Naciones Unidas A/CN.9/630/Add.1

Asamblea General

Distr. general
25 de abril de 2007
Español
Original: inglés

Comisión de las Naciones Unidas para el Derecho Mercantil Internacional
40º período de sesiones
Viena, 25 de junio a 12 de julio de 2007

Posible labor futura en la esfera del comercio electrónico

Documento general de referencia sobre los elementos necesarios para establecer un marco jurídico favorable al comercio electrónico: modelo de capítulo sobre la utilización internacional de métodos de autenticación y firmas electrónicas

Nota de la Secretaría*

Adición

En el anexo de la presente nota figura parte de un modelo de capítulo (primera parte, cap. I, secciones B y C de un documento general de referencia) sobre cuestiones jurídicas relacionadas con la utilización internacional de métodos de autenticación y firmas electrónicas.

* La presentación del presente documento por la Secretaría de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional se retrasó debido a la falta de personal.

V.07-82783 (S) 040607 050607

Anexo

Índice

Primera parte

Métodos de firma y autenticación electrónicas

[...]

I. Definición y métodos de autenticación y firma electrónicas

[…]

B. Principales métodos de firma y autenticación electrónicas

1. A los efectos del presente análisis se examinarán cuatro métodos principales de firma y autenticación: las firmas digitales; los métodos biométricos; las contraseñas y los métodos híbridos; y las firmas escaneadas o mecanografiadas.

1. Firmas numéricas basadas en criptografía de clave pública

2. Se entiende por "firma digital" la que se obtiene mediante aplicaciones tecnológicas en que se utiliza criptografía asimétrica, también denominada sistemas de cifrado de clave pública, para asegurar la autenticidad de los mensajes electrónicos y garantizar la integridad de su contenido. La firma digital se presenta de muchas formas distintas, por ejemplo, firmas digitales infalsificables, firmas ciegas y firmas digitales irrefutables.

a) Conceptos técnicos y terminología

i) Criptografía

3. Las firmas digitales se crean y verifican utilizando criptografía, rama de las matemáticas aplicadas que se ocupa de trasformar mensajes en formas aparentemente ininteligibles y se devuelven luego a su forma original. En las firmas digitales se utiliza lo que se denomina criptografía de clave pública, que se suele basar en el empleo de funciones algorítmicas para generar dos "claves" diferentes pero matemáticamente interrelacionadas (por ejemplo, grandes números producidos mediante una serie de fórmulas matemáticas aplicadas a números primos)[1]. Una de esas claves se utiliza para crear una firma digital o transformar datos en una forma en apariencia ininteligible, y la otra para verificar una firma digital o devolver el mensaje a su forma original[2]. El equipo y los programas informáticos que utilizan

---

[1] Cabe señalar, sin embargo, que el concepto de criptografía de clave pública que se examina aquí no implica necesariamente el empleo de algoritmos basados en números primos. En la actualidad se utilizan o se preparan otras técnicas matemáticas, como los criptosistemas de curvas elípticas, a los que suele atribuirse la posibilidad de ofrecer un alto grado de seguridad mediante el empleo de longitudes de clave considerablemente reducidas.

[2] Aunque el empleo de la criptografía es una de las principales características de las firmas digitales, el mero hecho de que éstas se utilicen para autenticar un mensaje que contenga información en forma digital no debe confundirse con el uso más general de la criptografía con fines de confidencialidad. El cifrado con fines de confidencialidad es un método utilizado para codificar una comunicación electrónica de tal modo que sólo puedan leerla el iniciador y el destinatario del mensaje. En varios países la ley limita, por razones de orden público que pueden

dos de esas claves se suelen denominar en conjunto “criptosistemas” o, más concretamente, “criptosistemas asimétricos” cuando se basan en el empleo de algoritmos asimétricos.

ii) Claves públicas y privadas

4. Se denomina “clave privada” a una clave complementaria con que se producen firmas digitales, que utiliza únicamente el firmante para crear la firma digital y debe mantenerse en secreto, mientras que la “clave pública”, es conocida de ordinario por más personas y la utiliza la parte que confía para verificar la firma digital. La clave privada puede mantenerse en una tarjeta con memoria, o es posible acceder a ella mediante un número de identificación personal (NIP) o un dispositivo de identificación biométrica, por ejemplo mediante el reconocimiento de una huella dactilar. En caso de que muchas personas tengan que verificar la firma digital del firmante, la clave pública debe ponerse a disposición de todas o distribuirse entre ellas, por ejemplo, adjuntando los certificados a las firmas o utilizando otros medios para asegurar que las partes que confían, y únicamente las que deben verificar la firma, puedan obtener los certificados conexos. Aunque las claves del par están matemáticamente relacionadas entre sí, si un criptosistema asimétrico se ha concebido y aplicado en forma segura es virtualmente imposible deducir la clave privada partiendo de una clave pública conocida. Los algoritmos más comunes para el cifrado mediante las claves públicas y privadas se basan en una característica importante de los grandes números primos, a saber: una vez que se multiplican uno por otro para obtener un nuevo número, resulta especialmente difícil y laborioso determinar cuáles fueron los dos números primos que crearon ese nuevo gran número[3]. De este modo, aunque muchas personas conozcan la clave pública de un determinado firmante y puedan utilizarla para verificar su firma, no pueden descubrir la clave privada de ese firmante ni utilizarla para falsificar firmas digitales.

iii) Función de control

5. Además de la creación de pares de claves se utiliza otro proceso fundamental, que suele denominarse “función de control”, para crear y verificar una firma digital. La función de control es un proceso matemático, basado en un algoritmo que crea una representación digital o forma comprimida del mensaje (llamada con frecuencia

---

incluir consideraciones de defensa nacional, el empleo de criptografía con fines de confidencialidad. Sin embargo, el empleo a efectos de autenticación produciendo una firma digital no implica necesariamente que se utilice la criptografía para dar carácter confidencial a la información durante el proceso de comunicación, porque la firma digital cifrada puede sencillamente añadirse a un mensaje no cifrado.

[3] Algunas de las normas existentes aplican el concepto de “inviabilidad computacional” para referirse a la prevista irreversibilidad del procedimiento, es decir, la expectativa de que sea imposible deducir la clave privada secreta del usuario a partir de su clave pública. “La inviabilidad computacional es un concepto relativo que se basa en el valor de los datos protegidos, el volumen de las operaciones informáticas previas necesario para protegerlos, el período durante el cual requieren protección y el costo y el tiempo necesarios para atacar dichos datos, factores que se evalúan en la perspectiva actual y en la de los futuros avances tecnológicos”. (Asociación de Abogados de los Estados Unidos, *Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce* (Chicago, Asociación de Abogados de los Estados Unidos, 1º de agosto de 1996, que figuran en http://www.abanet.org/scitech/ec/isc/dsgfree.html, consultado el 5 de abril de 2007).

