Doc. prel. No 18

Marzo de 2007

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

PROGRAMA PILOTO DE APOSTILLAS ELECTRÓNICAS (*e-APP*)

MEMORÁNDUM SOBRE CIERTOS ASPECTOS TÉCNICOS QUE PROVEEN LA BASE DEL MODELO SUGERIDO PARA LA EMISIÓN DE APOSTILLAS ELECTRÓNICAS (E-APOSTILLAS)

elaborado por
*Christophe Bernasconi (Oficina Permanente) y Rich Hansberger (*National Notary Association*)*

Documento preliminar No 18 de marzo de 2007
a la atención del Consejo de abril de 2007
de Asuntos Generales y Política de la Conferencia

Oficina Permanente
6, Scheveningseweg 2517 KT La Haya | Países Bajos
Tfno : +31 70 363 3303 | Fax : +31 70 360 4867
Correo : secretariat@hcch.net | dirección Internet : http://www.hcch.net

PROGRAMA PILOTO DE APOSTILLAS ELECTRÓNICAS (*e-APP*)

MEMORÁNDUM SOBRE CIERTOS ASPECTOS TÉCNICOS QUE PROVEEN LA BASE DEL MODELO SUGERIDO PARA LA EMISIÓN DE APOSTILLAS ELECTRÓNICAS (E-APOSTILLAS)

elaborado por
*Christophe Bernasconi (Oficina Permanente) y Rich Hansberger (*National Notary Association*)*

Introducción

1. En el marco del Programa Piloto de Apostillas Electrónicas (*e-APP*), la Conferencia de La Haya de Derecho Privado Internacional (HCCH) y la Asociación Nacional de Notarios (NNA) en colaboración con cualquier Estado interesado (o cualquiera de sus jurisdicciones internas), se encuentran desarrollando, promoviendo y asistiendo en la implementación de modelos de software de bajo costo, operativos y seguros para (i) la emisión y la utilización de Apostillas electrónicas (e-Apostillas), y (ii) la operación de Registros electrónicos de Apostillas (e-Registros). El *e-APP* fue oficialmente lanzado durante la Comisión Especial de Asuntos Generales y Política de la HCCH en abril de 2006. Este programa fue concebido para ilustrar cómo las Conclusiones y Recomendaciones de la Comisión Especial de 2003 sobre el Funcionamiento Práctico la Convención de La Haya sobre la Apostilla y el Foro Internacional de 2005 sobre la Notarización y las Apostillas Electrónicas puede implementarse en la práctica basándose en tecnología existente y ampliamente utilizada.[1] Debemos resaltar que el *e-APP* ofrece y promociona la adopción de modelos de software que son libremente configurables por parte de los Estados participantes. Adicionalmente, los Estados son bienvenidos a desarrollar sus propias soluciones de software y a trabajar en colaboración con otros dentro del marco del *e-APP*. Si bien no se requiere que los Estados, en virtud del *e-APP*, compartan sus sistemas o modelos en un ambiente de código abierto, se espera que, al menos, los Estados participantes utilicen el *e-APP* para educarse unos a otros acerca de su trabajo, visiones, y en la medida necesaria, sus ambientes legales.[2]

2. El propósito de este Memorándum es ofrecer información adicional y explicaciones sobre los aspectos técnicos del modelo sugerido para la emisión de Apostillas Electrónicas, particularmente en el uso de firmas digitales (I), el formato de una Apostilla Electrónica (II), así como el uso y situación legal de una versión impresa de una Apostilla Electrónica (III). El objetivo del *e-APP* es facilitar la comunicación y la cooperación entre los Estados participantes, y este Memorándum está redactado en base a ese espíritu de continua colaboración. Este Memorándum es, entonces, parte de un diálogo continuo entre los Estados participantes en el *e-APP* y reúne numerosas preguntas, reflexiones y sugerencias perspicaces realizadas por los Estados participantes, los observadores interesados, y los potenciales participantes del *e-APP*.

3. La participación en el *e-APP* no requiere del acuerdo formal entre los Estados, ni requiere ningún tipo de compromiso vinculante con el Programa Piloto. Al participar en el *e-APP*, alentamos a los Estados a compartir ideas, ejemplos y recursos en la mayor medida posible para facilitar una adopción más amplia de Apostillas y Registros Electrónicos.

---

[1] El e-APP tuvo un gran avance en febrero de 2007 cuando el estado de Kansas emitió la primera e-Apostilla de prueba de acuerdo con el modelo sugerido según la e-APP, y Colombia, el Estado receptor, oficialmente indicó su aceptación de esta e-Apostilla de prueba. Como resultado, las dos jurisdicciones ahora están listas para completar las autenticaciones de documentos públicos de forma totalmente electrónica. Además, el estado de Rhode Island se incorporó al e-APP adoptando e implementando el software de Registro del Programa el cual es gratuito y de código abierto. Toda persona interesada puede realizar una búsqueda en línea segura para una Apostilla emitida por los funcionarios de Rhode Island (actualmente en papel, pronto también estará en formato electrónico) ingresando el número y la fecha y el registro mostrará de manera automática si se encuentra una entrada correspondiente, permitiendo así a las partes receptoras verificar el origen de la Apostilla de manera mucho más rápida y eficiente que la actual.

