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. Dans le cadre du programme pilote d'Apostilles électroniques (*e-APP*), la HCCH et la NNA, en collaboration avec les États intéressés (ou leurs juridictions internes), développent, facilitent la mise en œuvre et font la promotion de modèles de logiciels peu onéreux, opérationnels et sécurisés pour (i) l'émission et l'utilisation d'Apostilles électroniques (e-Apostilles) et (ii) l'exploitation de registres électroniques d'Apostilles (e-Registres). L'*e-APP* a été officiellement lancé lors de la Commission spéciale sur les affaires générales et la politique d'avril 2006. Ce programme est conçu pour illustrer la manière dont les Conclusions et Recommandations de la Commission spéciale de 2003 sur le fonctionnement pratique de la Convention Apostille et du Forum international sur la notarisation et l'Apostille électroniques de 2005 peuvent être mises en œuvre en pratique grâce à l'utilisation de technologies déjà existantes et largement utilisées[1]. Il convient de souligner que l'*e-APP* offre et promeut l'adoption de modèles de logiciels pouvant être librement configurés par les États participants. Les États sont également encouragés à développer leurs propres logiciels et à travailler en collaboration avec d'autres dans le cadre de l'*e-APP*. Bien que les États n'aient pas d'obligation, en vertu de l'*e-APP*, de partager leurs systèmes ou modèles dans un environnement à code source libre, il est souhaité que les États participants utiliseront l'*e-APP* pour s'informer mutuellement de leurs travaux, vision et, dans la mesure nécessaire, de leurs environnements juridiques respectifs[2].

2. L'objet du présent mémoire est d'offrir des informations et explications supplémentaires sur les aspects techniques du modèle proposé pour l'émission d'e-Apostilles, et plus particulièrement sur (I) l'utilisation des signatures numériques, (II) le format d'une e-Apostille et (III) l'utilisation et le statut de la version imprimée d'une e-Apostille. L'objectif de l'*e-APP* est de faciliter les communications et la coopération entre les États participants. Le présent mémoire, produit dans ce même esprit, participe au dialogue continu entre les États participant au programme *e-APP* et rassemble des informations sur les réflexions, questions et suggestions perspicaces des États participants, observateurs intéressés et éventuels participants au programme *e-APP*.

3. La participation au programme *e-APP* ne requiert ni accord formel entre États, ni engagement contraignant envers le programme pilote. En prenant part à l'*e-APP*, les États sont encouragés à partager leurs idées, exemples et ressources dans la mesure du possible afin de faciliter une large adoption des Apostilles et Registres électroniques.

---

[1] L'*e-APP* a fait une percée en février 2007, lorsque l'état du Kansas a émis le premier prototype d'e-Apostille dans le cadre de l'*e-APP*. La Colombie, État destinataire, a officiellement indiqué accepter l'e-Apostille. Ces deux juridictions sont donc prêtes à authentifier les actes publics de manière entièrement électronique. En outre, l'état du Rhode Island s'est joint à l'*e-APP* en adoptant et mettant en œuvre le logiciel ouvert et gratuit de registre électronique du Programme. Toute personne intéressée peut désormais rechercher, en ligne et en toute sécurité, une Apostille émise par les autorités du Rhode Island (encore sur support papier, mais prochainement sous forme électronique), en saisissant son numéro et sa date. Le Registre fera automatiquement apparaître toute entrée correspondante, permettant ainsi aux destinataires de vérifier l'origine de l'Apostille bien plus facilement et efficacement qu'actuellement.

[2] Dans ce contexte, il est peut-être nécessaire de rappeler les termes des Conclusions du deuxième Forum international sur la notarisation et l'Apostille électroniques de Washington (mai 2006) qui disposent au para. 7 que : « Les participants ont également noté que les lois, règles ou toutes autres réglementations internes existantes relatives à l'exécution des actes notariés électroniques, à l'utilisation et la gestion des signatures électroniques ou à la transmission de documents électroniques (dont les actes notariés) continuent de s'appliquer dans le cadre des modèles proposés pour les besoins de l'*e-APP* [...] ». Le premier forum international sur la notarisation et l'Apostille électroniques, réuni à Las Vegas en mai 2005, avait déjà reconnu que « [l]a plupart des États ont désormais légiféré afin de reconnaître l'effet juridique des signatures et documents électroniques ». Le forum a encouragé les États « à poursuivre l'examen et l'amélioration de l'encadrement juridique en vue de l'utilisation des signatures et documents électroniques ». Les Conclusions des deux forums sont disponibles sur le site de la Conférence de La Haye à l'adresse < www.hcch.net > sous la rubrique « Espace Apostille ».

