NACIONES UNIDAS

A

Asamblea General

Distr.
GENERAL

A/CN.9/WG.IV/WP.71
31 de diciembre de 1996

ESPAÑOL
Original: INGLÉS

COMISIÓN DE LAS NACIONES UNIDAS PARA
EL DERECHO MERCANTIL INTERNACIONAL
Grupo de Trabajo sobre Comercio Electrónico
31° período de sesiones
Nueva York, 18 a 28 de febrero de 1997

PLANIFICACIÓN DE LA LABOR FUTURA SOBRE COMERCIO ELECTRÓNICO: FIRMAS DIGITALES, AUTORIDADES CERTIFICADORAS Y ASUNTOS JURÍDICOS CONEXOS

Nota de la Secretaría

ÍNDICE

INTRODUCCIÓN

1. Tras la aprobación de la Ley Modelo de la CNUDMI sobre Comercio Electrónico, la Comisión, en su 29º período de sesiones, hizo un examen de la labor futura en la esfera del comercio electrónico, en base a deliberaciones preliminares que tuvieron lugar en el seno del Grupo de Trabajo sobre Intercambio Electrónico de Datos en su 30º período de sesiones (A/CN.9/421, párrs. 109 a 119). Hubo acuerdo general en que la CNUDMI debía continuar su labor de preparación de normas jurídicas que introdujeran un elemento de previsibilidad al comercio electrónico, aumentando de esta manera el comercio en todas las regiones.

2. Se hicieron nuevas propuestas en cuanto a posibles temas y prioridades de la labor futura. Una de éstas era que la Comisión iniciara la preparación de normas sobre firmas digitales. Se dijo que la promulgación de leyes sobre firmas digitales, junto con leyes que reconocieran las actividades de las "autoridades de certificación" (en adelante denominadas "autoridades certificadoras"), u otras personas autorizadas a emitir certificados electrónicos u otras formas de garantía en cuanto al origen y la atribución de los mensajes "firmados" en forma digital, era considerada en muchos países como un elemento esencial del desarrollo del comercio electrónico. Se señaló que la posibilidad de confiar en firmas digitales sería fundamental para el crecimiento de la contratación, así como para la posibilidad de transferir derechos sobre mercancías u otros intereses por medios electrónicos. En muchas jurisdicciones se estaban preparando nuevas leyes relativas a las firmas digitales. Se informó de que el desarrollo de esas leyes ya era no uniforme. Si la Comisión decidiera emprender la labor en esa esfera, tendría una oportunidad para armonizar las nuevas leyes, o por lo menos para establecer principios comunes en el campo de las firmas electrónicas, proporcionando de esta forma una infraestructura internacional a dicha actividad comercial.

3. Se expresó un apoyo considerable a la propuesta. Ahora bien, el sentimiento general fue que si la Comisión decidía iniciar la labor en el campo de las firmas digitales por conducto de su Grupo de Trabajo sobre Intercambio Electrónico de Datos, debía dar a este grupo un mandato preciso. Se expresó también la opinión de que, como era imposible que la CNUDMI se dedicara a preparar normas técnicas, había que tener cuidado para que la Comisión no se viera envuelta en las cuestiones técnicas relativas a las firmas digitales. Se recordó que el Grupo de Trabajo, en su 30º período de sesiones, había reconocido la posible necesidad de realizar algunos trabajos sobre las autoridades certificadoras, y que dicha labor probablemente debiera realizarse en el contexto de los registros y los proveedores de servicios. Ahora bien, el Grupo de Trabajo convino también en que no debía embarcarse en ningún examen técnico relativo a las ventajas de utilizar normas determinadas (A/CN.9/421, párr. 111). Se expresó preocupación porque la labor sobre firmas digitales pudiera superar el ámbito del derecho mercantil y abarcar también cuestiones generales de derecho civil o administrativo. A esto se respondió que lo mismo sucedía con las disposiciones de la Ley Modelo, y que la Comisión no debía dejar de preparar reglas útiles simplemente porque esas reglas podían también ser útiles más allá del ámbito de las relaciones comerciales.

4. Otra propuesta, basada en las deliberaciones preliminares celebradas por el Grupo de Trabajo, fue que la labor futura se centrara en los proveedores de servicios. A este respecto, se mencionaron como posibles objeto de estudio las normas mínimas de ejecución en ausencia de un acuerdo entre las partes, el alcance del riesgo asumido por los destinatarios definitivos, la validez de esas reglas o acuerdos frente a terceros, la asignación de los riesgos de intervenciones pirata o de otros actos no autorizados, y el alcance de las garantías obligatorias, de haber alguna, o de otras obligaciones contraídas al prestar servicios con valor añadido (véase A/CN.9/421, párr. 116).

5. Se opinó en general que sería apropiado que la CNUDMI examinara la relación entre los proveedores de servicios, los usuarios y los terceros interesados. Se dijo que sería importante dirigir esa actividad hacia el desarrollo de normas y directrices internacionales de conducta comercial en esa

esfera, con miras a favorecer el comercio por conducto de medios electrónicos, en vez de adoptar como meta el establecimiento de un régimen reglamentario para los proveedores de servicios u otros reglamentos que pudieran ocasionar gastos inaceptables para la aplicación comercial del EDI (véase A/CN.9/421, párr. 117). Ahora bien, se expresó también la opinión de que el tema de los proveedores de servicios podría ser demasiado amplio y abarcar demasiadas situaciones de hecho diferentes que impedirían tratarlo como un tema único. Se convino en general en que las cuestiones relativas a los proveedores de servicios podrían ser tratadas en el contexto de cada nueva esfera de trabajo de la que se ocupara el Grupo de Trabajo.