[2] En este contexto, puede resultar útil recordar el párrafo 7 de las Conclusiones del Segundo Foro Internacional sobre la Notarización y las Apostillas Electrónicas (realizado en Washington en mayo de 2006), que dice lo siguiente: “Asimismo, los participantes observaron que si existen leyes, reglas o reglamentos internos con respecto a la realización de actos notariales electrónicos, el uso y la administración de firmas electrónicas, o la transmisión de documentos electrónicos (incluyendo actos notariales), estas leyes, reglas o reglamentos siguen siendo aplicables bajo los modelos propuestos desarrollados para el e-APP.[...].” El Primer Foro Internaciónal sobre la Notarización y las Apostillas Electrónicas (realizado en Las Vegas en mayo de 2005) ha reconocido que “[a]ctualmente la mayoría de los países han emitido legislación que reconoce el efecto legal de las firmas electrónicas y los documentos electrónicos"; el Foro alentó a los Estados a que "continúen revisando y aumentando el marco legal a fin de permitir el uso de firmas electrónicas y documentos electrónicos” (párrafo 2 de las Conclusiones). Las Conclusiones en español tanto del primero como del segundo Foro se encuentran disponibles en la “Apostille Section” (sitio en inglés) y el “Espace Apostille” (sitio en francés) del sitio web de la Conferencia de La Haya < www.hcch.net >.

I. Firmas Digitales: Una cuestión de confianza

A. Verificación de firmas digitales en Adobe

4. El modelo sugerido para la emisión de Apostillas Electrónicas utiliza tecnología PDF estándar (véase también parte II). Además, según el modelo sugerido, las Autoridades Competentes utilizan certificados digitales para firmar digitalmente la Apostilla Electrónica que están emitiendo. En este contexto, es importante resaltar que Adobe está diseñado de tal manera que cuando una persona firma digitalmente un documento Adobe PDF, éste no "confía" en el certificado digital. Adobe diseñó su software de PDF de esta manera como control y contrapeso de seguridad, por decirlo de alguna manera. Esto contrasta fuertemente (y es una crítica poco disimulada) con el enfoque tomado hasta ahora por el sistema operativo Microsoft Windows (véase sin embargo, los comentarios más abajo en el párrafo 11). El sistema operativo Windows (Windows 2000 y versiones subsiguientes) automáticamente confía en los certificados digitales de un cierto número de proveedores. La mayoría de los usuarios finales no son concientes de esto, lo que ha sido criticado por algunos expertos en seguridad como una falla de seguridad potencial. Si uno recibe un documento de Word firmado digitalmente, por ejemplo, por una Autoridad de Certificación en quien Microsoft ya ha decidido confiar, uno no recibirá ninguna alerta sobre la posibilidad o necesidad de revisar el certificado antes de aceptarlo. Por el contrario, Adobe requiere que el usuario final deliberadamente agregue el certificado a su lista de identidades de confianza para garantizar que el destinatario tenga la capacidad de decidir en quién confiar y en quién no.

5. El proceso de seguridad que Adobe ha establecido está diseñado de tal manera que el destinatario del documento puede verificar independientemente la autoridad e identidad del remitente del documento. El destinatario puede hacerlo contactando (*p. ej. llamando*) al remitente de manera directa, o la compañía u organización del remitente y verificando el cargo e identidad del remitente (en el segundo ejemplo, la compañía u organización responderán por el remitente efectivo). Otra opción es que el destinatario contacte a la Autoridad de Certificación (*p. ej*. acceder a su registro de clave público en línea) y verifique el origen del certificado. Una vez que está satisfecho con el proceso de verificación, el destinatario sigue los pasos descritos en la parte inferior para reconocer y confiar en el certificado digital del documento firmado por dicho remitente. Este proceso de reconocimiento y confianza del certificado digital sólo se debe hacer una vez, ya que cualquier documento futuro firmado digitalmente con el certificado de ese remitente será reconocido y aceptado de manera automática por el software Adobe del destinatario. El destinatario también puede elegir no verificar la autoridad e identidad del certificado digital del remitente, y optar por seguir de inmediato los pasos descritos en la parte inferior para confiar en el certificado digital del remitente en el primero y subsiguientes documentos.

6. Para configurar Adobe 7.0 Reader/Standard/Professional para que confíe en una Autoridad de Certificación digital, deben seguirse los siguientes pasos:

1. Haga clic en la firma digital en la que se confía.
2. Haga clic en el botón de Propiedades de la Firma en el cuadro de diálogo Estado de Validación de la Firma.
3. Haga clic en el botón Mostrar Certificado en la solapa Resumen del cuadro de diálogo Propiedades de la Firma.
4. Haga clic en la solapa Confianza.
5. Haga clic en el botón Agregar Identidades de Confianza.
6. Haga clic en el botón Aceptar.
7. En el cuadro de diálogo Importar Configuración de Contactos, seleccionar las casillas apropiadas de Confianza para confiar en el certificado digital.
8. Recomendamos que el usuario seleccione sólo la primera casilla para "Firmas y como una raíz de confianza".