I. Signatures électroniques : une question de confiance

A. Vérification des signatures numériques sous Adobe

4. Le modèle proposé pour l'émission d'e-Apostilles utilise une technique prête à l'emploi, la technologie PDF (voir également ci-dessous, partie II). En outre, en application de ce modèle, les Autorités compétentes utilisent des certificats numériques pour signer numériquement l'e-Apostille qu'elles émettent. Dans ce contexte, il est important de souligner que lorsqu'un document Adobe PDF est signé numériquement, Adobe, délibérément, ne « fait pas confiance » au certificat numérique. Adobe a conçu ainsi ses logiciels PDF afin de créer un contrepoids de sécurité, pour ainsi dire. Cette politique crée un contraste fort (et une critique à peine voilée) avec l'approche adoptée jusqu'alors par le système d'exploitation Windows de Microsoft (voir cependant les commentaires ci-dessous au para. 11). Le système d'exploitation Windows (Windows 2000 et versions suivantes) se fie de manière automatique aux certificats numériques émanant d'un certain nombre de prestataires. La plupart des utilisateurs finaux ne sont pas conscients de cette situation, qui a été critiquée par certains experts de la sécurité comme constituant une faille potentielle dans la sécurité. Si on reçoit un document Word revêtu d'une signature électronique, par exemple, provenant d'une autorité de certification dont Microsoft a déjà décidé qu'elle lui faisait confiance, on ne recevra aucune alerte quant à la possibilité ou au besoin d'examiner le certificat avant de l'approuver. Adobe, par contre, exige de l'utilisateur final l'ajout délibéré du certificat à sa liste d'identités de confiance afin d'assurer que le destinataire a la faculté de déterminer à qui se fier ou ne pas se fier.

5. Le processus de sécurité établi par Adobe est conçu de telle sorte que le destinataire du document peut vérifier de manière indépendante l'habilitation et l'identité de l'envoyeur du document. Le destinataire peut le faire en contactant (par exemple, par téléphone) soit l'envoyeur directement soit sa société ou son organisme et en contrôlant la qualité et l'identité de l'envoyeur (dans le second exemple, la société ou l'organisme se porterait garant de l'envoyeur effectif). Une autre possibilité consiste pour le destinataire à contacter l'autorité de certification (par exemple, accéder en ligne à son registre de clés publiques) et vérifier l'origine du certificat. Une fois qu'il est satisfait du processus de vérification, le destinataire suit alors les étapes décrites ci-dessous pour reconnaître et approuver le certificat numérique dans le document signé par cet envoyeur. Il est nécessaire de suivre le processus de reconnaissance et d'approbation du certificat numérique une seule fois, car tout document futur signé du certificat de cet envoyeur sera automatiquement reconnu et approuvé par le logiciel Adobe du destinataire. Le destinataire pourra également choisir de ne pas s'assurer de l'habilitation et de l'identité du certificat numérique de l'envoyeur, et décider au contraire de suivre immédiatement les étapes ci-dessous afin d'approuver le certificat numérique de l'envoyeur pour le premier document et les suivants.

6. Afin de configurer Adobe 7.0 Reader/Standard/Professional en vue d'approuver l'autorité émettrice du certificat numérique du Kansas, appliquer les étapes suivantes :

1. Cliquer sur la signature numérique que vous souhaitez approuver.
2. Cliquer sur le bouton Propriétés de la signature dans la boîte de dialogue État de validation de la signature.
3. Cliquer sur le bouton Afficher certificat dans l'onglet Résumé de la boîte de dialogue Propriétés de la Signature.
4. Cliquer sur l'onglet Approuver l'identité.
5. Cliquer sur le bouton Ajouter aux identités approuvées.
6. Cliquer sur OK.
7. Dans la boîte de dialogue Importer les options de contact, cocher les cases appropriées des Options d'approbation pour approuver le certificat numérique.
8. Nous recommandons à l'utilisateur de ne cocher que la première case correspondant à « Signatures et certificat racine approuvé ».

7. Il est très important de relever que le processus de vérification du certificat numérique d'un expéditeur particulier (une Autorité compétente par exemple) peut être renversé. En d'autres termes, un destinataire peut décider de *ne pas* faire confiance au certificat numérique de l'expéditeur. Il convient de suivre les étapes suivantes pour configurer Adobe 7.0 Reader/Standard/Professional afin de récuser une autorité de certification numérique :

1. Cliquer sur la signature numérique que vous souhaitez récuser
2. Cliquer sur le bouton Propriétés de la signature dans la boîte de dialogue État de validation de la signature.
3. Cliquer sur le bouton Afficher certificat dans l'onglet Résumé de la boîte de dialogue Propriétés de la Signature.
4. Cliquer sur l'onglet Approuver l'identité.
5. Cliquer sur le bouton Ajouter aux identités approuvées.
6. Cliquer sur OK.
7. Dans la boîte de dialogue Importer les options de contact, désélectionner les cases appropriées des Options d'approbation pour récuser le certificat numérique.
8. Exemple : si la première case pour « Signature et certificat racine approuvé » est cochée, simplement désélectionner cette case.

8. Pour plus de renseignements concernant l'approbation des signatures numériques sous Adobe, veuillez consulter les fichiers d'aide Adobe correspondant à l'entrée intitulée « Détermination du niveau de confiance d'un certificat » ou simplement « certificats numériques ».