"compendio del mensaje" o "huella dactilar" del mensaje) como "valor de control" o "resultado de control" de una longitud estándar que suele ser mucho menor que la del mensaje pero que sin embargo corresponde en lo esencial exclusivamente a éste. Todo cambio en el mensaje produce invariablemente un resultado de control diferente cuando se utiliza la misma función de control. En el caso de una función de control segura, a la que se denomina en ocasiones "función de control unidireccional", es prácticamente imposible deducir el mensaje inicial aunque se conozca su valor de control. Otra característica básica de las funciones de control es que también resulta casi imposible encontrar otro objeto binario (es decir, distinto del utilizado en un principio para obtener el compendio) que produzca el mismo compendio. Por ello, las funciones de control permiten que los programas informáticos de creación de firmas digitales funcionen con cantidades de datos más pequeñas y predecibles y proporcionen al mismo tiempo una sólida correlación probatoria con el contenido del mensaje inicial y así dan eficientemente garantías de que el mensaje no se haya modificado después de haberse firmado digitalmente.

iv) Firma digital

6. Para firmar un documento o cualquier otro elemento de información, en primer lugar el firmante delimita con exactitud los márgenes dentro de los cuales estará contenida la información que se ha de firmar. Acto seguido, una función de control del programa informático del firmante calcula un resultado de control que (a todos los efectos prácticos) corresponde exclusivamente a la información que se ha de firmar. Ese mismo programa informático transforma luego el resultado de control en una firma digital utilizando la clave privada del firmante. Así pues, la firma digital resultante corresponde exclusivamente a la información que se firma y a la clave privada utilizada para crear dicha firma digital. Generalmente, la firma digital (el cifrado del resultado de control del mensaje con la clave privada del firmante) se adjunta al mensaje y se almacena o transmite junto con él. Sin embargo, también puede enviarse o almacenarse como elemento de datos independiente, siempre que mantenga una vinculación fiable con el mensaje correspondiente. Como la firma digital corresponde exclusivamente a su mensaje, es inservible si se disocia permanentemente de éste.

v) Verificación de la firma digital

7. La verificación de la firma digital es el procedimiento con que se comprueba esa firma por remisión al mensaje original y a una clave pública dada, determinando de esa forma si la firma digital fue creada para ese mismo mensaje utilizando la clave privada que corresponde a la clave pública remitida. La verificación de una firma digital se efectúa calculando un nuevo resultado de control del mensaje original mediante la misma función de control utilizada para crear la firma digital. Seguidamente, utilizando la clave pública y el nuevo resultado de control, el verificador comprueba si la firma digital se creó utilizando la clave privada correspondiente y si el nuevo resultado de control calculado corresponde al resultado de control original que fue transformado en la firma digital durante el trámite de firma.

8. El programa de verificación confirmará que la firma digital ha sido "verificada" desde el punto de vista criptográfico: a) si se utilizó la clave privada del firmante para firmar digitalmente el mensaje, cosa que se reconocerá si se ha

utilizado la clave pública del firmante para verificar la firma, dado que esta clave pública sólo verificará una firma digital creada con la clave privada del firmante; y b) si el mensaje no se ha modificado, lo que se reconocerá si el resultado de control calculado por el verificador es idéntico al extraído de la firma digital durante el procedimiento de verificación.

vi) Otros usos de las tecnología de firma digital

9. Como se indicó *supra*, la tecnología de firma digital sirve para mucho más que meramente "firmar" comunicaciones electrónicas del mismo modo en que se utiliza la firma manuscrita para refrendar documentos (véase el párrafo [...]). Ciertamente, a menudo se utilizan, por ejemplo, certificados firmados digitalmente para "autenticar" servidores o sitios web, entre otras cosas, a fin de garantizar a sus usuarios que son lo que dicen ser o están efectivamente vinculados a la empresa que asegura administrarlos. La tecnología de firma digital puede utilizarse también para "autenticar", por ejemplo, programas informáticos con el fin de garantizar la autenticidad de los que se hayan descargado de un sitio web, para corroborar que un determinado servidor utiliza una tecnología generalmente reconocida por un cierto nivel de seguridad de la conexión, o para "autenticar" cualquier otro tipo de datos que se distribuyan o almacenen digitalmente.

b) Infraestructura de clave pública y prestadores de servicios de certificación

10. Para verificar una firma digital, el verificador debe tener acceso a la clave pública del firmante y tener la seguridad de que corresponde a su clave privada. Sin embargo, un par de claves pública y privada no tiene vinculación intrínseca con nadie; es simplemente un par de números. Se necesita otro mecanismo para vincular en forma fiable a una persona o entidad determinada con el par de claves. Ello es especialmente importante, porque tal vez no haya relación de confianza anterior entre el firmante y los destinatarios de las comunicaciones firmadas digitalmente. A tal efecto, las partes interesadas deben tener cierto grado de confianza en las claves pública y privada que se expidan.

11. Puede que exista el nivel de confianza requerido entre partes que confíen unas en otras, que se hayan tratado durante algún tiempo, que se comuniquen mediante sistemas cerrados, que actúen dentro de un grupo cerrado, o que puedan regir sus operaciones en base a un contrato, por ejemplo, en un acuerdo de asociación comercial. En una operación en la que participen sólo dos partes, cada una puede sencillamente comunicar (por un conducto relativamente seguro, como un servicio de mensajería o por teléfono) la clave pública del par de claves que cada parte utilizará. Sin embargo, este nivel de confianza puede no existir entre partes que se relacionen con poca frecuencia, que se comuniquen a través de sistemas abiertos (por ejemplo, Internet), que no formen parte de un grupo cerrado o que no tengan acuerdos de asociación comercial u otros acuerdos que rijan sus relaciones. Además, cabe tener presente que, en caso de que deban resolverse controversias en los tribunales o mediante arbitraje, puede resultar difícil demostrar si el dueño real de una determinada clave pública la ha revelado o no al destinatario.

12. Un posible firmante podría hacer una declaración pública indicando que debe considerarse que las firmas verificables por una clave pública determinada proceden de él. La forma y la eficacia jurídica de esa declaración se regirían por la ley del Estado promulgante. Por ejemplo, la presunción de que una firma electrónica

corresponde a un determinado firmante podría corroborarse con la publicación de la declaración en un boletín oficial o un documento de "autenticidad" reconocida por las autoridades públicas. Sin embargo, es posible que otras partes no estén dispuestas a aceptar la declaración, especialmente si no hay contrato previo que establezca con certeza el efecto jurídico de esa declaración publicada. La parte que se base en esa declaración publicada sin respaldo en un sistema abierto correría el gran riesgo de confiar inadvertidamente en un impostor, o de tener que impugnar el desconocimiento fraudulento de una firma digital (cuestión a menudo mencionada en el contexto del "repudio negativo" de firmas digitales) si la operación resulta desfavorable para el supuesto firmante.