7. Es importante resaltar que este proceso de confiar en un certificado digital de un remitente en particular (tal como una Autoridad Competente) también puede ser revertido. En otras palabras, un destinatario puede decidir, *no* confiar en el certificado digital del remitente. Para configurar Adobe 7.0 Reader/Standard/Professional para "dejar de confiar" en una Autoridad de Certificación digital, deben seguirse los siguientes pasos:

1. Haga clic en la firma digital en la que se desea "dejar de confiar".
2. Haga clic en el botón de Propiedades de la Firma en el cuadro de diálogo Estado de Validación de la Firma.
3. Haga clic en el botón Mostrar Certificado en la solapa Resumen del cuadro de diálogo Propiedades de la Firma.
4. Haga clic en la solapa Confianza.
5. Haga clic en el botón Agregar Identidades de Confianza.
6. Haga clic en el botón Aceptar.
7. En el cuadro de diálogo Importar Configuración de Contactos, deseleccionar las casillas apropiadas de Confianza para "dejar de confiar" en el certificado digital.
8. Ejemplo: Si la primera casilla para "Firmas y como una raíz de confianza" se encuentra seleccionada simplemente deseleccione esa casilla.

8. Para recibir información adicional sobre la confianza de firmas digitales en Adobe, por favor busque en los archivos de Ayuda de Adobe la entrada denominada "Determinar el nivel de confianza de un certificado" o simplemente "Certificados digitales".

9. Además de los procesos anteriormente descritos, los destinatarios de una Apostilla electrónica emitida según el modelo sugerido podrán usar otros métodos de verificación. En Kansas, por ejemplo (véase los comentarios en la nota a pie de página 1) la Autoridad de Certificación de Raíz del Estado de Kansas mantiene una Lista de Revocación de Certificados (CRL, siglas en inglés) a la que se puede acceder en la ubicación en Internet (URI) del CRL mediante el uso de un navegador Web estándar. Un segundo, y más simple método de verificación de un Certificado de Kansas es posible simplemente accediendo a al siguiente sitio web < https://digitalid.verisign.com/services/client/index.html >. En este sitio Web, cualquier destinatario de un documento firmado digitalmente por un funcionario del gobierno del Estado de Kansas puede ingresar la dirección de correo electrónico del titular para verificar, a) el estado actual del certificado digital en cuestión (si está actualizado y vigente, revocado, vencido, etc.) y, b) el número de serie del certificado digital. Los dos métodos de verificación previamente descritos están disponibles sin costo y proporcionan una manera simple de determinar la validez actual de un certificado digital.

10. A pesar de que estamos concientes de que el formato PDF no es una tecnología verdaderamente de código abierto, nos gustaría reiterar que el uso de la tecnología PDF según el modelo para las Apostillas Electrónicas es un modelo *sugerido* únicamente. En otras palabras, como ya hemos hecho notar, alentamos a las Autoridades Competentes a desarrollar modelos alternativos para compartir estos desarrollos con la comunidad participante del *e-APP*. Las Autoridades Competentes podrán elegir ofrecer modelos alternativos para el uso por parte de otras Autoridades Competentes bajo el auspicio del *e-APP* (siempre que los modelos sean de licencia libre), pero incluso si los modelos no son ofrecidos para el uso de otras Autoridades Competentes, se espera que la información acerca de los modelos podrá estar disponible gratuitamente para la comunidad del *e-APP*.

11. Creemos que es interesante indicar ciertos avances que se han llevado a cabo por parte de Microsoft con respecto a su próxima versión de Microsoft Office 2007. Esta nueva versión incluirá un soporte incorporado para firmas digitales casi idéntico al de Adobe. Por lo tanto, se puede suponer que una Autoridad Competente podrá firmar digitalmente una Apostilla Electrónica en Microsoft Word 2007 con la misma seguridad y garantías que actualmente cuenta con Adobe PDF. Pensamos que este avance nos muestra una importante tendencia al apoyo de la tecnología recomendada por el *e-APP*.

El hecho de que Microsoft apoye la tecnología recomendada por el *e-APP* (aunque no sea intencional) refleja un desarrollo positivo que muy pronto permitirá a cualquier Autoridad Competente que cuente con una copia de Microsoft Word 2007 firmar Apostillas Electrónicas de manera segura y fiable, permitiendo así un más amplio uso y distribución de las Apostillas Electrónicas. La nueva versión de Microsoft Word 2007 también incluye un soporte integrado y gratuito para la conversión de PDF. Por lo tanto, en resumen, la Autoridad Competente podrá elegir distribuir la Apostilla electrónica electrónicamente en Word *o* PDF tan sólo haciendo clic en un botón.

B. Nociones básicas de Infraestructura de Clave Pública (PKI, siglas en inglés).

12. El modelo de confianza de la firma digital de Adobe PDF se basa en las pautas operativas de una Infraestructura de Clave Pública (PKI). Si bien sólo tenemos espacio aquí para discutir los principios básicos de PKI,[3] es importante notar que una PKI involucra ciertos actores clave, incluyendo una Autoridad de Certificación (AC) y una Autoridad de Registro (AR). Una AC es un tercero independiente de cualquier transacción que ocurra dentro de una PKI. La AC emite un certificado digital que se utiliza para firmar digitalmente el PDF. LA AC es una organización controlada que debe cumplir estrictos procedimientos operativos para mantener la confianza de los certificados digitales que emite. Contratada por la AC, la AR es únicamente responsable de validar la identidad y establecer los derechos y obligaciones relacionados de una persona que solicita un certificado digital. Retomando el ejemplo de la primera Apostilla Electrónica de prueba, el Estado de Kansas en los Estados Unidos actuó como AR emitiendo un certificado digital a un empleado de la oficina del *Kansas Secretary of State*. La confianza dentro de una PKI se basa en que la AC y la AR actúen responsablemente y se sujeten a auditorias e inspecciones independientes. Sin embargo, la confianza dentro de una PKI también se encuentra en manos de las partes que realizan la transacción que por lo general incluye un firmante y un receptor del documento. Como se explicó anteriormente, si el receptor del documento *confía* en que la AC y en la AR son actores creíbles, entonces el receptor del documento puede a su vez confiar en que el firmante del documento es quién sostiene ser y se encuentra actuando dentro del ámbito de su autoridad. En otras palabras, el receptor del documento tiene la completa autoridad para confiar o no confiar en las transacciones dentro del marco de una PKI.