6. Otra propuesta fue que la Comisión iniciara la preparación de las nuevas normas de carácter general que se necesitaban para aclarar cómo se podían realizar las funciones tradicionales de los contratos por medio del comercio electrónico. Se dijo que abundaban las incertidumbres en cuanto al significado de "ejecución", "entrega" y otros términos en el contexto del comercio electrónico, en el que la oferta, la aceptación y la entrega del producto de podían realizar en redes de computadoras abiertas en todo el mundo. El rápido crecimiento del comercio basado en las computadoras, así como las transacciones a través de la Internet y otros sistemas habían dado prioridad a este tema. Se sugirió que la Secretaría preparara un estudio para aclarar el alcance de esta labor. Si la Comisión, tras haber examinado el estudio, decidiera emprender esta tarea, una opción sería incluir dichas normas en la sección de "Disposiciones especiales" de la Ley Modelo de la CNUDMI sobre comercio electrónico.

7. Otra propuesta fue que la Comisión centrara su atención en la cuestión de la incorporación por remisión. Se recordó que en el Grupo de Trabajo se había acordado que sería conveniente tratar ese tema en el contexto de la labor más general sobre las cuestiones de los registros y los proveedores de servicios (A/CN.9/421, párr. 114). La Comisión convino en general en que la cuestión se podría tratar en el contexto de la labor sobre autoridades certificadoras.

8. Tras las deliberaciones pertinentes, la Comisión convino en que era conveniente incluir la cuestión de las firmas digitales y las autoridades certificadoras en el programa de la Comisión, siempre que esto se utilizara como una oportunidad para tratar los otros temas sugeridos por el Grupo de Trabajo para la labor futura. En cuanto a la necesidad de dar un mandato más preciso al Grupo de Trabajo, se convino también en que las normas uniformes que se habrían de preparar debían incluir cuestiones tales como la base jurídica para apoyar los procesos de certificación, incluidas las incipientes tecnologías de autentificación y certificación digital, la aplicabilidad de los procesos de certificación, la asignación de los riesgos y las responsabilidades de los usuarios, los proveedores y los terceros interesados en el contexto de la utilización de técnicas de certificación, las cuestiones específicas de la certificación mediante el empleo de registros, y la incorporación por remisión.

9. La Comisión pidió a la Secretaría que preparara un estudio de antecedentes sobre las cuestiones de las firmas digitales y los proveedores de servicios, sobre la base de un análisis de las leyes que se estaban preparando en diversos países. Teniendo a la vista ese estudio, el Grupo de Trabajo examinaría la conveniencia y viabilidad de preparar normas uniformes sobre los temas mencionados más arriba. Se convino en que la labor del Grupo de Trabajo en su 31° período de sesiones podía comprender la preparación de proyectos de normas sobre algunos de los aspectos de los temas mencionados más arriba. Se pidió al Grupo de Trabajo que proporcionara a la Comisión elementos suficientes para adoptar una decisión fundamentada en cuanto al ámbito de las normas uniformes que se prepararían. En vista del ámbito amplio de las actividades abarcadas por la Ley Modelo de la CNUDMI sobre Comercio Electrónico y por la posible labor futura en esta esfera, se decidió cambiar el nombre del

Grupo de Trabajo sobre Intercambio Electrónico de Datos a "Grupo de Trabajo sobre Comercio Electrónico"1/.

10. La presente nota contiene un estudio preliminar de la cuestión de las firmas digitales y cuestiones conexas. Se preparó teniendo como antecedente la Ley Modelo de la CNUDMI sobre Comercio Electrónico, y teniendo en cuenta también los textos legislativos recientemente adoptados o que se estaban preparando en diversos países. En el estudio se aprovechó también la labor de otras organizaciones, en particular el proyecto de prácticas internacionales uniformes sobre autentificación y certificación que prepara la Cámara de Comercio Internacional (CCI), y las directrices sobre firmas digitales publicadas por la American Bar Association, y los resultados de una reunión de un grupo especial de expertos en la que participaron expertos en la esfera de las firmas digitales y de la secretaría de la CNUDMI.

11. De conformidad con instrucciones recientes relativas a un control más estricto y a la limitación de la documentación de las Naciones Unidas, las observaciones aclaratorias de los proyectos de disposiciones son tan breves como es posible. Las explicaciones adicionales se darán en forma oral.

I. OBSERVACIONES GENERALES SOBRE FIRMAS DIGITALES

A. Funciones de las firmas

12. El artículo 7 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico se basa en el reconocimiento de las funciones que cumple una firma manuscrita en papel. Durante la preparación de la Ley Modelo, el Grupo de Trabajo examinó las siguientes funciones tradicionales de las firmas manuscritas: identificar a una persona, proporcionar la certidumbre en cuanto a su participación personal en el acto de la firma, y vincular a esa persona con el contenido de un documento. Se señaló además que una firma podría cumplir otras diversas funciones, según cual fuera la naturaleza del documento firmado. Por ejemplo, una firma podría constituir un testimonio de la intención de una parte de considerarse vinculada por el contenido de un contrato firmado, de la intención de una persona de respaldar la autoría de un texto, de la intención de una persona de asociarse al contenido de un documento escrito por otra persona, y del hecho de que una persona estaba en un lugar determinado a una hora determinada.