13. Una forma de resolver algunos de estos problemas es recurrir a uno o más terceros para vincular a un firmante identificado o su nombre con una clave pública determinada. El tercero se conoce en general, en la mayoría de las normas y directrices técnicas, como "autoridad certificadora", "prestador de servicios de certificación" o "proveedor de servicios de certificación" (en la Ley Modelo de la CNUDMI sobre Firmas Electrónicas[4] se ha elegido el término "prestador de servicios de certificación"). En algunos países, esas autoridades certificadoras se han ido organizando jerárquicamente, en lo que suele denominarse infraestructura de clave pública (ICP). Las autoridades certificadoras de una ICP pueden establecerse conforme a una estructura jerárquica en la que algunas certifican únicamente a otras que prestan servicios directamente a los usuarios. En tal estructura, algunas autoridades certificadoras quedan subordinadas a otras. En otras formas concebibles de organizarlas, todas ellas pueden funcionar en pie de igualdad. En toda ICP de gran tamaño podría haber entidades de certificación subordinadas y superiores. Otras soluciones pueden ser, por ejemplo, la expedición de certificados por las partes que confían.

i) Infraestructura de clave pública

14. Establecer una ICP es una forma de crear confianza en que a) la clave pública del usuario no ha sido alterada y corresponde efectivamente a la clave privada del mismo usuario; y b) que se han utilizado buenas técnicas criptográficas. Para crear la confianza señalada más arriba, una ICP puede prestar diversos servicios, como los siguientes: a) gestión de las claves criptográficas utilizadas para las firmas digitales; b) certificación de que una clave pública corresponde a una clave privada; c) suministro de claves a usuarios finales; d) publicación de información sobre la revocación de claves públicas y certificadas; e) administración de símbolos personales (por ejemplo, tarjetas con memoria) que permitan identificar al usuario con información de identificación personal exclusiva o que permitan generar y almacenar claves privadas individuales; f) comprobación de la identificación de los usuarios finales y prestación de servicios a éstos; g) prestación de servicios de marcado cronológico; y h) gestión de las claves criptográficas utilizadas con fines de confidencialidad en los casos en que se autorice el empleo de esa técnica.

15. Una ICP suele basarse en diversos niveles jerárquicos de autoridad. Por ejemplo, los modelos considerados en ciertos países para establecer una posible ICP entrañan referencias a los siguientes niveles: a) una "autoridad principal" única que certificaría la tecnología y las prácticas de todas las partes autorizadas para expedir

[4] Véase la nota [...] [Publicación de las Naciones Unidas, Nº de venta S.02.V.8].

pares de claves o certificados criptográficos en relación con el empleo de dichos pares de claves, y llevaría un registro de las autoridades de certificación subordinadas[5]; b) diversas autoridades de certificación, subordinadas a la "principal", que certificarían que la clave pública de un usuario corresponde en realidad a la clave privada del mismo usuario (es decir, que no ha sido objeto de manipulación indebida); y c) diversas entidades locales de registro, subordinadas a las autoridades de certificación, que recibirían de los usuarios peticiones de pares de claves criptográficas o de certificados relativos al empleo de esos pares de claves, exigirían pruebas de identidad a los posibles usuarios y las verificarían. En ciertos países se prevé que los notarios podrían actuar como autoridades locales de registro o prestar apoyo a dichas autoridades.

16. Las ICP organizadas en una estructura jerárquica pueden ampliarse en el sentido de que es posible que incorporen "colectividades" enteras de nuevas ICP, por el mero expediente de que la "autoridad principal" establezca una relación de confianza con la "autoridad principal" de la nueva colectividad[6]. La autoridad principal de la nueva colectividad puede incorporarse directamente en régimen de sujeción a la autoridad principal de la ICP receptora, subordinándose a ella. La autoridad principal de la nueva colectividad podrá convertirse también en prestador de servicios de certificación subordinado de otro de los prestadores de servicios de certificación subordinados de la ICP existente. Otro aspecto interesante de las ICP jerarquizadas es que resulta fácil establecer el historial de certificación, porque éste va en una sola dirección, retrospectivamente desde el certificado del usuario hasta el momento en que éste elige una entidad en que confiar. Además, el historial de certificación en una ICP jerarquizada es relativamente breve, y los usuarios de un sistema jerarquizado saben implícitamente para qué aplicaciones sirve un certificado, según la posición que ocupe el prestador de servicios de certificación en esa jerarquía. Sin embargo, las ICP jerarquizadas también tienen desventajas, principalmente porque se basan en la confianza depositada en una sola de ellas. Si la autoridad principal se ve comprometida, ello afecta a toda la ICP. Además, en algunos países ha resultado difícil elegir una sola entidad como autoridad principal e imponer esta jerarquía a todos los demás prestadores de servicios de certificación[7].

17. La llamada ICP "en malla" es una opción ante la ICP jerarquizada. Conforme a este modelo, los prestadores de servicios de certificación forman parte de una relación entre iguales. Cualquiera de los que actúan conforme a este modelo puede ser el depositario de la confianza. Por regla general, el usuario confía en el que expidió su certificado. Los prestadores de servicios de certificación podrán expedirse recíprocamente certificados; este par de certificados refleja su relación de confianza mutua. La ausencia de jerarquía en este sistema significa que los prestadores de servicios de certificación no pueden imponer condiciones que rijan los tipos de certificados expedidos por otros prestadores de dichos servicios. Si uno

---

[5] La cuestión de si un gobierno debe tener capacidad técnica para conservar o recrear claves de confidencialidad privada podría abordarse a nivel de las autoridades principales.

[6] William T. Polk y Nelson E. Hastings, "*Bridge Certification Authorities: Connecting B2B Public Key Infrastructures*", National Institute of Standards and Technology (septiembre de 2000), que figuran en http://csrc.nist.gov/pki/documents/B2B-article.pdf, consultado el 30 de marzo de 2007.

[7] Polk y Hastings (véase la nota [6]), señalan que en los Estados Unidos de América, fue muy difícil elegir al organismo del gobierno federal que asumiría la autoridad general respecto de la ICP federal.

de ellos desea limitar la confianza que se otorgue a otros, deberá indicar estas limitaciones en los certificados expedidos a sus colegas[8]. Sin embargo, armonizar las condiciones y las limitaciones de reconocimiento mutuo puede resultar sumamente complejo.

18. La tercera estructura opcional es la del prestador de servicios de certificación "intermedio". Ésta puede resultar especialmente útil para que varias colectividades de ICP anteriores confíen en sus respectivos certificados. A diferencia del prestador de servicios de certificación de una ICP "en malla", el "intermediario" no expide certificados directamente a los usuarios. No se prevé tampoco que este "intermediario" sea objeto de la confianza de los usuarios de la ICP, como sería el caso de un prestador de servicios de certificación "principal". En lugar de ello, el "intermediario" establece relaciones de confianza entre iguales con las distintas colectividades de usuarios, permitiendo de este modo que éstos conserven los depositarios naturales de su confianza en sus ICP respectivas. Si una colectividad de usuarios implanta un dominio de confianza en forma de una ICP jerarquizada, el prestador de servicios de certificación "intermedio" establece una relación con la autoridad principal de esa ICP. Sin embargo, si la colectividad de usuarios implanta un dominio de confianza creando una red de ICP, el prestador de servicios de certificación "intermedio" necesita únicamente entablar una relación con uno de los prestadores de servicios de certificación de la ICP, que pasa a ser el "principal" prestador de servicios de certificación de esa ICP a efectos de la "mediación de confianza" con la otra ICP. Esta "mediación de confianza", que une a dos o más ICP por su relación mutua con un prestador de servicios de certificación "intermedio" permite a los miembros de distintas colectividades de usuarios interactuar entre sí mediante el prestador de servicios de certificación "intermedio", con un grado de confianza determinado[9].

ii) Prestador de servicios de certificación

19. Para vincular un par de claves a un posible firmante, el prestador de servicios de certificación (o autoridad certificadora) expide un certificado, que es un registro electrónico en que se indica una clave pública junto con el nombre del suscriptor del certificado como "sujeto" del certificado, y con el que puede confirmarse que el firmante potencial que figura en el certificado posee la clave privada correspondiente. La función principal del certificado es vincular una clave pública a un firmante concreto. El "receptor" del certificado que desee confiar en la firma digital creada por el firmante que figura en él puede utilizar la clave pública indicada en ese certificado para verificar si la firma digital se creó con la clave privada correspondiente. Si dicha verificación es positiva, se obtiene técnicamente cierta garantía de que la firma digital fue creada por el firmante y de que la parte del mensaje utilizada en la función de control (y, por ello, el correspondiente mensaje de datos) no se ha modificado desde que se firmó digitalmente.