13. Además del modelo de confianza de la PKI, existen otras características importantes que se encuentran incluidas o pueden incluirse en una infraestructura PKI dada.

(1) Una característica importante es que los participantes de una infraestructura PKI pueden confiar en la Declaración de Prácticas de Certificación (CPS). La CPS contiene una declaración de roles, responsabilidades y requisitos que rigen la emisión, uso y administración de certificados digitales dentro de un PKI en particular, entre otras cosas. Por lo tanto, a manera de ejemplo una CPS, puede declarar que todos los certificados digitales emitidos según la CPS requieren que el solicitante de un certificado digital se identifique personalmente y mediante una AR adecuada. En muchos casos, una CPS es redactada para cumplir con la Política de Certificado de Infraestructura de Clave Pública Internet X.509 y el Marco de Referencia de las Prácticas de Certificación de la Fuerza de Trabajo de Ingeniería de Internet (IETF, siglas en inglés). En el marco del *e-APP*, el estado de Kansas en los Estados Unidos ha emitido la siguiente CPS que rige su administración de certificados digitales.

(2) Una entidad gubernamental o privada puede además estar sujeta a leyes, normas y/o reglamentaciones locales que rigen la emisión y uso de certificados digitales. Por ejemplo, respecto de la primera Apostilla Electrónica

[3] Los lectores interesados en una explicación más detallada de PKI pueden empezar por aquí: < http://en.wikipedia.org/wiki/Public_key_infrastructure > (desde el 19 de marzo 2007). Las fuentes de referencias generales y especiales son abundantes, y Wikipedia provee una excelente introducción en la materia.

de prueba emitida por la Autoridad Competente de Kansas, las reglamentaciones estatales locales rigen la emisión y administración de certificados digitales por la AC Raíz de Kansas. Una importante característica de estas reglamentaciones es que se requiere por ley a todos los solicitantes que se presenten en persona ante un funcionario autorizado del gobierno y, presenten al menos una identificación con foto brindada por el gobierno a una Autoridad de Registro Local, a fin de solicitar y recibir un certificado digital de la AC del estado de Kansas. En este momento, Kansas permite a los *Chiefs Elections Officers* de servir como Autoridades Locales de Registro.

(3) Para brindar una verificación de revocación más rápida y confiable, una AC podrá activar una característica conocida como *Online Certificate Status Protocol* (OSCP). El OCSP permite controles más rápidos y confiables del estado de revocación de un certificado digital emitido por una AC en particular. Por lo tanto, el OCSP, si bien no es obligatorio bajo una PKI, puede brindar un medio más eficiente y rápido de verificar si un certificado digital ha sido revocado o es todavía válido. Si bien el estado de Kansas todavía no ofrece una verificación de revocación OCSP, podría hacerlo en el futuro.

14. Entendemos que el proceso de firma electrónica segura como se inserta en la tecnología de Adobe y se describe arriba concuerda con la Ley Modelo de la CNUDMI sobre Firmas Electrónicas (véase en especial, los artículos 6, 7 Y 12(3)), siempre y cuando, naturalmente, la conducta del firmante y del proveedor de servicios de certificación reúnan los requisitos establecidos en los Artículos 8 y 9 de la Ley Modelo. La Ley Modelo de la CNUDMI en su Artículo 2(a) define la firma electrónica como "los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo [es decir, la Apostilla], que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos". Y el requisito de fiabilidad de una firma electrónica, según lo establece el Artículo 6 de la Ley Modelo de la CNUDMI, "quedará cumplido en relación con un mensaje de datos si se utiliza una firma electrónica que, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo aplicable, sea fiable y resulte igualmente apropiada para los fines con los cuales se generó o comunicó ese mensaje." El proceso de firma electrónica segura de Adobe según se describe arriba cumple con esta definición de firma electrónica.[4]

15. Además, el estándar aplicado en el Artículo 12(3) de la Ley Modelo de la CNUDMI para el reconocimiento de firmas electrónicas creadas en otro Estado proporciona otra base relevante para el reconocimiento entre Estados partes de la Convención, de Apostillas Electrónicas emitidas de conformidad con el modelo sugerido en el *e-APP*.[5] Otra vez, nosotros pensamos que el modelo sugerido por el *e-APP* ofrece un altísimo nivel de fiabilidad y por consiguiente, las Apostillas Electrónicas emitidas según este modelo deberían ser reconocidas entre Estados partes. Estas razones se amplían más aún a través del principio general de la Convención de que una Apostilla producida válidamente en un Estado parte de la Convención debe ser reconocida por otro Estado parte de la Convención.[6] Finalmente, y tal vez sea lo más importante, puede resultar de utilidad recordar que miles (si no millones) de Apostillas se emiten todos los años usando

---

[4] Véase también las definiciones de "mensaje de datos" y "firmante" en el Art. 2(c) y 2(d), respectivamente, de la Ley Modelo de la CNUDMI sobre Firmas Electrónicas, Art. 2(c): Art. 2(c) "Por "mensaje de datos" se entenderá la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax"; Art. 2(d): "Por "firmante" se entenderá la persona que posee los datos de creación de la firma y que actúa por cuenta propia o por cuenta de la persona a la que representa".

