as possible, the use of the Register which every Competent Authority has to operate under Article 7 of the Convention. The e-APP dramatically enhances the advantages and benefits of these Registers by making them accessible online. (We would suggest that even if a Competent Authority never chose to issue an e-Apostille Certificate, keeping an electronic register is something every Competent Authority should be doing now). Imagine, for example, that every Competent Authority kept an online electronic Apostille Register that facilitated immediate and reliable verification of any Apostille issued by a Competent Authority. We would go a long way toward combating fraud with such a simple and global solution because every Apostille Certificate would be verifiable against an Internet-accessible e-Register. The challenge, of course, is that every Competent Authority must oblige by agreeing to host an e-Register. We have a long way to go before this ideal scenario plays itself out, but the e-APP, by offering a free, open source e-Register, goes quite a long way toward accomplishing this goal. In addition, the easy accessibility of the e-Register will provide the most important verification tool available for record-keeping and evidentiary purposes.

26. (b) Another method to link the printed version of an e-Apostille Certificate to the underlying public document is to add the exact date and moment of the signing of the underlying public document to the information provided under standard item 2 of the

Apostille Certificate. Thus, item 2 of an Apostille Certificate could include the following information: “John Doe, on 2007.01.12 13:46:17 -06'00”. It goes without saying that this additional information cannot be imposed as a general condition for paper Apostille Certificates; moreover, because this process requires a slight modification to the Model Apostille Certificate annexed to the Convention, we also do not want to impose it for e-Apostilles under the e-APP, but we do feel comfortable recommending this addition to Competent Authorities because it enhances the security features of an e-Apostille.

27. (c) Another method we recommend to allow printing while, at the same time, countering fraud, is bar coding. By embedding an Adobe “paper forms” bar code on the e-Apostille Certificate that includes data that is unique both to the e-Apostille Certificate and to the underlying public document, anybody (equipped with a scanning device, see below) presented with the printed version of the e-Apostille Certificate and the (underlying) public document, could scan the bar code to verify whether these printed documents do indeed belong together.

28. A “paper forms” bar code in the Help files of Adobe Designer 7.0 is defined as follows: “A paper forms barcode electronically captures user-supplied data in an interactive PDF form. When an end user fills the form using Adobe Reader or Acrobat, the barcode is updated automatically to encode the user-supplied data. The user can then return the filled form by printing it and returning it by fax, mail, or hand. Upon receipt, the user-supplied data can be decoded using a scanning device.” As described in this definition, the “end user” would be an official charged with completing Apostille Certificates as or on behalf of a Competent Authority. As envisioned under the e-APP, an Adobe paper forms bar code, otherwise known as a “dynamic” (as opposed to static) bar code, would allow the Competent Authority to embed, into the bar code, information that could include all the information contained in the 10 standard items of an Apostille Certificate, as well as the information contained in the digital certificate (such as the signer’s name, email address, etc.). Upon receipt of a printed e-Apostille Certificate containing such a bar code, the recipient could scan the bar code to reveal the values it contains; thus, the recipient of the printed e-Apostille could compare the values contained in the bar code against the information on the printed e-Apostille Certificate or the information contained in the e-Register to verify that the values in the bar code match the values in the printed e-Apostille Certificate or e-Register. Because bar codes are very difficult to forge, the recipient would have a high degree of assurance that nobody has tampered with the document. Bar codes, then, provide the most value when an e-Apostille Certificate is printed. Further, if the electronic original is lost, and only the printed e-Apostille remains, the bar code can continue to provide reliable verification into the foreseeable future. Thus, in the manner just described important data supplied by the user can be integrated into the bar code for security verification.

29. Of course, this solution presupposes that (a) the Competent Authorities have the software to produce bar codes and (b) that the recipients have the technology to scan and process bar codes, which presents a practical problem but one that can be overcome without too many obstacles. With the purchase of Adobe Standard or Professional comes the software “Adobe Designer”, which allows Competent Authorities to include bar codes in a PDF form, such as an e-Apostille Certificate, at no additional cost and with only minimal effort. In addition, the low cost of bar code scanners and their widespread use in the marketplace means that acquiring such a scanner should not represent too great an obstacle for many Competent Authorities. As for the previous point, we feel that we should not impose but merely suggest or recommend the use of bar codes.