20. Para asegurar la autenticidad del certificado con respecto tanto a su contenido como a su fuente, el prestador de servicios de certificación lo firma en forma digital.

---

[8] Polk y Hastings, *Bridge Certification Authorities* … (véase la nota [5]).

[9] La estructura que se eligió en último término para establecer el sistema de ICP del gobierno federal de los Estados Unidos fue la del prestador de servicios de certificación "intermedio" (Polk y Hastings, véase la nota [6]). El mismo modelo siguió el Gobierno del Japón para establecer su sistema de ICP.

La firma digital del prestador de servicios de certificación que figura en el certificado se puede verificar utilizando su clave pública, que figura en el certificado de otra entidad certificadora (que puede ser, aunque no necesariamente, de un nivel jerárquico superior) y ese otro certificado puede autenticarse a la vez utilizando la clave pública incluida en un tercer certificado, y así sucesivamente hasta que la persona que confíe en la firma digital tenga seguridad suficiente de su autenticidad. Entre otros métodos posibles para verificar la firma digital, esa firma se puede registrar en un certificado emitido por el prestador de servicios de certificación (que se denomina en ocasiones "certificado raíz")[10].

21. En todos los casos, el prestador de servicios de certificación que expida el certificado podrá firmarlo digitalmente durante el período de validez del otro certificado utilizado para verificar la firma digital del prestador de servicios de certificación. Para fomentar la confianza en la firma digital del prestador de servicios de certificación, algunos Estados prevén la publicación en un boletín oficial de la clave pública del prestador de servicios de certificación o de ciertos datos sobre el certificado raíz (como su "huella dactilar").

22. La firma digital correspondiente a un mensaje, ya sea creada por el firmante para autenticar un mensaje o por un prestador de servicios de certificación para autenticar su certificado, deberá contener por lo general un sello cronológico fiable para que el verificador pueda determinar con certeza si la firma digital se creó durante el "período de validez" indicado en el certificado y, en cualquier caso, si el certificado era válido (es decir, no figuraba en una lista de los revocados) en el momento pertinente, que es una condición para poder verificar una firma digital.

23. Para que una clave pública y su correspondencia con un firmante determinado se puedan utilizar fácilmente en una verificación, el certificado podrá publicarse en un repertorio o difundirse por otros medios. Normalmente, estos repertorios son bases de datos en línea de certificados y de otro tipo de información a las que se puede acceder y que pueden utilizarse para verificar firmas digitales.

24. Una vez expedido, puede que un certificado no sea fiable, por ejemplo si el titular falsifica su identidad ante el prestador de servicios de certificación. En otros casos, un certificado puede ser suficientemente fiable cuando se expide pero dejar de serlo posteriormente. Si la clave privada ha quedado "en entredicho", por ejemplo, si el firmante ha perdido el control de ésta, el certificado puede dejar de ser fiable y el prestador de servicios de certificación (a petición del firmante o aun sin su consentimiento, según las circunstancias), puede suspender (interrumpir temporalmente el período de validez) o revocar (invalidar de forma permanente) el certificado. Oportunamente después de suspender o revocar un certificado, cabe prever que el prestador de servicios de certificación haga pública la revocación o suspensión o notifique este hecho a las personas que soliciten información o de que se tenga conocimiento de que han recibido una firma digital verificable por remisión al certificado que carezca de fiabilidad. Del mismo modo, se debe examinar también, cuando proceda, si corresponde revocar el certificado del prestador de servicios, así como el certificado para verificar la firma de la entidad a cargo de la indicación cronológica en los vales que ésta expida y aquéllos de la entidad

---

[10] *Documentos Oficiales de la Asamblea General, quincuagésimo sexto período de sesiones, Suplemento Nº 17* y corrección (A/56/17 y Corr. 3), párr. 279.

certificadora que hubiera expedido los certificados de dicha entidad encargada de la indicación cronológica.

25. La explotación de las autoridades certificadoras podría estar a cargo de prestadores de servicios del sector privado o de autoridades estatales. En algunos países, por razones de orden público, se prevé que sólo las entidades públicas estén autorizadas para actuar como autoridades certificadoras. Sin embargo, en la mayoría de los países los servicios de certificación se dejan totalmente en manos del sector privado, los prestadores de servicios de certificación administrados por el Estado coexisten con los privados. Existen también sistemas de certificación cerrados, en los que establecen sus propios prestadores de servicios grupos pequeños. En algunos países los prestadores de servicios de certificación de propiedad estatal expiden certificados únicamente para respaldar firmas digitales utilizadas por la administración pública. Sean públicas o privadas estas autoridades certificadoras y deban o no obtener licencia para funcionar, normalmente hay más de una en la ICP. Plantea especial inquietud la relación entre ellas (véanse los párrafos [15] a [18] *supra*).

26. Puede que corresponda al prestador de servicios de certificación o a la autoridad principal asegurar que sus requisitos de política se cumplan de forma permanente. Aunque la elección de las autoridades certificadoras puede basarse en diversos factores, como la solidez de la clave pública utilizada y la identidad del usuario, la fiabilidad del prestador de servicios de certificación puede depender también de su observancia de las normas para expedir certificados y de la precisión con que evalúe los datos recibidos de los usuarios que soliciten certificados. Es de especial importancia el régimen de responsabilidad que se aplique al prestador de servicios de certificación con respecto al cumplimiento, en todo momento, de la política y los requisitos de seguridad de la autoridad principal o del prestador de servicios de certificación superior, o de cualquier otro requisito aplicable. Igualmente importante es la obligación del prestador de servicios de certificación de actuar conforme a las declaraciones que haya hecho sobre sus normas y prácticas, como se prevé en el apartado a) del párrafo 1 del artículo 9 de la Ley Modelo sobre Firmas Electrónicas.

c) Problemas prácticos para establecer la infraestructura de clave pública

27. Pese a los conocimientos considerables sobre las tecnologías de firma digital y su funcionamiento, para implantar en la práctica infraestructuras de clave pública y mecanismos de firma digital han surgido algunos problemas que han impedido utilizar la firma digital conforme a las expectativas.