[5] Art. 12(3) dice lo siguiente: "Toda firma electrónica creada o utilizada fuera [del Estado promulgante] producirá los mismos efectos jurídicos en [el Estado promulgante] que toda firma electrónica creada o utilizada en [el Estado promulgante] si presenta un grado de fiabilidad sustancialmente equivalente."

[6] Es en base a este principio que la Oficina Permanente ha reiterado que las Apostillas extranjeras no pueden ser rechazadas por el Estado receptor sólo en base a que no están de acuerdo a la manera a la cual las Apostillas son emitidas en el Estado receptor (por ejemplo, con vistosos listones, remaches o lacres). Véase la Conclusión y Recomendación Nro. 13 de la reunión de la Comisión Especial de 2003.

estampillas de firmas o copias escaneadas de firmas holográficas. A pesar de que estas técnicas para firmar ofrecen niveles significativamente inferiores de seguridad que el modelo sugerido por el *e-APP*, nunca -- a nuestro leal saber y entender – han causado graves problemas de reconocimiento de Apostillas extranjeras.

C. Viabilidad a largo plazo de documentos PDF

16. Hemos recibido preguntas relativas a la viabilidad a largo plazo de un producto comercial como el Adobe PDF y más específicamente cómo el *e-APP* atendería el tema de si un documento PDF firmado digitalmente realizado en el año 2007 sería visible por algún receptor, sin costo, en el año 2030 (o más adelante). Si bien ésta es un área que atrae mucho interés y que está siendo estudiada activamente,[7] el alcance de este Memorándum no se extiende a la discusión de archivo de documentos a largo plazo. La especificación de PDF existente es parcialmente una especificación que permite que cualquiera, libre de pago de derechos o licencias, desarrolle software que lea y escriba en la especificación de PDF. Significativamente, Adobe recientemente ha anunciado que publicará la especificación completa de PDF a un organismo internacional independiente y abierto para uso público.[8] En breve, permitir que la especificación PDF sea administrada por un organismo independiente permite que los desarrolladores de software puedan acceder y ver documentos en formato PDF utilizando un estándar abierto en el futuro sin tener que comprar una licencia Adobe.

II. El formato de una Apostilla electrónica: puede ser ya sea, un archivo PDF continuo y único o un archivo PDF con un documento adjunto.

17. En el *e-APP*, contemplamos dos formatos distintos pero en última instancia idénticos para las Apostillas electrónicas. Ambos métodos protegen el documento subyacente y el Certificado de la Apostilla electrónica de modificaciones no autorizadas, pero cada uno presenta una interfaz diferente al destinatario.

18. Con el primer método, una Autoridad Competente puede agregar el Certificado de Apostilla como la última página de un documento público existente en PDF. Usando este método, entonces, el destinatario abriría el documento PDF y encontraría el Certificado de Apostilla incluido como la última página del mismo documento PDF. Si se elige este formato, el documento público subyacente y el Certificado de Apostilla electrónica forman un documento continuo o, dicho de otra manera, un solo archivo PDF. Se puede elegir imprimir una o más páginas de ese archivo único, por lo que el Certificado de Apostilla electrónica se puede imprimir de manera separada (véase punto III en la parte inferior para más información).

19. Con el segundo método, un documento público subyacente se adjunta como un archivo separado al Certificado de Apostilla electrónico. Este es el método que Kansas eligió para su Apostilla electrónica de prueba. El destinatario recibe un sólo archivo PDF, pero al abrirlo, el usuario primero ve el Certificado de Apostilla electrónica, y luego puede abrir el documento público subyacente para visualizarlo como un archivo PDF separado. Según nuestra opinión, este método provee una interfaz más intuitiva al destinatario del documento apostillado (por cierto, podemos indicar que éste también es el método adoptado por el Departamento de Estado de los Estados Unidos para la presentación electrónica de patentes y su modelo de Apostillas electrónicas). Al adjuntar el documento público subyacente como un archivo al Certificado de Apostilla electrónica, se intenta

---

[7] Los lectores interesados en investigar más acerca de este tema tal vez deseen revisar el trabajo de LTANS (Archivo a Largo Plazo y Servicios Notariales) el grupo de trabajo de IETF (Grupo de Tareas de Ingeniería de Internet, el IETF es una gran comunidad abierta de diseñadores de redes, operadores, proveedores e investigadores abocados a la evolución de la arquitectura y operación de Internet, está abierto a cualquier persona interesada), el Grupo de Trabajo LTANS está desarrollando una Sintaxis de Registros de Pruebas para almacenamiento a largo plazo y recuperación de documentos firmados digitalmente durante períodos largos y posiblemente no determinados. Visite < http://www.ietf.org/html.charters/ltans-charter.html > (desde el 19 de marzo de 2007) para mayor información.