13. En un medio electrónico, el original de un mensaje no se puede distinguir de una copia, no lleva una firma manuscrita y no está impreso en papel. El potencial de fraude es considerable, debido a la facilidad con que se pueden interceptar y alterar datos en forma electrónica sin posibilidad de detección, y a la velocidad con que se procesan transacciones múltiples. La finalidad de las diversas técnicas que ya están disponibles en el mercado o que se están desarrollando es ofrecer los medios técnicos para que algunas o todas las funciones identificadas como características de las firmas manuscritas se puedan cumplir en un medio electrónico. Estas técnicas se pueden denominar, en general, "firmas electrónicas".

1/ Documentos Oficiales de la Asamblea General, quincuagésimo primer período de sesiones, Suplemento No. 17 (A/51/17), párrs. 216 a 224.

B. Firmas digitales y otras firmas electrónicas

14. Al examinar la conveniencia y viabilidad de preparar reglas jurídicas uniformes para las firmas digitales, y con miras a ayudar a la Comisión en su examen del alcance de esas posibles reglas uniformes, el Grupo de Trabajo quizá desee examinar las diversas técnicas ya disponibles o en desarrollo, cuya finalidad es proporcionar equivalentes funcionales de las firmas manuscritas y otras formas de mecanismos de autentificación que se utilizan en un medio basado en el papel.

1. Las firmas electrónicas basadas en técnicas distintas de la criptografía de clave pública

15. Cabe recordar que, además de las "firmas digitales" basadas en la criptografía de clave pública, que constituye el tema principal de esta nota, hay otros diversos dispositivos, con frecuencia denominados mecanismos de "firma electrónica" que ya se están utilizando o que se prevé utilizar en el futuro y que permiten cumplir una o más de las funciones de las firmas manuscritas mencionadas anteriormente. Por ejemplo, ciertas técnicas se basarían en la autentificación mediante un dispositivo biométrico basados en las firmas manuscritas. Con este dispositivo, se firmaría en forma manual utilizando un lápiz especial en una pantalla de computadora o en un bloque digital. La firma manuscrita sería luego analizada por la computadora y almacenada como un conjunto de valores numéricos que se podrían agregar a los datos de un mensaje y recuperar en pantalla para que el receptor pudiera autentificar la firma. Este sistema de autentificación exige el análisis previo de muestras de firmas manuscritas y su almacenamiento utilizando el dispositivo biométrico.

16. El Grupo de Trabajo quizá desee considerar si el ámbito de su labor debería ampliarse para abarcar las firmas electrónicas en general. Dicha labor exigiría a la Secretaría la realización de más investigaciones para determinar las consecuencias técnicas y jurídicas de utilizar dispositivos de "firmas" basados en técnicas distintas de la criptografía de clave pública. La presente nota hace hincapié en las cuestiones relacionadas con las firmas digitales basadas en la criptografía de clave pública en vista de la disponibilidad de información preliminar suficiente en cuanto a las consecuencias jurídicas de las firmas digitales, y a la existencia de proyectos de leyes sobre este tema en un cierto número de países.

17. El Grupo de Trabajo, al examinar la conveniencia y viabilidad de preparar normas uniformes aplicables tanto a las firmas digitales como a otras formas de firmas electrónicas, quizá desee considerar si la CNUDMI debe intentar el desarrollo de normas uniformes a un nivel intermedio entre el nivel muy general de la Ley Modelo y las normas más concretas que tratan de los aspectos específicos de una o más técnicas determinadas. En todo caso, y en consonancia con la neutralidad de la Ley Modelo en cuanto a los medios, esas normas uniformes, si se refirieran a las firmas digitales, no deberían desalentar la utilización de otros métodos.

2. Las firmas digitales basadas en la criptografía de clave pública2/

a) Terminología y conceptos técnicos

2/ Numerosos elementos de la descripción del funcionamiento de un sistema de firmas digitales incluidos en esta sección se basan en las directrices sobre firmas digitales de la ABA (American Bar Association), págs. 8 a 17.

i) Criptografía

18. Las firmas digitales se crean y verifican utilizando la criptografía, la rama de las matemáticas aplicadas que se ocupa de transformar mensajes en formas aparentemente ininteligibles y devolverlas a su forma original. Las firmas digitales utilizan lo que se denomina "criptografía de clave pública", que con frecuencia se basa en el empleo de funciones algorítmicas para generar dos "claves" diferentes pero matemáticamente relacionadas entre sí (por ejemplo, grandes números producidos utilizando una serie de fórmulas matemáticas aplicadas a números primarios). Una de esas claves se utiliza para crear una firma digital o transformar datos en una forma aparentemente ininteligible, y la otra para verificar una firma digital o devolver el mensaje a su forma original. El equipo y los programas de computadora que utilizan dos de esas claves se suelen denominar en forma colectiva "criptosistemas" o, más concretamente, "criptosistemas asimétricos" cuando se basan en el empleo de algoritmos asimétricos.