9. Outre les processus décrits ci-dessus, les destinataires d'une e-Apostille émise en application du modèle proposé peuvent utiliser tout autre moyen de vérification. Au Kansas par exemple (voir la note de bas de page 1), l'autorité de certification racine tient une liste de révocations de certificats (CRL) à laquelle on peut accéder au moyen d'un navigateur Internet standard en allant à l'adresse internet (URI) de la CRL. Une deuxième méthode de vérification d'un certificat du Kansas – au demeurant plus simple – consiste à se connecter au site Web suivant : < https://digitalid.verisign.com/services/client/index.html >. Sur ce site web, tout destinataire d'un document comportant une signature numérique en provenance d'un représentant de l'état du Kansas peut saisir l'adresse de courrier électronique du titulaire du certificat afin de vérifier a) le statut actuel du certificat numérique en cause (s'il est en cours et valable, révoqué, périmé, etc.) et b) le numéro d'ordre du certificat numérique. Les deux méthodes de vérification indiquées ci-dessus sont disponibles gratuitement et fournissent un moyen simple de déterminer la validité actuelle d'un certificat numérique.

10. Bien que nous soyons conscients que le format PDF n'est pas complètement un logiciel à code source libre, il sera rappelé que l'utilisation du format PDF comme modèle pour les e-Apostilles est simplement suggérée. En d'autres termes, et ainsi que relevé précédemment, les autorités compétentes sont encouragées à développer d'autres modèles et à partager ces développements avec les participants du programme *e-APP*. Les Autorités compétentes peuvent choisir d'offrir ces modèles pour que les autres autorités compétentes puissent les utiliser dans le cadre de l'*e-APP* (du moins tant que ces modèles sont sous licence libre). Même si les modèles ne sont pas offerts aux autres Autorités compétentes pour utilisation, les informations portant sur ces modèles pourraient être accessibles gratuitement à la communauté de l'*e-APP*.

11. Des développements intéressants chez Microsoft méritent d'êtres soulignés. La future version de Microsoft Office 2007 comportera un support intégré pour les signatures numériques sous une forme quasiment identique à celle d'Adobe. On peut donc supposer qu'une Autorité compétente pourrait signer numériquement une e-Apostille sous Microsoft Word 2007 avec la même sûreté et les mêmes assurances que celles qui résultent actuellement du PDF d'Adobe. Nous pensons que cette évolution est le signe d'une importante tendance à l'appui de la technologie recommandée dans le cadre de l'*e-APP*. Le fait que Microsoft soutienne la technologie recommandée dans le

cadre de l'*e-APP* (même sans le faire intentionnellement) traduit une évolution favorable qui permettra très bientôt à toute Autorité compétente disposant d'un exemplaire de Microsoft Word 2007 d'émettre des e-Apostilles en toute sécurité, soutenant ainsi une utilisation et une distribution encore plus étendues des e-Apostilles. La nouvelle version de Microsoft Word 2007 intègre également une possibilité de conversion gratuite pour PDF. Pour résumer, l'Autorité compétente pourrait donc choisir de distribuer l'e-Apostille électroniquement en Word *ou* en PDF en cliquant simplement sur un bouton.

B. Rudiments des infrastructures à clés publiques (ICP)

12. Le modèle d'approbation de signature électronique Adobe PDF est fondé sur les directives fonctionnelles d'une infrastructure à clés publiques (ICP). Bien que le présent mémoire ne permette d'exposer que les principes de base d'une ICP[3], il est important de noter que l'ICP implique des acteurs clés, au nombre desquels une autorité de certification (CA) et une autorité d'enregistrement (AE). Une AC est une tierce partie indépendante à toute transaction qui intervient dans le cadre d'une ICP. L'AC délivre un certificat numérique, utilisé pour signer numériquement un document PDF. L'AC est une organisation contrôlée qui doit appliquer des procédures de fonctionnement strictes afin de conserver la confiance placée dans les certificats numériques qu'elle délivre. L'AE est une partie sous contrat avec l'AC chargée uniquement de prouver l'identité et établir les droits et devoirs d'une personne requérant un certificat numérique. Reprenant ici l'exemple du premier essai d'e-Apostille, l'état du Kansas a agi en qualité d'AE en délivrant un certificat numérique à un employé du *Secretary of State's office* du Kansas. La confiance en une ICP est fondée sur l'AC et l'AE agissant de manière responsable et se soumettant à une surveillance et des auditeurs indépendants. Cependant, cette confiance dépend également des parties, à savoir le signataire et le destinataire du document signé électroniquement. Ainsi qu'expliqué précédemment, si le destinataire du document pense que l'AC et l'AE sont des acteurs crédibles, il peut alors penser que le signataire du document est bien celui qu'il prétend être et qu'il agit dans le champ de son autorité. En d'autres termes, le destinataire du document possède une entière autorité pour se fier ou ne pas se fier aux transactions dans le cadre d'une ICP.

13. Outre le modèle d'approbation de l'ICP, des caractéristiques importantes sont ou peuvent être insérées dans une ICP donnée.

(1) L'une des caractéristiques sur laquelle les participants de l'ICP peuvent se reposer est l'instruction d'exercice de certification (CPS). Elle contient entre autres la description des rôles, responsabilités et conditions gouvernant la délivrance, l'utilisation et la gestion des certificats numériques pour une ICP donnée. Ainsi, une instruction d'exercice de certification pourrait, par exemple, déclarer que tous les certificats numériques délivrés en vertu de l'instruction font obligation au demandeur d'un certificat numérique d'être identifié en personne par une autorité d'enregistrement appropriée. Une instruction d'exercice de certification est écrite dans de nombreux cas, pour satisfaire aux exigences de l'*Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* de l'IETF (*Internet Engineering Task Force*). Dans le cadre de l'*e-APP*, l'état du Kansas (États-Unis d'Amérique) a délivré l'instruction d'exercice de certification suivante, qui gouverne sa gestion des certificats numériques.