[8] Los lectores puede referirse al comunicado de prensa de Adobe acerca de este tema aquí: < http://www.adobe.com/aboutadobe/pressroom/pressreleases/200701/012907OpenPDFAIIM.html > (desde el 19 de marzo de 2007).

dejar bien en claro al destinatario al abrir el documento por primera vez que se trata de una Apostilla. A partir de allí, puede abrir el documento público para visualizar sus contenidos.

20. Según el *e-APP*, una Autoridad Competente puede seleccionar cualquier modelo, y el *e-APP* no pretende sugerir que uno u otro sea preferible.

III. Impresión de las Apostillas electrónicas

21. Imprimir el Certificado de Apostilla electrónica (con o sin el documento público subyacente) presenta por lo menos dos cuestiones que se deben tratar por separado: (A) cómo evitar la reutilización fraudulenta del Certificado de Apostilla electrónica en el soporte impreso; y (B) Cómo garantizar que la impresión de un Certificado de Apostilla electrónica reunirá los requisitos de mantenimiento de archivos y las reglas sobre las pruebas en soporte papel.

A. Cómo evitar la reutilización fraudulenta de un Certificado de Apostilla electrónica

22. El problema de evitar la reutilización de la versión impresa de un Certificado de apostilla electrónico es difícil de resolver en la era del software de edición digital de imagen. Incluso si usáramos el primer método descrito arriba exclusivamente, uno podría elegir imprimir sólo el Certificado de Apostilla electrónica como una página separada, y nos enfrentaríamos con el problema de la reutilización fraudulenta de esa Apostilla en otros documentos. De hecho, uno puede simplemente capturar el Certificado de Apostilla con “imprimir pantalla” (escriba “Apostilla” en la Búsqueda de Imágenes de Google...) o puede pasar 30 minutos en Microsoft Word para crear un Certificado de Apostilla falso que parezca perfectamente válido y que se puede imprimir fácilmente con fines fraudulentos. Nuevamente sugerimos comparar el *e-APP* con los niveles de seguridad y anti-fraude que se han logrado en el ámbito de papel solamente. Si tenemos en cuenta no sólo la Apostilla electrónica sino también el elemento de Registro electrónico del *e-APP*, estamos convencidos que el *e-APP* excede en mucho los niveles actuales de seguridad y protección anti-fraude.

23. Otro desafío es la imposibilidad (y, por obvias razones, no es tampoco recomendable) de construir un sistema centralizado de administración de Apostillas Electrónicas, al menos no por el momento. Aunque es verdad que un sistema centralizado nos permitiría conseguir soluciones de seguridad rentables en el sistema, de las cuales toda Autoridad Competente podría aprovecharse, en el marco del *e-APP*, no tenemos la opción de crear ni un sistema centralizado (ya que seguramente sería necesaria una nueva Convención) ni la capacidad de imponer un requisito específico de software o hardware a una Autoridad Competente (debido a que la Convención es neutral desde el punto de vista técnico).

24. Teniendo esto en cuenta, la reutilización fraudulenta de una Apostilla electrónica o de papel es un problema que debe ser abordado. Existen tres soluciones principales en este sentido: (a) El Registro electrónico; (b) agregar la fecha y momento exactos de firma del documento público subyacente en la información provista en la mención impresa 2 del Certificado de Apostilla; y (c) usar códigos de barras.

25. (a) No tenemos ninguna duda con respecto a que la mejor forma de impedir la reutilización fraudulenta de cualquier Apostilla (sea electrónica o de papel) es fomentando todo lo posible el uso del Registro que toda Autoridad Competente debe tener según el Artículo 7 de la Convención. El *e-APP* amplía considerablemente las ventajas y beneficios de estos Registros al hacerlos accesibles en línea. (Sugerimos que aunque una Autoridad Competente no decida nunca emitir un Certificado de Apostilla electrónica, toda Autoridad Competente debería ya de mantener un registro electrónico). Imaginemos, por ejemplo, que toda Autoridad Competente mantuviera un Registro electrónico de Apostillas en línea que facilitará una verificación inmediata y fiable de cualquier Apostilla emitida por una Autoridad Competente. Esto significaría un gran avance en la lucha contra el fraude con una solución simple y global ya que, todos los Certificados de Apostillas podrían verificarse en un Registro electrónico accesible por Internet. El desafío, naturalmente, es que toda Autoridad Competente se comprometa a

ofrecer un Registro electrónico. Tenemos un largo camino por recorrer antes de lograr este panorama ideal, pero al ofrecer un Registro electrónico abierto y gratuito, el *e-APP* nos acerca mucho más a este objetivo. Además, la fácil accesibilidad del Registro electrónico proporcionará la herramienta de verificación disponible más importante con respecto a mantenimiento de archivos y las reglas sobre las pruebas.

26. (b) Otro método para vincular la versión impresa del Certificado de Apostilla electrónico al documento público subyacente es agregar la fecha y momento exactos en que se firmó el documento público a la información provista en la mención impresa 2 del Certificado de Apostilla: Por lo tanto, la mención 2 de un Certificado de Apostilla podría incluir la siguiente información “Juan Pérez, el 2007.01.12 13:46:17 -06'00”. No hace falta decir que esta información adicional no se puede imponer como una condición general para los Certificados de Apostilla en soporte papel. Además, debido a que este proceso requiere una pequeña modificación del Certificado de Apostilla Modelo adjunto a la Convención, tampoco queremos imponerlo para la Apostillas electrónicas según el *e-APP*, pero nos parece apropiado recomendar su inclusión a las Autoridades Competentes ya que amplía las características de seguridad de una Apostilla electrónica.