19. Si bien el empleo de la criptografía es una de las características principales de las firmas digitales, el mero hecho de que una firma digital se utilice para autentificar un mensaje que contiene información en forma digital, no debe confundirse con el uso más general de la criptografía con fines de confidencialidad. La codificación con fines de confidencialidad es un método utilizado para codificar una comunicación electrónica de modo que sólo el originador y el destinatario del mensaje puedan leerlo. En un cierto número de países, el empleo de la criptografía con fines de confidencialidad está limitado por las leyes en base de consideraciones de política pública que pueden abarcar la defensa nacional. Ahora bien, el empleo de la criptografía con fines de autentificación para producir una firma digital, no implica necesariamente el empleo de la codificación para dar carácter confidencial a la información durante el proceso de comunicación, dado que la firma digital codificada puede sencillamente añadirse a un mensaje no codificado. El Grupo de Trabajo quizá desee examinar en qué medida las posibles normas uniformes sobre firmas digitales deben reconocer que el empleo de la criptografía con fines de autentificación es distinto de su uso con fines de confidencialidad.

20. Para ilustrar las razones por las que pudieran necesitarse normas diferentes cuando la codificación se utiliza con fines de confidencialidad o en el contexto de las firmas digitales, cabe señalar que cuando la codificación se utiliza para mantener la confidencialidad de los mensajes, en muchas circunstancias, por ejemplo, cuando el mensaje codificado tiene valor como instrumento jurídico, financiero o de responsabilidad pública, es importante que haya una forma de recuperar los mensajes codificados si se pierde la clave privada. La tecnología, cuando se la utiliza correctamente, permite al originador del par de claves retener o reconstituir la clave perdida. Ahora bien, puede que no haya necesidad de retener o reconstituir la clave privada utilizada para crear firmas digitales, y la capacidad técnica para hacerlo podría reducir la confianza de los usuarios y del público en general en el sistema en su conjunto.

ii) "Claves criptográficas públicas y privadas"

21. Las claves complementarias utilizadas para las firmas digitales se denominan arbitrariamente la "clave privada", que es utilizada sólo por el firmante para crear la firma digital, y la "clave pública", que de ordinario conocen más personas y que se utiliza para que la parte correspondiente pueda verificar la firma digital3/. Si es necesario que muchas personas verifiquen firmas digitales del firmante, la clave

---

3/ El usuario de una clave privada debe mantenerla en secreto. Cabe señalar que el usuario individual no necesita conocer la clave privada. Esa clave privada probablemente se mantendrá en una tarjeta inteligente, o se podrá acceder a ella mediante un número de identificación personal o, en la situación ideal, mediante un dispositivo de identificación biométrica, por ejemplo, mediante el reconocimiento de una huella digital.

pública debe estar a su disposición o en su poder, por ejemplo publicándola en un repositorio en línea o en cualquier otra forma de directorio público de fácil acceso. Si bien las claves del par están matemáticamente relacionadas entre sí, el diseño y la ejecución en forma segura de un criptosistema asimétrico hace virtualmente imposible que las personas que conocen la clave pública puedan derivar de ella la clave privada. Los algoritmos más comunes para la codificación mediante el empleo de claves públicas y privadas se basan en una característica importante de los grandes números primarios: una vez que se multiplican entre sí para producir un nuevo número, es virtualmente imposible determinar cuáles

fueron los dos números primarios que crearon ese nuevo número más grande4/. De esta forma, aunque muchas personas puedan conocer la clave pública de un firmante determinado, y utilizarla para verificar sus firmas, no podrán descubrir la clave privada del firmante y utilizarla para falsificar firmas digitales.

22. Cabe señalar, sin embargo, que el concepto de la criptografía de clave pública no implica necesariamente el empleo de los algoritmos mencionados anteriormente basados en números primarios. En la actualidad se están utilizando o desarrollando otras técnicas matemáticas, como los criptosistemas de curvas elípticas, que se suelen describir como sistemas que ofrecen un alto grado de seguridad mediante el empleo de longitudes de clave significativamente reducidas. Al examinar las cuestiones de la criptografía de clave pública, el Grupo de Trabajo quizá desee tener en cuenta la difusión que están teniendo estos sistemas en el comercio internacional. Al mismo tiempo, el Grupo de Trabajo quizá desee adoptar una actitud técnicamente neutral, teniendo en cuenta la tecnología actual sin excluir por anticipado futuros cambios en las técnicas de computación que se utilizan para producir los pares de claves. Por otra parte, esa apertura a los avances técnicos de la industria de las computadoras estaría en consonancia con la decisión adoptada por la Comisión relativa a la imposibilidad de que la CNUDMI se embarque en la preparación de normas técnicas y a la necesidad de que actúe con precaución, para no verse envuelta en las cuestiones técnicas de las firmas digitales (véase el párrafo 3 supra).

iii) "La función parásita"

23. Además de la generación de pares de claves, se utiliza otro proceso fundamental, generalmente conocido con el nombre de "función parásita", tanto para crear como para verificar una firma digital. Una función parásita es un proceso matemático, basado en un algoritmo que crea una representación digital, o forma comprimida del mensaje, a menudo conocida con el nombre de "compendio de mensaje" o "huella digital" del mensaje, en forma de un "valor parásito" o "resultado parásito" de una longitud estándar que suele ser mucho menor que la del mensaje, pero que es no obstante substancialmente singular del mismo. Todo cambio en el mensaje produce invariablemente un resultado parásito diferente cuando se utiliza la misma función parásita. En el caso de una función parásita segura, a veces denominada "función parásita de una sola dirección", es virtualmente imposible derivar el mensaje original aun cuando se conozca su valor parásito. Estas funciones, por lo tanto, hacen posible que el programa para crear firmas digitales funcione con cantidades más pequeñas y predecibles de datos, proporcionando no obstante una fuerte correlación testimonial del contenido original del mensaje, y dando garantías eficaces de que el mensaje no ha sido modificado desde que fue firmado en forma digital.