(2) Une entité gouvernementale ou privée peut également être soumise à des lois, règles et réglementations locaux gouvernant la délivrance et l'utilisation des certificats numériques. En ce qui concerne par exemple la première Apostille électronique d'essai, délivrée par l'autorité compétente du Kansas, la réglementation locale régit la délivrance et la gestion des certificats numériques par l'autorité de certification racine de l'état du Kansas. Une caractéristique importante de cette réglementation est que tout demandeur

[3] Les lecteurs souhaitant plus d'explications sur l'ICP peuvent consulter < http://fr.wikipedia.org/wiki/Infrastructure_à_clés_publiques > (au 19 mars 2007). Il existe d'abondantes sources généralistes et spécialisées et Wikipedia fournit une excellente introduction en la matière.

d'un certificat numérique a l'obligation, de par la loi, de se présenter en personne devant un fonctionnaire autorisé et de présenter à une autorité locale d'enregistrement au moins un document d'identité délivré par une autorité gouvernementale et comportant une photographie, pour demander et recevoir un certificat numérique de l'autorité de certification du Kansas. Le Kansas autorise actuellement les *Chief Election Officers* à agir comme autorités locales d'enregistrement.

(3) Une autorité de certification peut autoriser un outil connu sous le nom de *Online Certificate Status Protocol* (OCSP) afin de permettre un contrôle plus rapide et plus fiable du statut du certificat numérique. L'OCSP permet une vérification plus rapide et plus fiable du statut de révocation d'un certificat numérique délivré par une autorité de certification donnée. Ainsi, l'OCSP, bien que non obligatoire dans le cadre d'une ICP, peut être plus efficace et rapide pour vérifier si un certificat numérique donné a été révoqué ou est toujours valable. Bien que l'autorité de certification de l'état du Kansas n'offre pas encore d'OCSP, elle pourrait le faire dans l'avenir.

14. À notre avis, le processus de signature électronique sécurisé intégré dans la technologie Adobe et décrit ci-dessus est conforme à la Loi type de la CNUDCI sur les signatures électroniques de 2001 (voir notamment les art. 6, 7 et 12(3)) pour autant, bien entendu, que la conduite du signataire et du prestataire de service de certification remplisse les conditions figurant aux articles 8 et 9 de la Loi type. L'article 2(a) de la Loi type définit une signature électronique comme étant « des données sous forme électronique contenues dans un message de données ou jointes ou logiquement associées audit message [en l'occurrence, l'Apostille], pouvant être utilisées pour identifier le signataire dans le cadre du message de données et indiquer qu'il approuve l'information qui y est contenue ». Et l'exigence de fiabilité d'une signature électronique, selon l'article 6 de la Loi type de la CNUDCI, « est satisfaite dans le cas d'un message de données s'il est fait usage d'une signature électronique dont la fiabilité est suffisante au regard de l'objet pour lequel le message de données a été créé ou communiqué, compte tenu de toutes les circonstances, y compris toute convention en la matière ». Le processus sécurisé de signature électronique Adobe décrit ci-dessus se conforme bien à cette définition d'une signature électronique[4].

15. En outre, la norme appliquée par l'article 12(3) de la Loi type de la CNUDCI pour la reconnaissance des signatures électroniques créées dans un autre État apporte un autre cadre autorisé pour la reconnaissance entre États parties à la Convention des e-Apostilles émises conformément au modèle suggéré dans l'*e-APP*[5]. Là encore, nous sommes d'avis que le modèle suggéré dans le cadre de l'*e-APP* offre un très haut niveau de fiabilité et qu'ainsi les e-Apostilles émises selon ce modèle devraient être reconnues entre les États parties. Cet argument est encore appuyé par le principe général en vertu de la Convention selon lequel une Apostille régulièrement produite dans un État partie à la Convention doit être reconnue par tout autre État partie à la Convention[6]. Enfin, et c'est peut-être le plus important, il peut être utile de rappeler que des milliers (sinon des millions) d'Apostilles sont émises tout les ans au moyen de griffes ou de copies numérisées de signatures manuscrites; bien que ces techniques de signature offrent un niveau de sécurité nettement inférieur à celui du modèle suggéré dans le cadre de

[4] Voir également les définitions des termes « message de données » et « signataire » aux art. 2(c) et 2(d) respectivement de la Loi type de la CNUDCI sur les signatures électroniques. Art. 2(c) : « Le terme « message de données » désigne l'information créée, envoyée, reçue ou conservée par des moyens électroniques ou optiques ou des moyens analogues, notamment, mais non exclusivement, l'échange de données informatisées (EDI), la messagerie électronique, le télégraphe, le télex et la télécopie » ; art. 2(d) : « Le terme « signataire » désigne une personne qui détient des données afférentes à la création de signature et qui agit soit pour son propre compte, soit pour celui de la personne qu'elle représente ».