27. (c) Otro método que recomendamos para permitir la impresión y al mismo tiempo contrarrestar el fraude, es el código de barras. Al insertar un código de barras de “formularios de papel" Adobe en el Certificado de Apostilla electrónico que incluya datos que sean únicos tanto para el Certificado de Apostilla electrónico como para el documento público subyacente, cualquier persona (que cuente con un dispositivo para escanear, véase abajo) a la que se entregue la versión impresa del Certificado de Apostilla electrónico y el documento público (subyacente) podría escanear el código de barras para verificar si esos documentos impresos van juntos.

28. Un código de barras de “formularios de papel” en las carpetas de Ayuda de Adobe Designer 7.0 se define de la siguiente manera: “Un código de barras de formulario de papel captura electrónicamente los datos provistos por el usuario en un formulario PDF interactivo. Cuando el usuario completa el formulario usando Adobe Reader o Acrobat, el código de barras se actualiza de manera automática para codificar los datos provistos por el usuario. El usuario puede luego regresar al formulario completo y devolverlo por fax, correo o personalmente. Al recibirlo, los datos provistos por el usuario se pueden decodificar usando un dispositivo para escanear”. Según se describe en esta definición, el "usuario" sería un funcionario encargado de completar los Certificados de Apostilla en carácter de Autoridad Competente o en representación de ella. Según lo prevé el *e-APP*, un código de barras de formulario de papel Adobe, también conocido como código de barras "dinámico" (en contraposición a estático), permitiría que la Autoridad Competente inserte la información del código de barras que podría incluir toda la información incluida en los 10 menciones impresas de un Certificado de Apostilla, así como también la información contenida en el certificado digital (como el nombre, dirección de correo electrónico del firmante, etc.). Al recibir un Certificado de Apostilla electrónico impreso con dicho código de barras, el destinatario podría escanear el código de barras para revelar la información que contiene. De esta manera, el destinatario de la Apostilla electrónica impresa podría comparar la información incluida en el código de barras con la información del Certificado de Apostilla electrónico impreso, o la información incluida en el Registro electrónico, para verificar que la información del código de barras corresponde a la información del Certificado de Apostilla electrónico impreso o el Registro electrónico. Debido a que es muy difícil falsificar códigos de barras, el destinatario tendría un alto grado de seguridad de que el documento no ha sido alterado. Entonces, los códigos de barras son de gran importancia cuando el Certificado de Apostilla electrónico se imprime. Además, si el original electrónico se pierde, y sólo queda la Apostilla electrónica impresa, el código de barras puede seguir brindando una verificación fiable en un futuro inmediato. De la manera indicada, los datos importantes provistos por el usuario se pueden integrar al código de barras para la verificación de seguridad.

29. Naturalmente, esta solución presupone que (a) las Autoridades Competentes tienen el software para producir códigos de barras y (b) los destinatarios tienen la tecnología para escanear y procesar códigos de barras, lo que presenta un problema práctico pero que se puede solucionar sin mucha dificultad. Con la compra de Adobe Standard o

Professional se recibe el software "Adobe Designer", que permite a las Autoridades Competentes incluir códigos de barras en un formulario PDF, como un Certificado de Apostilla electrónico, sin costo adicional y con un mínimo esfuerzo. Además, el bajo costo de los escáners de código de barras y su uso difundido en el mercado implica que adquirir dicho escáner no representa un mayor obstáculo para muchas Autoridades Competentes. En cuanto al punto anterior, creemos que no se debe imponer sino simplemente sugerir o recomendar el uso de códigos de barras.

30. Algunos comentarios sobre *marcas de agua digitales*. No creemos que todo el Certificado de Apostilla debiera aparecer como una marca de agua en el documento público subyacente. Esta alternativa generaría un cambio considerable en el formato del Certificado de Apostilla y por lo tanto no respetaría el Certificado Modelo adjunto a la Convención. Además, una marca de agua de tal tamaño haría que el documento subyacente fuese difícil de leer. También presenta problemas prácticos con documentos de múltiples páginas. Sin embargo, sí queremos investigar la posibilidad de usar, como una característica de seguridad recurrente, una pequeña marca de agua que apareciera en un lugar discreto en cada página del documento público subyacente (como repetir el número del Certificado de Apostilla electrónico en una esquina de cada página del documento subyacente).

B. Cómo garantizar que la impresión reunirá los requisitos de mantenimiento de archivos y reglas sobre la prueba en soporte papel

31. Creemos firmemente que es una meta importante contar con la posibilidad de poder imprimir una Apostilla electrónica (el Certificado y el documento subyacente) de tal manera que se pueda confiar en la versión impresa con fines de mantenimiento de archivos y reglas sobre la prueba. Puesto de otra manera, tal vez la pregunta sea: "¿cómo se puede imprimir una Apostilla electrónica y verificar que su estado electrónico original no haya sido alterado?" Esta pregunta naturalmente nos lleva al tema de la transformación en la era digital. Las recomendaciones en la sección A también beneficiarán los requisitos de mantenimiento de archivos y reglas sobre la prueba solamente en soporte papel, al igual que el uso del Registros electrónicos; la información adicional en la mención impresa 2 del Certificado de Apostilla electrónico y los códigos de barra permitirán la verificación del origen y por lo tanto de la autenticidad de una Apostilla electrónica impresa.