iv) "Firma digital"

24. Para firmar un documento o cualquier otro material de información, el firmante delimita primero en forma precisa el espacio de lo que se ha de firmar. La información delimitada para la firma puede denominarse "mensaje". Seguidamente, mediante una función parásita del programa del firmante se

---

4/ Ciertas normas existentes, como las disposiciones de las directrices sobre firma digital de la ABA, se refieren a la noción de la "no viabilidad computacional" para describir la prevista irreversibilidad del proceso, es decir, la esperanza de que será imposible derivar la clave privada secreta de un usuario a partir de su clave pública. El término "no viabilidad computacional" es un concepto relativo, basado en el valor de los datos protegidos, la capacidad computacional general requerida para protegerlos, el tiempo necesario para protegerlos y el costo y el tiempo necesario para atacar esos datos, evaluando esos factores en función de la tecnología actual y de los adelantos tecnológicos previstos para el futuro (ABA Digital Signature Guidelines, pág. 9, nota 23).

calcula un resultado parásito que, a todos los fines prácticos, es único del mensaje. El programa del firmante transforma luego el resultado parásito en una firma digital utilizando la clave privada del firmante. La firma digital resultante es, por lo tanto, exclusiva del mensaje y de la clave privada utilizada para crearla.

25. Típicamente, la firma digital (es decir, un resultado parásito digitalmente firmado del mensaje) se adhiere a su mensaje y se almacena o transmite junto con el mismo. Ahora bien, puede también ser enviado o almacenado como un elemento de datos separado, siempre que mantenga una vinculación fiable con su mensaje. Dado que la firma digital es exclusiva de su mensaje, resulta inútil si se la desvincula de éste en forma permanente.

v) Verificación de la firma digital

26. La verificación de la firma digital es el proceso de comprobar esa firma por referencia al mensaje original y a una clave pública dada, determinando de esta forma si la firma digital fue creada para ese mismo mensaje utilizando la clave privada que corresponde a la clave pública referida. La verificación de una firma digital se logra calculando un nuevo resultado parásito del mensaje original, mediante la misma función parásita utilizada para crear la firma digital. Seguidamente, utilizando la clave pública y el nuevo resultado parásito, el verificador comprueba si la firma digital fue creada utilizando la clave privada correspondiente, y si el nuevo resultado parásito calculado corresponde al resultado parásito original que fue transformado en la firma digital durante el proceso de la firma.

27. El programa de verificación confirmará la firma digital como "verificada": 1) si se utilizó la clave privada del firmante para firmar digitalmente el mensaje, lo que se sabe que ocurre si se utiliza la clave pública del firmante para verificar la firma, dado que esta clave pública sólo verificará una firma digital creada con la clave privada correspondiente; y 2) si el mensaje no ha sido modificado, lo que se sabe que ocurre si el resultado parásito computado por el verificador es idéntico al resultado parásito extraído de la firma digital durante el proceso de verificación.

b) Infraestructura de claves públicas (PKI) y autoridades certificadoras

28. Para verificar una firma digital, el verificador debe tener acceso a la clave pública del firmante y debe tener seguridades de que corresponde a la clave privada del firmante. Ahora bien, un par de clave pública y privada no tiene ninguna vinculación intrínseca con ninguna persona; es simplemente un par de números. Se necesita un mecanismo adicional para vincular en forma fiable a una persona o entidad determinada al par de claves. Para que la codificación de la clave pública pueda cumplir su función específica, es necesario disponer de un medio de enviar claves a una gran diversidad de personas, muchas de las cuales no son conocidas del remitente y con las que no ha desarrollado ninguna relación de confianza. A tal efecto, las partes interesadas deben tener un alto grado de confianza en las claves pública y privada que se emiten.

29. El nivel de confianza requerido puede existir entre partes que confíen unas en otras, que se han tratado durante algún tiempo, que se comunican mediante sistemas cerrados, que operan dentro de un grupo cerrado, o que pueden regir sus operaciones en base a un contrato, por ejemplo, en un acuerdo de asociación comercial. En una transacción en la que participan sólo dos partes, cada una puede sencillamente comunicar (por un canal relativamente seguro, como un correo privado o un teléfono restringido) la clave pública del par de claves a cada una de las partes que la utilizarán. Ahora bien, este nivel de confianza puede no existir entre partes que no realizan transacciones con frecuencia, que se comunican a través de sistemas abiertos (por ejemplo, la World Wide Web o la Internet), que no forman parte de un grupo cerrado o que no tienen acuerdos de asociación comercial u otros acuerdos que rijan sus relaciones.

30. Además, dado que la codificación de clave pública es una tecnología altamente matemática, todos los usuarios deben tener confianza en las aptitudes, los conocimientos y los dispositivos de seguridad de las partes que emiten las claves pública y privada5/.