[5] L'art. 12(3) est rédigé ainsi : « Une signature électronique créée ou utilisée en dehors de [*l'État adoptant*] a les mêmes effets juridiques dans [*l'État adoptant*] qu'une signature électronique créée ou utilisée dans [*l'État adoptant*] à condition qu'elle offre un niveau de fiabilité substantiellement équivalent. »

[6] C'est sur la base de ce principe que le Bureau Permanent a fait valoir de manière constante que les Apostilles étrangères ne peuvent être rejetées par un État de réception au seul motif qu'elle ne sont pas conformes au mode d'émission des Apostilles dans l'État de réception (par exemple, revêtues de rubans colorés, de cachets de cire, et de rubans). Voir Conclusion et Recommandation No 13 de la réunion de la Commission spéciale de 2003.

l'*e-APP*, elles n'ont - à notre connaissance - jamais entraîné de problèmes graves de reconnaissance d'Apostilles étrangères.

C. Viabilité à long terme des documents PDF

16. Des questions sont posées sur la viabilité à long terme d'un produit commercial comme Adobe PDF, et plus particulièrement sur la manière dont l'*e-APP* pourrait permettre la lecture gratuite en 2030 ou au-delà d'un document PDF signé numériquement en 2007. Bien que l'objet du présent mémoire ne permette pas de débattre le thème de l'archivage électronique à long terme des documents, cette question fait l'objet d'études importantes et actives[7]. Les spécifications du format PDF existantes sont partiellement ouvertes et permettent à tout un chacun, gratuitement, de développer des logiciels lisant et écrivant conformément aux spécifications du format. Adobe a récemment annoncé, très significativement, qu'il communiquait l'intégralité de sa spécification PDF à un organisme international indépendant et ouvert pour utilisation publique[8]. En bref, cela permettra aux concepteurs de logiciels d'accéder et de visionner des documents PDF en utilisant ce standard ouvert pour l'avenir, sans avoir besoin d'acquérir une licence Adobe.

II. Le format d'une e-Apostille : soit un fichier PDF continu unique, soit un fichier PDF avec une pièce jointe

17. Dans le cadre de l'*e-APP*, nous avons envisagé deux formats distincts mais identiques en définitive pour les e-Apostilles. Les deux méthodes protègent le document sous-jacent et le certificat d'e-Apostille contre les modifications sans autorisation, mais chacune présente une interface différente au destinataire.

18. En vertu de la première méthode, une Autorité compétente peut ajouter le certificat d'Apostille en dernière page d'un acte public sous-jacent existant en PDF. Selon cette méthode, le destinataire ouvrira donc le document PDF et trouvera le certificat d'e-Apostille intégré en dernière page du même document PDF. Si ce format est choisi, le document public sous-jacent et le certificat d'e-Apostille constituent un document unique en continu, ou en d'autres termes, un fichier PDF unique. On pourrait toujours décider d'imprimer une ou plusieurs pages de ce fichier unique, de sorte que le certificat d'e-Apostille pourrait être imprimé seul (voir le point III ci-dessous pour plus de renseignements à cet égard).

19. En vertu de la seconde méthode, le document public sous-jacent est joint au certificat d'e-Apostille à titre de fichier distinct. C'est la méthode choisie par le Kansas pour son e-Apostille d'essai. Le destinataire reçoit là encore un fichier PDF unique, mais à l'ouverture du fichier, le destinataire visionne d'abord le certificat d'e-Apostille, et peut alors ouvrir le document public sous-jacent joint afin de le visionner à titre de fichier PDF distinct. À notre avis, cette méthode présente une interface plus intuitive au destinataire du document revêtu de l'Apostille (on peut remarquer que c'est celle qu'a adopté le Département d'État des États-Unis pour ses dépôts de brevet électroniques et son modèle d'e-Apostille). En joignant l'acte public sous-jacent à titre de fichier au certificat d'e-Apostille, le but consiste à expliciter pour le destinataire lors de sa première ouverture du document qu'il s'agit d'une Apostille. À partir de là, il peut ensuite ouvrir l'acte public sous-jacent afin de visionner son contenu.

20. Dans le cadre de l'*e-APP*, une Autorité compétente peut choisir l'un ou l'autre modèle, et l'*e-APP* ne prétend pas que l'un ou l'autre est préférable.

---

[7] Les lecteurs suffisamment intéressés pour aller plus loin sur ce sujet pourront consulter les travaux du groupe de travail de l'IETF (*Internet Engineering Task Force*, grande communauté de concepteurs de réseaux, opérateurs, vendeurs et chercheurs s'intéressant à l'évolution de l'architecture et du bon fonctionnement d'Internet. Ce groupe est ouvert à toute personne intéressée), du LTANS (*Long-Term Archive and Notary Services*). Ce groupe de travail développe actuellement un *Evidence Record Syntax* pour l'archivage à long terme et l'extraction des documents signés numériquement pour des périodes longues et éventuellement indéterminées. Voir < http://www.ietf.org/html.charters/ltans-charter.html > (au 19 mars 2007) pour plus d'informations.

[8] Voir le communiqué de presse d'Adobe à l'adresse
< http://www.adobe.com/fr/aboutadobe/pressroom/pr/jan2007/adobe_pdf_iso.pdf > (au 19 mars 2007).

III. Impression de l'e-Apostille

21. L'impression du certificat d'e-Apostille (avec ou sans le document public sous-jacent) soulève au moins deux questions qu'il faut traiter séparément : (A) Comment empêcher une réutilisation frauduleuse du certificat d'e-Apostille sur le support imprimé ? (B) Comment assurer que l'impression d'un certificat d'e-Apostille remplira les exigences d'archivage et des règles d'administration de la preuve sur papier uniquement ?