28. La firma digital funciona bien como un medio para verificar las firmas que se crean durante el período de validez de un certificado. Sin embargo, cuando el certificado caduca o se revoca la clave pública correspondiente pierde validez, aunque no esté en entredicho el par de claves. Por ello, todo mecanismo de ICP requeriría un sistema de gestión de la firma digital para asegurar que la firma siga disponible a lo largo del tiempo. La dificultad principal proviene del riesgo de que los registros electrónicos “originales” (esto es, los dígitos binarios o “bitios” que conforman el fichero informático en que se registra la información), incluida la firma digital, pueden resultar ilegibles o poco fiables con el tiempo, principalmente por la obsolescencia del programa, del equipo físico o de ambos. De hecho, la firma digital podría resultar insegura por los avances científicos en materia de

criptoanálisis; el programa de verificación de las firmas podría faltar durante períodos prolongados, o el documento podría perder su integridad[11]. Por ello, la conservación a largo plazo de la firma electrónica es en general problemática. Aunque por un tiempo se consideró que la firma digital era indispensable a efectos de archivo, la experiencia ha demostrado que no está exenta de riesgos a largo plazo. Como toda modificación del registro posterior al momento de creación de la firma dará lugar a que la verificación no funcione, las operaciones de reformateado destinadas a mantener la legibilidad futura del registro (como la "migración" o la "conversión") pueden afectar a la durabilidad de la firma[12]. En realidad, la firma digital se concibió más para dar seguridad a la comunicación de información que para conservarla[13]. Las iniciativas para superar este problema todavía no han dado con una solución duradera[14].

---

[11] Jean-François Blanchette, "*Defining electronic authenticity*: *An interdisciplinary journey*", disponible en http://polaris.gseis.ucla.edu/blanchette/papers/dsn.pdf, consultado el 5 de abril de 2007 (monografía publicada en un suplemento de las actas de la Conferencia internacional sobre sistemas y redes fiables de 2004, celebrada en Florencia (Italia) del 28 de junio al 1º de julio de 2004, págs. 228 a 232).

[12] "Al fin y al cabo, lo único que se conserva en un contexto electrónico son bitios. Sin embargo desde hace tiempo está claro que es muy difícil mantener indefinidamente un conjunto de bitios. Con el transcurso del tiempo, el conjunto de bitios resulta ilegible (para la computadora y por ello para las personas) por la obsolescencia tecnológica de la aplicación informática y del equipo (es decir, el dispositivo lector). Hasta ahora, el problema de la durabilidad de las firmas digitales basadas en ICP no se ha estudiado bien, por su complejidad .... Aunque los instrumentos de autenticación utilizados anteriormente, como firmas manuscritas, sellos, marchamos, huellas dactilares, etc., también pueden reformatearse (por ejemplo, reproducirse en microfilmes) por la obsolescencia del soporte de papel, no se inutilizan del todo a causa de ello. Siempre queda por lo menos una copia que puede compararse con otros medios de autenticación originales." (Jos Dumortier y Sofie Van den Eynde en *Electronic Signatures and Trusted Archival Services*, pág 5, que figura en (http://www.law.kuleuven.ac.be/icri/publications/172DLM2002.pdf?where, consultado el 5 de abril de 2007.

[13] En 1999, archivistas de varios países pusieron en marcha el proyecto *International Research on Permanent Authentic Records in Electronic Systems* (*InterPARES*) cuyo objetivo era profundizar los conocimientos teóricos y metodológicos indispensables para la conservación a largo plazo de los registros auténticos creados y mantenidos en formato digital (véase http://www.interpares.org/, consultado el 5 de abril de 2007). El proyecto de informe del grupo de trabajo sobre autenticación, que formaba parte de la primera etapa del proyecto, (*InterPARES*1 terminada en 2001) indicaba que la firma digital y la infraestructura de clave pública (ICP) son ejemplos de tecnologías elaboradas y aplicadas como medio de autenticación de registros electrónicos que se transmiten **por el espacio.** Si bien es cierto que los responsables de archivos y los informáticos confían en las tecnologías de autenticación para asegurar la autenticidad de los registros, jamás se pretendió que éstas fueran un medio de asegurar la autenticidad de los registros electrónicos **en el tiempo**, ni son viables actualmente como tales. Este documento está en http://www.interpares.org/documents/atf_draft_final_report.pdf, consultado el 5 de abril de 2007. El informe final de InterPARES1 puede consultarse en http://www.interpares.org/book/index.htm. La continuación del proyecto (*InterPARES*2), tiene por objeto elaborar y enunciar los conceptos, principios, criterios y métodos con los que asegurar la creación y el mantenimiento de registros exactos y fiables y la conservación a largo plazo de registros auténticos en el contexto de las actividades artísticas, científicas y gubernamentales realizadas entre 1999 y 2001.

[14] Por ejemplo, la Iniciativa europea de normas para firmas electrónicas (EESSI), fue lanzada en 1999 por la *Information and Communications Technology Standards Board*, grupo de organizaciones colaboradoras que se ocupa de la normalización y actividades conexas en el ámbito de la tecnología de la información y la comunicación creado para coordinar las

29. Otro ámbito en el que las firmas digitales y los sistemas de ICP pueden plantear problemas prácticos es la seguridad de los datos y la protección de la esfera privada. Los prestadores de servicios de certificación deben mantener a buen recaudo las claves utilizadas para firmar los certificados que expidan a sus clientes, y podrán verse expuestos a tentativas de obtener acceso a las claves sin autorización (véase también la segunda parte, párrafos [...] a [...], *infra*. Además, los prestadores de servicios de certificación tienen que obtener una serie de datos personales y comerciales de las personas que soliciten certificados, y archivarlos a efectos de consulta futura. Además, deben adoptar las medidas pertinentes para que el acceso a dicha información se ajuste a las leyes aplicables en materia de protección de los datos[15]. No obstante, el acceso no autorizado a los datos sigue siendo una amenaza real.

---

iniciativas en materia de normalización a fin de apoyar la aplicación de la Directiva de la Unión Europea sobre la firma electrónica (véase la nota [...] [Diario Oficial de las Comunidades Europeas, L/13/12]. El consorcio de la EESSI (iniciativa de normalización con la que se procura plasmar los requisitos de la directiva europea sobre la firma electrónica en normas europeas) ha procurado satisfacer la necesidad de asegurar la conservación a largo plazo de los documentos firmados criptográficamente, mediante su norma sobre el formato de firma electrónica (*Electronic Signature Formats* ES 201 733, ETSI 2000). En el formato se distingue entre los momentos de validación de la firma: la validación inicial y la validación posterior. El formato de ésta última abarca toda la información que puede utilizarse en su momento en el trámite de validación, como la relativa a la revocación, la indicación de fecha y hora, las políticas de firma, etc. Esta información se reúne en la etapa de validación inicial. Preocupaba a los creadores de estos formatos de firma electrónica el riesgo de seguridad para la validez de la firma por la degradación de la clave criptográfica. Como salvaguardia contra este riesgo de degradación, las firmas de la EESSI se estampan periódicamente con indicación de fecha y hora, ajustando los algoritmos de firma y el tamaño de la clave a los métodos modernos de análisis criptográfico. El problema de la longevidad de los programas informáticos se abordó en un informe de 2000 de la EESSI, en que se presentaron los "servicios de archivo 'fiables'", ("*trusted archival services*"), un tipo nuevo de servicio comercial que prestarían órganos y gremios profesionales competentes aún no determinados para garantizar la conservación a largo plazo de los documentos firmados criptográficamente. En el informe se enumeran varios requisitos técnicos que deberían cumplir estos servicios de archivo, entre ellos la "retrocompatibilidad" con el equipo y los programas informáticos, mediante la conservación de este equipo o la emulación (véase Blanchette, "*Defining electronic authenticity* ..." nota [12]). En el sitio http://www.law.kuleuven.ac.be/icri/publications/91TAS-Report.pdf?where=, consultado el 12 de abril de 2007, figura un estudio de seguimiento sobre la recomendación de la EESSI acerca de los servicios de archivo fiables, realizado por el Centro interdisciplinario de derecho y tecnología de la información de la Universidad Católica de Lovaina (Bélgica), titulado *European Electronic Signature Standardization Initiative: Trusted Archival Services* (tercera etapa, informe final, 28 de agosto de 2000). La EESSI se dio por terminada en octubre de 2004. No parece hallarse en funciones actualmente ningún sistema para aplicar estas recomendaciones (véase Dumortier y Van den Eynde, *Electronic Signatures and Trusted Archival Services* (véase la nota [13]).