31. Un firmante potencial podría hacer una declaración pública indicando que las firmas verificables por una clave pública determinada deben ser consideradas como auténticas de ese firmante. Ahora bien, puede que otras partes no estén dispuestas a aceptar la declaración, especialmente si no hay ningún contrato previo que establezca con certidumbre el efecto jurídico de esa declaración publicada. La parte que se base en esa declaración publicada sin respaldo en un sistema abierto corre un gran riesgo de confiar inadvertidamente en un impostor, o de tener que contrarrestar una negativa falsa de una firma digital (cuestión que suele denominarse de "repudio negativo") si la transacción resulta desventajosa para el supuesto firmante.

32. Una de las soluciones a estos problemas es el empleo de uno o más terceros de confianza para vincular a un firmante identificado o el nombre del firmante a una clave pública determinada. El tercero en quien se confía se conoce en general, en la mayoría de las normas y directrices técnicas, como una "autoridad certificadora". En unos cuantos países, esas autoridades certificadoras están siendo organizadas en forma jerárquica en lo que se suele denominar una infraestructura de clave pública (PKI).

i) Infraestructura de claves públicas (PKI)

33. El establecimiento de una infraestructura de claves públicas (PKI) es una forma de impartir confianza en que: 1) la clave pública del usuario no ha sido alterada y corresponde de hecho a la clave privada del mismo usuario; 2) se han utilizado buenas técnicas de codificación; 3) se puede confiar en las entidades que emiten las claves criptográficas en cuanto a la retención o el restablecimiento de las claves pública y privada que se puedan utilizar para efectuar una codificación de confidencialidad en los casos en que esté autorizado el empleo de esa técnica; 4) los sistemas de codificación diferentes son intercambiables. Para poder impartir el grado de confianza descrito más arriba, una PKI puede ofrecer diversos servicios, incluidos los siguientes: 1) gestión de las claves criptográficas utilizadas para las firmas digitales; 2) certificación de que una clave pública corresponde a una clave privada; 3) provisión de claves a usuario finales; 4) establecimiento de los privilegios que tendrán los diversos usuarios del sistema; 5) publicación de un directorio seguro de certificados o claves públicas; 6) administración de contraseñas personales (por ejemplo, en tarjetas inteligentes) que permitan identificar al usuario con información de identificación personal singular o que permitan generar y almacenar claves privadas individuales; 7) comprobación de la identificación de los usuarios finales y suministro de servicios a éstos; 8) suministros de servicios de repudio negativo; 9) suministro de servicios de marcado cronológica; 10) gestión de las claves de codificación utilizadas con fines de confidencialidad en los casos en que esté autorizado el empleo de esa técnica.

34. Una infraestructura de claves públicas (PKI) se suele basar en diversos niveles jerárquicos de autoridad. Por ejemplo, los modelos considerados en ciertos países para el establecimiento de una posible PKI incluyen referencias a los siguientes niveles: 1) una "autoridad básica" única que certificaría la tecnología y las prácticas a todas las partes autorizadas a utilizar certificados o pares de claves criptográficas en relación con el empleo de dichos pares de claves, y llevaría un registro de las

---

5/ En los casos en que las claves criptográficas pública y privada son emitidas por los propios usuarios, puede que ese elemento de confianza deba ser aportado por certificadores de claves públicas.

autoridades de certificación subordinadas6/; 2) diversas autoridades de certificación, situadas debajo de la autoridad "básica", 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 alterada); y 3) diversas autoridades locales de registro, situadas debajo de las autoridades de certificación, que reciben de los usuarios pedidos de pares de claves criptográficas o certificados relativos al empleo de esos pares de clave, que exigen pruebas de identidad a los posibles usuarios y la verifican. En ciertos países, se prevé que los escribanos públicos podrían actuar como autoridades locales de registro, o prestar apoyo a estas autoridades.

35. El Grupo de Trabajo quizá desee realizar un examen de carácter general sobre la cuestión de las PKI. Ahora bien, esas cuestiones quizá no se presten fácilmente a la armonización a nivel internacional. La organización de una PKI puede comprender diversas cuestiones técnicas, así como cuestiones de política pública que es preferible dejar al arbitrio de cada Estado7/. A este respecto, quizá sea necesario que cada Estado que contemple el establecimiento de una PKI adopte decisiones, por ejemplo, respecto de: 1) el formato y el número de niveles de autoridad que se incluirán en una PKI; 2) si sólo las autoridades certificadoras pertenecientes a la PKI podrán emitir pares de claves criptográficas o si éstos podrían ser emitidos también por los propios usuarios; 3) si las autoridades certificadoras de la validez de los pares de claves criptográficos deben ser entidades públicas o si también las entidades privadas podrían actuar como autoridades certificadoras; 4) si el proceso de autorizar a una entidad determinada para actuar como autoridad certificadora debe adoptar la forma de una autorización expresa, o "licencia", por parte del Estado, o si se pueden utilizar otros métodos para controlar la calidad de las operaciones de las autoridades certificadoras permitiendo que éstas funcionen sin una autorización específica; 5) el grado en que el empleo de la criptografía se debe autorizar para fines de confidencialidad; y 6) si las autoridades gubernamentales deben retener el acceso a la información codificada mediante un mecanismo de "custodia de claves" o de otro tipo. El Grupo de Trabajo quizá desee recomendar que en la labor futura de la Comisión con respecto a las firmas digitales no se traten las cuestiones mencionadas más arriba.

ii) Autoridades certificadoras

36. Para vincular un par de claves a un posible firmante, la autoridad certificadora emite un certificado, un archivo electrónico que indica una clave pública junto con el nombre del suscriptor del certificado como el "sujeto" del certificado, y puede confirmar que el firmante potencial identificado en el certificado posee la clave privada correspondiente. La función principal del certificado es vincular una clave pública con una persona determinada. El "receptor" del certificado que desee confiar en una firma digital creada por la persona nombrada en el certificado puede utilizar la clave pública indicada en ese certificado para verificar si la firma digital fue creada con la clave privada correspondiente. Si dicha verificación es positiva, se obtiene la garantía de que la firma digital fue creada por el tenedor de la clave pública indicada en el certificado, y que el mensaje correspondiente no ha sido modificado desde que fue firmado en forma digital.