A. Comment empêcher une réutilisation frauduleuse du certificat d'e-Apostille

22. La question de la prévention de la réutilisation de la version imprimée d'un certificat d'e-Apostille est difficile à résoudre à l'ère des logiciels d'édition d'images numériques. Même si nous devions utiliser la première méthode décrite ci-dessus de manière exclusive, on pourrait décider de n'imprimer que le certificat d'e-Apostille à titre de page distincte, et nous resterions confrontés au problème d'une réutilisation frauduleuse de ce certificat d'e-Apostille pour d'autres documents. On pourrait même simplement capturer une « impression d'écran » du certificat d'Apostille (tapez « Apostille » sous Google Image Search...) ou passer 30 minutes sous Microsoft Word pour créer un faux certificat d'Apostille d'apparence parfaitement valable qui pourrait alors facilement être imprimé dans un but frauduleux. Là encore, nous suggérons que l'*e-APP* soit évalué par rapport aux niveaux de sûreté et anti-fraude actuellement atteints dans l'environnement papier seul. En gardant à l'esprit non seulement l'e-Apostille de l'*e-APP* mais également sa composante d'e-Registre, nous sommes assez convaincus de ce que l'*e-APP* dépasse de loin les niveaux actuels de protection anti-fraude et de sûreté.

23. Un autre défi tient au fait qu'il n'est pas possible (et pour des motifs évidents, pas souhaitable) de construire un système centralisé de gestion des e-Apostilles, du moins, pas pour le moment. S'il est vrai qu'un tel système centralisé permettrait d'intégrer de manière économique des solutions de sécurité dans le système dont toute Autorité compétente pourrait tirer parti, le cadre de l'*e-APP* n'offre ni la possibilité de créer un système centralisé (qui nécessiterait une nouvelle Convention), ni la capacité d'imposer à une Autorité compétente une quelconque exigence concernant le matériel ou les logiciels (car la Convention est techniquement neutre).

24. Cela étant, la réutilisation frauduleuse d'une Apostille papier ou électronique est un problème qui doit être traité. Il existe trois solutions principales à cet égard : (a) l'e-Registre ; (b) l'ajout de la date et de l'heure exactes de la signature du document public sous-jacent aux renseignements fournis en vertu de l'élément normalisé 2 du certificat d'Apostille ; et (c) l'utilisation de codes à barres.

25. (a) Il ne fait guère de doute pour nous que le meilleur moyen de dissuader l'utilisation frauduleuse de toute Apostille (qu'il s'agisse d'une Apostille électronique ou sur papier) consiste à encourager autant que possible l'utilisation du Registre que toute Autorité compétente doit tenir en vertu de l'article 7 de la Convention. L'*e-APP* démultiplie de manière spectaculaire les avantages et bénéfices de ces Registres en les rendant accessibles en ligne. (Nous suggérons que même si une Autorité compétente ne décidait jamais d'émettre un certificat d'e-Apostille, la tenue d'un registre électronique est une mesure que chaque Autorité compétente devrait avoir déjà prise). Supposons par exemple que chaque Autorité compétente tienne un Registre d'Apostilles électronique en ligne facilitant une vérification immédiate et fiable de toute Apostille émise par une Autorité compétente. Nous ferions un grand pas dans la lutte contre la fraude avec une telle solution simple et globale, car chaque certificat d'Apostille pourrait être comparé avec un e-Registre accessible par Internet. Le défi, bien entendu, est que chaque Autorité compétente joue le jeu en acceptant d'héberger un e-Registre. Nous sommes loin de la réalisation de ce scénario idéal, mais l'*e-APP*, en proposant un e-Registre gratuit en logiciel ouvert, va assez loin dans l'atteinte de cet objectif. En outre, la facilité d'accès à l'e-Registre fournira l'outil de vérification le plus important qui soit disponible aux fins d'archivage et de preuve.

26. (b) Une autre méthode pour relier la version imprimée d'un certificat d'e-Apostille au document public sous-jacent consiste à ajouter la date et l'heure exactes de la signature du document public sous-jacent aux renseignements fournis en vertu de

l'élément normalisé 2 du certificat d'Apostille. Ainsi l'élément 2 d'un certificat d'Apostille comprendrait, par exemple, les renseignements suivants : « X, le 12/01/2007 13:46:17 - 06'00 ». Il va sans dire que ces renseignements supplémentaires ne sauraient être imposés à titre de condition générale pour les certificats d'Apostille sur papier; en outre, comme ce processus impose une légère modification du modèle de certificat d'Apostille joint en annexe à la Convention, nous ne souhaitons pas l'imposer pour les e-Apostilles en vertu de l'*e-APP* mais nous sommes confiants dans la recommandation de cet ajout auprès des Autorités Compétentes parce qu'il améliore les éléments de sûreté d'une e-Apostille.