[15] Véase Organización de Cooperación y Desarrollo Económicos (OCDE), *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, (París, 1980), que puede encontrarse en http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html, consultado el 7 de febrero de 2007; el Convenio para la protección de las personas en relación con el proceso automático de datos personales, del Consejo de Europa, *European Treaty Series*, Nº 108), que puede encontrarse en http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm, consultado el 7 de febrero de 2007; los Principios rectores sobre la utilización de ficheros computarizados de datos personales de las Naciones Unidas (resolución 45/95 de la Asamblea General), que figura en http://193.194.138.190/html/menu3/b/71.htm, consultado el 7 de febrero de 2007; y la

2. Biométrica

30. La medición biométrica se utiliza para identificar a una persona por sus rasgos físicos o de comportamiento intrínsecos. Los rasgos que pueden utilizarse para el reconocimiento biométrico son el ADN, las huellas dactilares, el iris, la retina, la geometría de las manos o el rostro, el termograma facial, la forma de la oreja, la voz, el olor corporal, la configuración de los vasos sanguíneos, la letra, el modo de andar y la forma de mecanografiar.

31. La utilización de dispositivos biométricos supone por lo general captar una muestra biométrica de algún rasgo biológico de una persona. Esta muestra tiene forma digital. A continuación se extraen datos biométricos de esa muestra para crear una plantilla de referencia. Por último, los datos biométricos almacenados en esa plantilla se comparan con los obtenidos del usuario final a efectos de verificación, para que se pueda indicar si se ha logrado o no la identificación o la verificación de la identidad[16].

32. Por su naturaleza, los dispositivos biométricos tienen características especiales que se deben tener debidamente en cuenta. Estas características, que pueden diferir en alguna medida según el rasgo elegido como referencia, repercuten considerablemente en la idoneidad de la tecnología para la aplicación prevista.

33. Algunos de los riesgos que se plantean guardan relación con el almacenamiento de los datos biométricos, porque las pautas biométricas son por lo general irrevocables. Si la integridad de los sistemas biométricos ha resultado comprometida, el usuario legítimo no tiene otra opción que la de revocar los datos de identificación y cambiarse a otro conjunto de datos de identificación intactos. Por ello, se necesitan reglas especiales para impedir el uso indebido de las bases de datos biométricas.

34. Las técnicas biométricas no pueden ser absolutamente exactas, pues los rasgos biológicos tienden a ser intrínsecamente variables, por lo que toda medición puede tener un margen de error. Al respecto, la biométrica no se considera un factor identificador exclusivo, sino semiexclusivo. A fin de reflejar estas variaciones, puede manipularse la exactitud de la biométrica fijando un umbral de correlación para cotejar la plantilla de referencia con la muestra extraída. Sin embargo, un umbral bajo de correlación puede sesgar el ensayo induciendo una aceptabilidad falsa, mientras que uno elevado tal vez tienda a inducir rechazos erróneos. Sin embargo, la exactitud de la autenticación basada en métodos biométricos puede resultar apropiada en la mayoría de las aplicaciones comerciales.

35. Además, se plantean cuestiones relativas a la protección de los datos y los derechos humanos en lo tocante al almacenamiento y la divulgación de datos

---

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Diario Oficial de las Comunidades Europeas, L 281, de 23 de noviembre de 1995), que figura en (http://eurlex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett, consultado el 7 de febrero 2007).

[16] *International Association for Biometrics (iAfB)* e *International Computer Security Association (ICSA)1999 Glossary of Biometric Terms* que figura en http://www.afb.org.uk/docs/glossary.htm, consultado el 7 de febrero de 2007.

biométricos. Las leyes sobre protección de los datos[17], aunque no hagan referencia expresa a los sistemas biométricos, tienen por objeto proteger los datos personales de las personas físicas, cuyo procesamiento, a la vez en su forma primaria y como plantillas, es la base de la tecnología biométrica[18]. Además, tal vez se requieran medidas para proteger a los consumidores del riesgo de la utilización privada de datos biométricos y del eventual robo de identidad. Pueden entrar en juego también otros ámbitos jurídicos, como la legislación laboral y en materia de salud[19].

36. Los medios técnicos pueden ayudar a abordar algunas preocupaciones. Por ejemplo, el almacenamiento de datos biométricos en tarjetas o fichas con memoria puede salvaguardarlos de la posibilidad de acceso no autorizado si se almacenan en un sistema informático centralizado. Además, se han creado prácticas óptimas para reducir riesgos en distintos ámbitos, como el alcance y las capacidades; la protección de los datos, el control de los datos personales por el usuario; y la divulgación, auditoría, rendición de cuentas y supervisión[20].

37. Se considera en general que los dispositivos biométricos brindan un elevado grado de seguridad. Aunque resultan compatibles con una diversidad de usos, en la actualidad los utilizan principalmente los gobiernos, en particular los servicios de seguridad, como los permisos de inmigración y los controles de acceso.

38. También se han elaborado aplicaciones comerciales, en que se utiliza con frecuencia la biométrica en el contexto de un procedimiento de autenticación basado en dos factores, que exige la presentación de un elemento biométrico que la persona tiene en su poder y otro que esa persona conoce (por lo general, una contraseña o un NIP). Además, se han creado aplicaciones para guardar en memoria y comparar las características de una firma manuscrita. Se registra en tablillas digitales la presión de la pluma de escribir y el tiempo que se tarda en firmar. Los datos se almacenan luego en forma algoritmo que servirá a efectos de comparación con firmas futuras. No obstante, por las características intrínsecas de la biométrica, se deben tener presentes los peligros del aumento gradual y descontrolado de su uso en operaciones comerciales corrientes.

39. Si se utiliza la firma biométrica como sustituto de la firma manuscrita, puede plantearse un problema relativo a la prueba. Como se señaló antes, la fiabilidad de la prueba biométrica varía según las tecnologías utilizadas y el margen aceptado de reconocimiento erróneo. Además, existe la posibilidad de que se manipulen indebidamente o se falsifiquen los datos biométricos memorizados en formato digital.

---

[17] Véase la nota [15].