6/ La cuestión de si un gobierno debe tener la capacidad técnica para retener o restablecer claves de confidencialidad privadas se puede tratar al nivel de la autoridad básica.

7/ Ahora bien, en el contexto de la certificación cruzada, la necesidad de que esto funcione a nivel global exige que las PKI establecidas en diversos países tengan la capacidad para comunicarse entre sí.

37. Para asegurar la autenticidad del certificado con respecto tanto a su contenido como a su fuente, la autoridad certificadora lo firma en forma digital. La firma digital de la autoridad certificadora incluida en el certificado se puede verificar utilizando la clave pública de esta última incluida en otro certificado de otra autoridad certificadora (que puede, aunque no debe, ser de un nivel jerárquico superior), y ese otro certificado puede a su vez ser autentificado utilizando la clave pública incluida en un tercer certificado, y así sucesivamente, hasta que la persona que desea confiar en la firma digital tenga seguridades suficientes de su autenticidad. En cada caso, la autoridad que emite el certificado debe firmarlo en forma digital durante el período operacional del otro certificado utilizado para verificar la firma digital de la autoridad certificadora.

38. La firma digital correspondiente a un mensaje, ya sea creado por el tenedor de un par de claves para autentificar un mensaje o por una autoridad de certificación para autentificar su certificado, debe por lo general contener un sello cronológico fiable para que el verificador pueda determinar con certeza si la firma digital fue creada durante el "período operacional" indicado en el certificado, que es una condición para poder verificar una firma digital.

39. Para que una clave pública y su correspondencia con un tenedor específico se pueda utilizar fácilmente en una verificación, el certificado se debe publicar en un repositorio o difundir por otros medios. Normalmente, los repositorios son bases de datos en línea de certificados y otros tipos de información que se puede recuperar y utilizar para verificar firmas digitales. Según el tipo de aplicación, la recuperación de un certificado se puede lograr en forma automática haciendo que el programa de verificación consulte directamente al repositorio para obtener los certificados que necesita.

40. Una vez emitido, un certificado puede resultar no fidedigno, por ejemplo si el tenedor falsifica su identidad ante la autoridad certificadora. En otros casos, un certificado puede ser suficientemente fidedigno cuando se emite pero puede dejar de serlo más adelante. Si la clave privada ha quedado "expuesta", por ejemplo si el tenedor de la clave privada pierde el control sobre la misma, el certificado puede dejar de ser fiable y la autoridad certificadora (a petición del tenedor o aun sin el consentimiento de éste, según las circunstancias) puede suspender (interrumpir temporalmente el período operacional) o revocar (invalidar en forma permanente) el certificado. Inmediatamente después de suspender o revocar un certificado, la autoridad debe por lo general publicar un aviso de revocación o suspensión o notificar este hecho a las personas que solicitan información o que son receptoras conocidas de una firma digital verificable por remisión al certificado que ya no es digno de confianza.

41. Las autoridades de certificación pueden depender de autoridades gubernamentales o de proveedores de servicios del sector público. Algunos países disponen que, por razones de política pública, sólo las autoridades gubernamentales estarán autorizadas para funcionar como autoridades de certificación. En otros países se considera que estos servicios deben estar abiertos a la competencia del sector privado. Independientemente de que las autoridades certificadoras sean entidades públicas o proveedores de servicios del sector privado, y de que las autoridades certificadoras deban obtener una licencia, normalmente hay más de una autoridad certificadora dentro de la PKI. De particular interés es la relación entre las autoridades certificadoras. Las autoridades certificadoras de una PKI pueden estar clasificadas en un orden jerárquico, en el virtud del cual algunas autoridades sólo certifican los actos de otras autoridades que prestan servicios directos al usuario. En una estructura de este tipo, las autoridades de certificación están subordinadas a otras autoridades. En otras estructuras posibles, algunas autoridades de certificación pueden funcionar en un nivel de igualdad con otras autoridades. En las PKI grandes, probablemente habrá autoridades de certificación superiores y subordinadas. En todo caso, ante la falta de una PKI internacional, se pueden plantear diversos problemas relacionados con el reconocimiento de los certificados emitidos por las autoridades de otros países. El reconocimiento de certificados extranjeros se puede denominar "certificación cruzada". En tales casos, es necesario que las autoridades de certificación básicamente equivalentes (o las autoridades de certificación que estén dispuestas a asumir ciertos riesgos con respecto a los certificados emitidos por

otras autoridades) reconozcan mutuamente los servicios suministrados por cada una de ellas, de modo que los usuarios respectivos se puedan comunicar entre sí en forma más eficiente y con mayor confianza en la fidelidad de los certificados que se emiten.