27. (c) Une autre méthode que nous recommandons pour permettre l'impression tout en contrant la fraude consiste en l'utilisation de codes à barres. En intégrant dans le certificat d'e-Apostille un code à barres Adobe « formulaires papier » qui comporte des données particulières à la fois au certificat d'e-Apostille et au document public sous-jacent, quiconque (disposant d'un dispositif de lecture, voir ci-dessous) se verrait soumettre une version imprimée du certificat d'e-Apostille et le document public (sous-jacent) pourrait lire le code à barres afin de vérifier si ces documents imprimés correspondent effectivement.

28. Un code à barres « formulaires papier » est défini de la manière suivante dans les fichiers d'aide *d'Adobe Designer* 7.0 : « un code à barres capture électroniquement des données fournies par l'utilisateur dans un formulaire PDF interactif. Lorsque l'utilisateur final remplit le formulaire en utilisant Adobe Reader ou Acrobat, le code à barres est automatiquement mis à jour pour coder les données fournies par l'utilisateur. L'utilisateur peut alors renvoyer le formulaire complété en l'imprimant et en le faxant, postant ou le remettant en mains propres. Après réception, les données de l'utilisateur peuvent être décodées en utilisant un scanner [traduction libre du Bureau Permanent]. Selon cette définition, « l'utilisateur final » serait un représentant de l'administration chargé de remplir les certificats d'Apostille en qualité d'Autorité compétente ou pour le compte de celle-ci. Sous la forme envisagée par l'*e-APP*, un code à barres formulaires papier Adobe, dit également code à barres « dynamique » (par opposition à statique), permettrait à l'Autorité compétente d'intégrer au code à barres des renseignements qui pourraient comprendre tous les renseignements figurant dans les 10 éléments normalisés d'un certificat d'Apostille, ainsi que les renseignements figurant dans le certificat numérique (tels que le nom du signataire, son adresse de courrier électronique, etc.). À la réception d'un certificat d'e-Apostille comportant un tel code à barres, le destinataire pourrait lire le code à barres afin de révéler les valeurs qu'il contient; le destinataire d'une e-Apostille imprimée pourrait donc comparer les valeurs figurant dans le code à barres avec les renseignements figurant sur le certificat d'e-Apostille imprimé ou les renseignements figurant dans l'e-Registre en vue de vérifier que les valeurs du code à barres correspondent aux valeurs du certificat d'e-Apostille imprimé ou de l'e-Registre. Comme les codes à barres sont très difficiles à falsifier, le destinataire bénéficierait d'un haut niveau d'assurance de ce que le document n'a pas été altéré. Les codes à barres offrent donc la plus grande valeur lorsqu'un certificat d'e-Apostille est imprimé. En outre, si l'original électronique est perdu, le code à barres peut continuer de fournir une vérification fiable pour l'avenir prévisible. De la manière indiquée ici, des données importantes fournies par l'utilisateur peuvent ainsi être intégrées au code à barres aux fins d'un contrôle de sûreté.

29. Bien entendu, cette solution suppose que (a) les Autorités compétentes disposent des logiciels nécessaires pour produire des codes à barres et (b) les destinataires disposent de la technologie nécessaire pour lire et traiter les codes à barres, ce qui représente une difficulté pratique, mais qui peut être surmontée sans trop d'obstacles. L'achat d'*Adobe Standard* ou *Professional* est accompagné du logiciel « *Adobe Designer* » qui permet aux Autorités compétentes d'inclure des codes à barres dans un formulaire PDF, tel qu'un certificat d' e - Apostille, sans autres frais et avec des efforts minimes. En outre, le faible coût des lecteurs optiques de codes à barres et leur large utilisation sur le marché signifie que l'achat d'un tel lecteur ne devrait pas représenter un obstacle excessif pour nombre d'Autorités compétentes. Comme au point qui précède, nous sommes d'avis que nous ne devrions pas exiger mais seulement suggérer ou recommander l'utilisation des codes à barres.

30. Quelques remarques sur les *filigranes*. Nous ne pensons pas que l'intégralité du certificat d'Apostille devrait figurer en filigrane au document public sous-jacent. Une telle démarche représenterait une divergence importante par rapport au format du certificat d'Apostille, et ne serait donc pas conforme au modèle d'Apostille joint en annexe à la Convention. En outre, un filigrane d'aussi grande taille rendrait difficile la lecture du document sous-jacent. Il soulève également des problèmes pratiques pour les documents de plusieurs pages. Toutefois, nous souhaitons bien explorer l'utilisation d'un petit filigrane à titre de mesure de sûreté récurrente apparaissant à un emplacement discret sur chaque page du document public sous-jacent (tel que la répétition du numéro du certificat d'e-Apostille dans un coin de chaque page du document sous-jacent).

B. Comment assurer que l'impression observera les exigences d'archivage et d'administration de la preuve sur papier

31. Nous sommes fermement convaincus de ce que la possibilité d'imprimer une e-Apostille (le certificat et le document sous-jacent) d'une manière permettant de se fier à la version imprimée aux fins d'archivage et d'administration de la preuve constitue un objectif important. En d'autres termes, la question est peut-être : comment imprimer une e-Apostille et vérifier qu'elle n'a pas été modifiée par rapport à son état initial électronique ? Cette question bien entendu tient à la celle de la transformation à l'ère numérique. Les recommandations sous la partie A profiteront également aux exigences d'archivage et de preuve sur papier uniquement car l'utilisation de l'e-Registre, les renseignements supplémentaires en vertu de l'élément 2 du certificat d'e-Apostille et le code à barres permettront la vérification de la source et donc de l'authenticité d'une e-Apostille imprimée.