[18] Paul de Hert, "*Biometrics: Legal Issues and Implications,* documento de antecedentes para el Instituto de Estudios Tecnológicos Prospectivos de la Comisión Europea (Centro Común de Investigación de la Dirección General de las Comunidades Europeas, 2005), pág. 13 http://cybersecurity.jrc.es/docs/LIBE%20Biometrics%20March%2005/LegalImplications_Paul_de_Hert.pdf.

[19] Por ejemplo, en el Canadá, se examinó la utilización de la biométrica con respecto a la aplicación de la Ley de Protección de la Información Personal y Documentos Electrónicos (2000, cap. 5) en el lugar de trabajo (véase *Turner v. TELUS Communications Inc*., 2005 FC 1601, 29 de noviembre de 2005 (Tribunal Federal del Canadá).

[20] Como ejemplo de prácticas óptimas, véase la *Bio Privacy Initiative, Best Practices for Privacy-Sympathetic Biometric Deployment*, del Grupo Biométrico Internacional que puede consultarse en http://www.bioprivacy.org/.

40. Pueden aplicarse a la utilización de firmas biométricas los mecanismos generales para verificar la fiabilidad previstos en la Ley Modelo de la CNUDMI sobre Firmas Electrónicas[21] y la Ley Modelo de la CNUDMI sobre Comercio Electrónico[22], así como en la más reciente Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales[23]. Para asegurar la uniformidad, también podría ser útil elaborar directrices internacionales sobre el uso y la gestión de métodos biométricos[24]. Debe estudiarse con atención si estas normas serían prematuras habida cuenta del grado de desarrollo actual de las tecnologías biométricas, y si ello no obstaculizaría el avance de éstas.

3. Contraseñas y métodos híbridos

41. Para controlar el acceso a información o servicios y para "firmar" comunicaciones electrónicas se utilizan contraseñas y códigos. En la práctica, este último uso es menos frecuente, por el riesgo de poner en entredicho el código si se transmite en mensajes no cifrados. Como fuere, las contraseñas y los códigos son el método de "autenticación" más utilizado a efectos del control del acceso y la verificación de la identidad en una diversidad de operaciones, incluidas casi todas las bancarias por Internet, la retirada de efectivo en cajeros automáticos y las compras con tarjeta de crédito.

42. Cabe reconocer que es posible utilizar muchas tecnologías para "autenticar" una operación electrónica. En una operación determinada pueden emplearse varias de ellas o diversas versiones de la misma. Por ejemplo, la dinámica de la firma a efectos de autenticación puede conjugarse con criptografía para ratificar la integridad del mensaje. Opcionalmente, pueden transmitirse contraseñas por Internet mediante criptografía (por ejemplo, el SSL en los navegadores) para protegerlas, conjuntamente con la utilización de sistemas biométricos para crear una firma digital (criptografía asimétrica), que al recibirse genera un justificante de autenticación del protocolo Kerberos (criptografía simétrica). Al elaborar marcos jurídicos y normativos para reglamentar estas tecnologías, se deberá prestar atención a las de carácter múltiple. Los marcos jurídicos y normativos de los sistemas de autenticación electrónica deberán tener flexibilidad suficiente para abarcar tecnologías híbridas, porque los que se centran expresamente en tecnologías específicas pueden obstaculizar la utilización de las tecnologías múltiples[25]. La

---

[21] (Véase la nota [...]) [Publicación de las Naciones Unidas, Nº de venta S.02.V.8].

[22] (Véase la nota [...]) [Publicación de las Naciones Unidas, Nº de venta S.99.V.4].

[23] La Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales fue finalizada por la CNUDMI en su 38º período de sesiones (Viena, 4 a 15 de julio de 2005), y aprobada oficialmente por la Asamblea General el 23 de noviembre de 2005 (resolución 60/21 de la Asamblea General, anexo) que puede consultarse en http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention.html.

[24] Éstas podrían compararse con los criterios de fiabilidad expuestos en la "Guía para la incorporación al derecho interno de la Ley Modelo de la CNUDMI sobre Firmas Electrónicas (véase la nota [...] [Publicación de las Naciones Unidas, Nº de venta S.02.V.8), párrafo 75].

[25] *Foundation for Information Policy Research, Signature Directive Consultation Compilation*, 28 de octubre de 1998, en que figura una recopilación de las respuestas presentadas durante las consultas sobre la Directiva de la Unión Europea acerca de la firma electrónica, preparada a petición de la Comisión Europea, y que figura en www.fipr.org/publications/sigdirecon.html, consultado el 12 de abril de 2007.

aceptación de estos criterios tecnológicos híbridos se facilitaría mediante disposiciones neutrales respecto de las tecnologías.

4. Firmas escaneadas y nombres mecanografiados

43. La razón principal del interés legislativo por el comercio electrónico en la esfera del derecho privado ha sido la inquietud respecto del efecto que las nuevas tecnologías pueden tener en la aplicación de normas de derecho concebidas para otros medios. Esta atención a la tecnología ha conducido con frecuencia, deliberadamente o no, a centrarse en tecnologías avanzadas que hacen más seguros los métodos de autenticación y firma electrónicas. En ese contexto suele perderse de vista que muchas de las comunicaciones mercantiles en el mundo, cuando no la mayoría, no utilizan ninguna tecnología concreta de autenticación o firma.

44. En la práctica cotidiana, las empresas de todo el mundo se consideran satisfechas, por ejemplo, intercambiando correos electrónicos sin ningún tipo de autenticación o firma que no sea el nombre mecanografiado, el título y la dirección de las partes al pie de sus comunicaciones. En ocasiones se da a ellas un aspecto más oficial utilizando imágenes de firmas manuscritas reproducidas en facsímil o escaneadas, lo que, desde luego, constituye únicamente una copia digitalizada del original manuscrito. Ni los nombres mecanografiados en correos electrónicos sin cifrar ni las firmas escaneadas brindan mucha seguridad ni sirven para demostrar categóricamente la identidad del iniciador de la comunicación electrónica en que figuren. Sin embargo, las empresas deciden libremente utilizar estas formas de "autenticación" en aras de la facilidad, la conveniencia y la economía de las comunicaciones. Es importante que los legisladores y los responsables de formular las políticas tengan presentes estas prácticas mercantiles generalizadas al examinar la reglamentación de la autenticación y la firma electrónicas. Todo requisito estricto al respecto, en particular la imposición de un método o tecnología determinados, puede poner inadvertidamente en duda la validez y aplicabilidad de un número considerable de operaciones que se realizan todos los días sin utilizar ningún tipo de autenticación o firma. Ello, a la vez, puede incitar a las partes de mala fe a eludir las obligaciones que hayan asumido libremente impugnando la autenticidad de sus propias comunicaciones electrónicas. No es realista prever que la imposición de requisitos relativamente estrictos en materia de autenticación y firma haría que todas las partes los aplicaran cotidianamente. Las experiencias recientes con métodos avanzados, como la firma digital, ha demostrado que los problemas relativos a sus costos y su complejidad limitan con frecuencia la utilidad práctica de las técnicas de autenticación y firma.