30. A few comments on *watermarks*. We do not believe the full Apostille Certificate should appear as a watermark to the underlying public document. Such an approach would amount to a substantial change of the format of the Apostille Certificate and thus not be in line with the Model Certificate attached to the Convention. In addition, such a large watermark would make the underlying document difficult to read. It also poses practical problems with multi-page documents. However, we do want to explore using a small watermark as a recurring security feature that appeared in an unobtrusive location on each page of the underlying public document (such as repeating the number of the e-Apostille Certificate in a corner of each page of the underlying document).

B. How to Ensure that Printing will Accommodate Paper-only Recordkeeping and Evidence Requirements

31. We firmly believe that being able to print an e-Apostille (the Certificate and the underlying document) in such a manner that the printed version could be relied upon for recordkeeping and evidence purposes is an important goal. Put another way, perhaps the question is "how can we print an e-Apostille and verify that it has not been altered from its electronic original state?" This question, of course, goes to the subject of transformation in the digital age. The recommendations in section A. will also benefit paper-only recordkeeping and evidence requirements as the use of the e-Register, the additional information under item 2 of the e-Apostille Certificate and the bar codes will allow for verification of the origin and thus of the authenticity of a printed e-Apostille.

32. In this Memorandum, we do not intend to determine whether a printed version of an e-Apostille has the same legal standing as the electronic original. This question is likely to become relevant only if and when there is litigation about the origin of an e-Apostille, in which case both the paper and electronic versions of the Apostille are likely to be produced in court. On the basis of at least the electronic version – and certainly in combination with the Register and particularly if it is an e-Register accessible online as suggested by the e-APP – it will then be possible to assess with a very high degree of certainty the origin of the Apostille. Of course we assume that the receiving party would keep not just a printed version of the Apostille but also the electronic original. We actually believe that it is far more likely that the receiving party will keep only the electronic original.

33. Many governmental agencies store official documents electronically and only produce printed versions as true certified copies (birth certificates in the US, for example, are rarely stored in paper form; company charters, as another example, are almost exclusively electronic in many countries). Why should the reasoning or the standards be different for (e-)Apostilles? Also, as noted above (see para. 15), it is common practice to issue paper Apostilles bearing a signature stamp or a scanned copy of a holographic signature and we are not aware of any problems relating to the recognition of such Apostilles. A printed version of an e-Apostille Certificate issued under the model of the e-APP offers security and anti-fraud features which greatly exceed this common practice. Thus, it would be surprising to see recipients, courts and other end-users questioning the relevance of these e-APP features when, in fact, they enhance the genuineness of a paper document.

34. Finally, under the e-APP, we will continue to encourage States to put in place appropriate e-legislation (see Conclusion 2 of the First International Forum on e-Apostilles and e-Notarisation), but we not believe that we have to wait for this to happen everywhere. The e-APP may actually be regarded as a catalyst, in any event, both for States with enabling laws already in place and for those only now considering such laws.

IV. Further Suggested Changes

35. In addition to the suggestions discussed above, the following changes will be made to the e-Apostille model as originally suggested under the e-APP:

The original PDF software model will be changed so as to ensure that text boxes 2, 6 and 8 cannot be modified. As a result, all the text boxes will be equally protected from unauthorised modification.

It is also suggested (but not required) that the position of the person certifying the document be entered in text box 7.

Conclusion

36. As noted above, perhaps the most important goal of the e-APP is communication and dialogue with a view to ensuring the effective operation of the highly successful Apostille Convention in an electronic environment. The authors intend this Memorandum to extend and encourage that dialogue, but we also wish to emphasise that electronic documents and electronic signatures are with us now and only show signs of becoming increasingly commonplace – if not *de facto* standards for transactions. We firmly believe Competent Authorities under the e-APP can benefit by a) operating e-Registers, b) exchanging e-Apostilles, and c) sharing their experiences and knowledge with each other. We have come to determine that the public service that Competent Authorities provide by issuing Apostilles can only be strengthened under the e-APP.

37. This Memorandum has been prepared in response to some of the questions and comments received since the launch of the e-APP in April 2006. We would like to thank all those who participated in this exchange of ideas for their helpful contributions. They have helped us to realise that the processes and ideas clarified in this Memorandum should be shared with other Competent Authorities considering implementation of the e-APP and indeed with a wider audience. To that end, these processes and ideas will be reflected in the educational material relating to the e-APP.

38. At the end of the day, the e-APP is intended to extend the reach of the Apostille Convention into the electronic medium, where new questions undoubtedly will arise. However, we are convinced that we can address those questions well while still honouring the purpose of the Convention and making its operation more effective and secure.

39. We believe that these enhanced security features and standardised processes will not only improve the operation of the Convention, but will also provide more confidence among recipients of foreign Apostilles to accept and act upon them.