32. L'objet de ce mémoire n'est pas de déterminer si une version imprimée d'une e-Apostille a le même statut juridique que l'original électronique. La question est susceptible de se poser uniquement si et lorsqu'un contentieux surviendra au sujet de la source d'une e-Apostille, auquel cas les versions sur papier et électronique de l'Apostille seront probablement présentées toutes deux au tribunal. Sur le fondement de la version électronique au moins — et certainement combinée avec le Registre et tout particulièrement s'il s'agit d'un e-Registre accessible en ligne comme suggéré par l'*e-APP* —, il sera alors possible de juger de l'origine de l'Apostille avec un très haut niveau de certitude. Bien entendu, nous supposons que la partie destinataire conserverait non seulement une version imprimée de l'Apostille mais également l'original électronique. Nous pensons en fait qu'il est bien plus probable que la partie destinataire ne conservera que l'original électronique.

33. De nombreux organismes administratifs stockent les documents officiels sous forme électronique et ne produisent de versions imprimées qu'à titre d'extrait certifié conforme (par exemple, les extraits de naissance aux États-Unis sont rarement stockés sous forme papier; les statuts de sociétés, à titre d'autre exemple, sont presque exclusivement électroniques dans nombre de pays). Pourquoi le raisonnement ou les exigences seraient-ils différents pour les (e-)Apostilles ? En outre, comme noté ci-dessus (voir para. 15), il est courant d'émettre des Apostilles sur papier qui comportent une signature au moyen d'une griffe ou d'une copie numérisée d'une signature manuscrite, et nous n'avons connaissance d'aucun problème concernant la reconnaissance de telles Apostilles. Une version imprimée d'un certificat d'e-Apostille émis conformément au modèle de l'*e-APP* offre des éléments de sûreté et anti-fraude dépassant largement cette pratique courante. Il serait donc surprenant de voir des destinataires, tribunaux et autres utilisateurs finaux contester la pertinence de ces éléments d'*e-APP* alors qu'en fait ils renforcent le caractère authentique d'un document sur papier.

34. Enfin, dans le cadre de l'*e-APP*, nous continuerons d'encourager les États à mettre en place une e-réglementation appropriée (voir Conclusion 2 du Premier Forum International sur la notarisation et l'Apostille électroniques), mais nous pensons qu'il ne sera pas nécessaire d'attendre que cela se produise partout. L'*e-APP* peut en fait être considéré comme un catalyseur, en tout état de cause, à la fois pour les États disposant déjà de lois d'application et pour ceux qui envisagent actuellement de telles lois.

IV. Autres modifications proposées

35. Outre les propositions examinées ci-dessus, les modifications suivantes seront apportées au modèle d'e-Apostille tel qu'initialement proposé dans le cadre de l'*e-APP* :

Le modèle de logiciel PDF original sera modifié afin d'assurer que les cadres de texte 2, 6 et 8 ne peuvent pas être modifiés. En conséquence, tous les cadres de texte doivent être également protégés contre la modification sans autorisation.

Il est également suggéré (mais non exigé) de saisir les données relatives à la qualité de la personne certifiant le document dans le cadre 7.

Conclusion

36. Ainsi qu'indiqué précédemment, l'objectif le plus important de l'*e-APP* est peut-être la communication et le dialogue en vue d'assurer le fonctionnement efficace de la fructueuse Convention Apostille dans un environnement électronique. Les auteurs du présent mémoire souhaitent encourager et élargir ce dialogue mais également souligner que les documents électroniques et les signatures numériques sont une réalité de plus en plus répandue, voire la règle pour les transactions. Les Autorités compétentes peuvent, grâce à l'*e-APP*, trouver des avantages à a) utiliser des registres électroniques, b) échanger des Apostilles électroniques, et c) partager leurs expériences et connaissances. Le service public fourni par les Autorités compétentes délivrant les Apostilles ne peut que se renforcer dans le cadre de l'*e-APP*.

37. Ce mémoire a été préparé pour répondre aux questions et observations reçues depuis le lancement de l'*e-APP* en avril 2006. Nous voudrions remercier tous ceux qui ont participé à cet échange d'idées pour leurs utiles contributions. Ils nous ont aidés à prendre conscience du fait que les processus et idées explicités dans cette Note devraient être partagés avec d'autres Autorités compétentes envisageant la mise en œuvre de l'*e-APP*, voire avec un public plus large. À cet effet, ces processus et idées seront traduits dans les matériels de formation actuellement en cours d'élaboration.

38. En fin de compte, l'*e-APP* a pour but d'étendre la portée de la Convention Apostille vers le support électronique, où de nouvelles questions se poseront sans aucun doute. Toutefois, nous sommes convaincus de ce que nous pourrons traiter ces questions tout en honorant l'objet de la Convention et en rendant son fonctionnement plus efficace et plus sûr.

39. Ces éléments de sécurité renforcés et processus normalisés, selon nous, ne pourront qu'améliorer le fonctionnement de la Convention, mais apporteront également une plus grande confiance parmi les destinataires d'Apostilles étrangères en vue de les accepter et de leur donner effet.