C. Utilización de la identidad electrónica*

45. En el ámbito electrónico, las personas físicas o jurídicas pueden recurrir a diversos prestadores de servicios. Cuando una persona se inscribe con uno ellos para utilizar dichos servicios, se crea una "identidad" electrónica. Además, una sola identidad puede vincularse a diversas cuentas, correspondientes a cada aplicación o plataforma. La multiplicidad de identidades y cuentas puede dificultar su utilización

* Esta sección se ampliará en una versión definitiva del documento general de consulta.

tanto para el usuario como para el prestador de servicios. Estas dificultades pueden evitarse si se crea una identidad electrónica única para cada persona.

46. La inscripción ante un prestador de servicios y la creación de una identidad electrónica supone establecer una relación de confianza mutua entre la persona y el prestador. La creación de una identidad electrónica única requiere conjugar estas relaciones bilaterales en un marco más amplio que permita su gestión conjunta, en lo que se denomina gestión de la identidad. Entre las ventajas de ésta pueden figurar desde la perspectiva del prestador, mejoras de la seguridad, la facilitación del cumplimiento de las normas pertinentes y la agilización de las operaciones comerciales, así como, desde el punto de vista del usuario, la facilitación del acceso a la información.

47. Cabría describir la gestión de la identidad en el contexto de los dos enfoques siguientes: el paradigma tradicional de acceso del usuario (conexión, o *log-on*), basado en una tarjeta con memoria y los datos conexos que usa el cliente para conectarse a un servicio, y el paradigma de servicio innovador, basado en un sistema por el que se prestan servicios personalizados a los usuarios y a sus dispositivos.

48. El criterio de la gestión de la identidad basado en el acceso del usuario se centra en la administración de la autenticación del usuario, los derechos de acceso, las restricciones a éste, los perfiles de las cuentas, las contraseñas y otros atributos de uno o varios sistemas o aplicaciones. El objetivo es facilitar y controlar el acceso a las aplicaciones y los recursos y proteger al mismo tiempo la información personal y comercial confidencial frente a posibles usuarios no autorizados.

49. Conforme al criterio basado en el paradigma de servicios, el alcance de la gestión de la identidad se amplía y comprende todos los recursos de la empresa que se utilizan para prestar servicios en línea, como el equipo de la red, los servidores, los portales, el contenido, las aplicaciones y los productos, así como las credenciales, las libretas de direcciones, las preferencias y los derechos del usuario. En la práctica, ello puede incluir, por ejemplo, información relativa a las configuraciones de control de acceso establecidas por los padres y la participación en programas de fidelización.

50. Se impulsan iniciativas para ampliar la utilización de la gestión de la identidad en el plano empresarial y estatal. Sin embargo, cabe señalar que las opciones de política en las situaciones respectivas pueden ser muy diferentes. Concretamente, el criterio estatal puede orientarse más a atender mejor las necesidades de los ciudadanos, y por ello predisponerse a la interacción con personas naturales. En cambio, en las aplicaciones comerciales se debe tener presente la utilización cada vez mayor de máquinas automáticas en las operaciones comerciales, y por ello tal vez se deban adoptar elementos destinados a prever las exigencias concretas que plantean dichas máquinas.

51. Algunas de las dificultades observadas en los sistemas de gestión de la identidad son las preocupaciones relacionadas con la esfera privada derivadas de los riesgos que entraña la utilización indebida de identificadores exclusivos. Además, pueden plantearse problemas por las diferencias en las normas legales vigentes, en particular con respecto a la posibilidad de delegar la facultad de actuar en nombre de otra persona. Se han propuesto soluciones basadas en la cooperación empresarial voluntaria, dentro de lo que se llama un círculo de confianza, cuyos miembros están

obligados a confiar en la corrección y exactitud de la información que les presenten otros miembros. Sin embargo, tal vez este enfoque no baste para reglamentar todas las cuestiones conexas, y requiera la adopción de un marco jurídico[26]. Además, se prepararon directrices para establecer los requisitos legales que debería cumplir un círculo de infraestructuras de confianza[27].

52. Con respecto a la interoperabilidad técnica, la Unión Internacional de Telecomunicaciones (UIT) creó un Grupo Temático sobre gestión de identidades, para facilitar y promover la creación de un marco genérico [de gestión de identidades] y de mecanismos para divulgar identidades autónomas distribuidas, así como federaciones de identidades y su aplicación[28].

53. Además, se están presentando soluciones de gestión de la identidad en el contexto del gobierno electrónico. Por ejemplo, en el marco de la iniciativa de la Unión Europea titulada "i2010: una sociedad de la información europea para el crecimiento y el empleo" se puso en marcha un estudio sobre la materia para promover un enfoque coherente de la gestión de la identidad electrónica en el gobierno electrónico en el ámbito de la Unión Europea, basado en los conocimientos especializados existentes y en iniciativas de los Estados miembros de la Unión Europea[29].

54. Se ha hecho cada vez más habitual la distribución de dispositivos de firma electrónica, a menudo en forma de tarjetas con memoria, en el contexto de iniciativas de gobierno electrónico. Se han puesto en marcha campañas nacionales de distribución de estas tarjetas, entre otros países en Bélgica[30] y en Estonia. De resultas de estas iniciativas, muchos ciudadanos han recibido dispositivos que, entre otras cosas, les permiten utilizar firmas electrónicas a bajo costo. Aunque el objetivo principal de estas iniciativas tal vez no sea comercial, estos mecanismos pueden utilizarse igualmente en el ámbito comercial. Cada vez se reconoce más la convergencia de los dos ámbitos de aplicación[31].

---

[26] Véase *Modinis Study on Identity Management in eGovernment: Identity Management Issue Report* (Dirección General de Sociedad de la Información y Medios de Comunicación de la Comisión Europea, junio de 2006), págs. 9 a 12, que puede consultarse en https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/pub/Main/ProjectDocs/modinis.D3.9_Identity_Management_Issue_Interim_Report_II1.pdf.

[27] El Liberty Alliance Project (véase www.projectliberty.org) es una alianza de más de 150 empresas, organizaciones sin fines de lucro y entidades gubernamentales de todo el mundo. Este consorcio está empeñado en establecer una norma abierta de identidad federada de red que pueda utilizarse en la red con todos los dispositivos existentes y nuevos. La identidad federada da a empresas, gobiernos, empleados y consumidores la posibilidad de controlar, en condiciones más cómodas y seguras, la información sobre la identidad en la economía digital de la actualidad, y es un factor determinante para impulsar la utilización del comercio electrónico y los servicios de datos personalizados, así como los servicios basados en la web. Pueden afiliarse a ella todas las organizaciones comerciales y no comerciales.

[28] Véase http://www.itu.int/ITU-T/studygroups/com17/fgidm/index.html.

[29] Véase https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi.

[30] Véase http://eid.belgium.be/en/navigation/12000/index.html.

[31] Véase, por ejemplo, *2006 Korea Internet White Paper* (serie Organismo Nacional de Desarrollo de Internet de Corea, 2006) pág. 81, en que se alude a la doble utilización en aplicaciones de gobierno electrónico y comercio electrónico de la Ley de firmas electrónicas de la República de Corea, que puede consultarse en http://www.ecommerce.or.kr/activities/documents_view.asp?bNo=642&Page=1.