32. En este Memorándum, no tenemos la intención de decidir si una versión impresa de una Apostilla electrónica tiene la misma validez legal que el original electrónico. Esta pregunta probablemente sea relevante sólo cuando haya litigio sobre el origen de la Apostilla electrónica, en cuyo caso tanto la versión impresa de la Apostilla como la electrónica deberán presentarse ante un tribunal. Sobre la base de por lo menos la versión electrónica - y desde luego en combinación con el Registro, en especial si es un Registro electrónico con acceso en línea como sugiere el *e-APP* – será posible entonces evaluar con un altísimo grado de certeza el origen de la Apostilla. Por supuesto suponemos que el destinatario guardará no sólo la versión impresa de la Apostilla sino también la versión original electrónica. Realmente creemos que es mucho más probable que el destinatario guarde sólo la versión original electrónica.

33. Muchos organismos gubernamentales almacenan documentos oficiales electrónicamente y sólo producen versiones impresas como copias certificadas (por ejemplo, los certificados de nacimiento en los EE.UU. rara vez se guardan en soporte papel; otro ejemplo son los estatutos de las compañías que en muchos países son casi exclusivamente electrónicos). ¿Por qué las razones o los estándares deben ser diferentes para las Apostillas (electrónicas)? Además, como se mencionó anteriormente (véase párrafo 14), es una práctica común expedir Apostillas de papel con estampillas de firmas o copias escaneadas de firmas holográficas y no sabemos de ningún problema relacionado con el reconocimiento de dichas Apostillas. Una versión impresa de un Certificado de Apostilla electrónico expedido según el modelo del *e-APP* ofrece características de seguridad y anti-fraude que exceden en gran manera esta práctica. Por lo tanto, sería asombroso que los destinatarios, tribunales, y otros usuarios cuestionen la pertinencia de estas características del *e-APP* cuando de hecho perfeccionan la autenticidad de un documento de papel.

34. Finalmente, en el marco del *e-APP*, continuaremos alentando a los Estados a implementar legislación correspondiente en materia electrónica (véase Conclusión 2 del Primer Foro Internacional sobre la Notarización y las Apostillas Electrónicas), pero creemos que no tenemos que esperar que esto pase en todas partes. El *e-APP* se puede considerar en realidad como un catalizador, tanto para los Estados que ya cuentan con leyes de habilitación como para aquellos que recién ahora las están considerando.

IV. Otros cambios sugeridos

35. Además de las sugerencias analizadas arriba, se introducirán los siguientes cambios al modelo de la Apostilla electrónica, según se sugirió originalmente de conformidad con el *e-APP*:

El modelo de software PDF original se modificará para garantizar que las casillas de texto 2, 6 y 8 no se puedan modificar. Como resultado todas las casillas de texto se encontrarán igualmente protegidas de modificaciones no autorizadas.

También se sugiere (pero no se requiere) que el puesto de la persona que certifica el documento se ingrese en la casilla de texto 7.

Conclusión

36. Como se hizo notar más arriba, tal vez el objetivo más claro del *e-APP* es la comunicación y el diálogo a fin de asegurar el funcionamiento eficaz de una exitosa Convención sobre Apostilla en un ambiente electrónico. Los autores tienen la intención de que este Memorándum se extienda y aliente ese diálogo, pero también deseamos resaltar que los documentos electrónicos y las firmas electrónicas ya están entre nosotros y sólo muestran signos de ser cada vez más y más comunes, por no decir estándares *de facto* para las transacciones. Creemos firmemente que las Autoridades Competentes bajo el *e-APP* pueden beneficiarse mediante a) la operación de Registros Electrónicos, b) intercambio de Apostillas electrónicas, y c) compartiendo sus experiencias y conocimientos entre ellos. Hemos determinado que el servicio público que las Autoridades Competentes brindan mediante la emisión de Apostillas sólo puede ser fortalecida bajo el *e-APP*.

37. Este Memorándum ha sido preparado en respuesta a algunas de las preguntas y comentarios recibidos desde el lanzamiento del *e-APP* en abril de 2006. Quisiéramos agradecer a todos aquellos que participaron en este intercambio de ideas por sus valiosas contribuciones. Nos han ayudado a darnos cuenta que los procesos e ideas aclarados en este Memorándum deben ser compartidos con otras Autoridades Competentes que consideren la implementación del *e-APP* y también con un público más amplio. Con ese fin, estos procesos e ideas se reflejarán en el material educativo en relación con el *e-APP*.

38. A fin de cuentas, el *e-APP* busca extender el alcance de la Convención de Apostilla al medio electrónico, donde sin duda surgirán nuevos interrogantes. Sin embargo, estamos convencidos de que podemos abordar estas preguntas bien y al mismo tiempo honrar el propósito de la Convención y hacer que su implementación sea más efectiva y segura.

39. Creemos que estas características de seguridad mejoradas y estos procesos estandarizados no sólo mejorarán el funcionamiento de la Convención, sino que también darán a los destinatarios de Apostillas extranjeras una mayor confianza para aceptarlas y obrar en consecuencia.