42. Con respecto a la certificación cruzada o a las cadenas de certificados, cuando entran en juego múltiples políticas de seguridad se pueden plantear problemas jurídicos, por ejemplo, respecto de la identificación del autor del error que causó una pérdida, y de la fuente en que se basó el usuario. Cabe señalar que las normas jurídicas que se están considerando en ciertos países disponen que cuando los niveles de seguridad y las políticas se hacen conocer a los usuarios, y no hay negligencia por parte de las autoridades de certificación, no habrá responsabilidad por daños.

43. Puede que incumba a la autoridad certificadora, o a la autoridad principal, asegurar que los requisitos de sus políticas se cumplan en forma permanente. Si bien la selección de las autoridades certificadoras puede basarse en diversos factores, incluida la calidad de la clave pública utilizada y la identidad del usuario, la confianza en la autoridad certificadora puede depender también de la forma en que aplique las normas para emitir certificados y de la fiabilidad de su evaluación de los datos recibidos de los usuarios que solicitan certificados. Es sumamente importante el régimen de responsabilidad que se aplica a la autoridad certificadora con respecto al cumplimiento, en todo momento, de la política y los requisitos de seguridad de la autoridad principal o la autoridad de certificación superior, o de cualquier otro requisito aplicable.

44. El Grupo de Trabajo quizá desee tener en cuenta los siguientes factores al determinar si una autoridad certificadora es digna de confianza: 1) independencia (es decir, ausencia de un interés financiero o de otro tipo en las transacciones subyacentes); 2) recursos y capacidad financieros para asumir la responsabilidad por el riesgo de pérdida; 3) experiencia en tecnologías de clave pública y familiaridad con procedimientos de seguridad apropiados; 4) longevidad (las autoridades certificadoras pueden tener que presentar pruebas de certificaciones o claves de codificación muchos años después de que se hayan completado las transacciones subyacentes, por ejemplo en el contexto de un juicio o una reclamación de propiedad); 5) aprobación del equipo y los programas; 6) mantenimiento de un registro de auditoría y realización de auditorías por una entidad independiente; 7) existencia de un plan para casos de emergencia ("programas de recuperación en casos de desastres" o depósitos de claves); 8) selección y administración del personal; 9) disposiciones para proteger su propia clave privada; 10) seguridad interna; 11) disposiciones para suspender las operaciones, incluida la notificación a los usuarios; 12) garantías y representaciones (otorgadas o excluidas); 13) limitación de la responsabilidad; 14) seguros; 15) capacidad para intercambiar datos con otras autoridades certificadoras; y 16) procedimientos de revocación (en caso de que la clave criptográfica se haya perdido o haya quedado expuesta).

c) Sinopsis del proceso de la firma digital

45. El empleo de firmas digitales abarca por lo general los siguientes procesos, realizados por el firmante o por el receptor del mensaje firmado en forma digital:

1) El usuario genera o recibe un par de claves criptográficas único;

2) El remitente prepara el mensaje (por ejemplo, en forma de mensaje de correo electrónico en una computadora;

3) El remitente prepara un "compendio del mensaje", utilizando un algoritmo parásito seguro. En la creación de la firma digital se utiliza un resultado parásito derivado del mensaje firmado y de una clave privada determinada, que es exclusivo de éstos. Para que el resultado parásito sea

seguro, debe haber sólo una posibilidad mínima de que la misma firma digital se pueda crear mediante la combinación de cualquier otro mensaje o clave privada;

4) El remitente codifica el compendio del mensaje utilizando la clave privada. La clave privada se aplica al compendio del mensaje utilizando un algoritmo matemático. La firma digital es el compendio del mensaje codificado;

5) El remitente normalmente adjunta o adhiere su firma digital al mensaje;

6) El remitente envía la firma digital y el mensaje (codificado o no codificado) al receptor en forma electrónica;

7) El receptor utiliza la clave pública del remitente para verificar la firma digital de éste. Esta verificación con la clave pública del remitente prueba que el mensaje proviene exclusivamente del remitente;

8) El receptor también crea un "compendio del mensaje" utilizando el mismo algoritmo parásito seguro;

9) El receptor compara los dos compendios de mensajes. Si son iguales, el receptor sabe que el mensaje no ha sido modificado después de la firma. Aun cuando sólo se haya modificado una parte ínfima del mensaje después que ha sido firmado en forma digital, el compendio del mensaje creado por el receptor será diferente al compendio del mensaje creado por el remitente;

10) El receptor obtiene un certificado de la autoridad certificadora (o por conducto del originador del mensaje), que confirma la firma digital del remitente del mensaje. La autoridad certificadora es, por lo general un tercero de confianza que administra la certificación en el sistema de firmas digitales. El certificado contiene la clave pública y el nombre del remitente (y posiblemente otra información), y lleva la firma digital de la autoridad certificadora.

II. CUESTIONES JURÍDICAS Y POSIBLES DISPOSICIONES QUE SE DEBEN TENER EN CUENTA EN LAS NORMAS UNIFORMES SOBRE FIRMAS DIGITALES

A. Alcance de los trabajos

46. La Comisión, cuando decidió en su 29º período de sesiones incluir el tema de las firmas digitales y las autoridades certificadoras en su programa, convino también en que la cuestión debía aprovecharse como una oportunidad para tratar los otros temas sugeridos por el Grupo de Trabajo para la labor futura (véase el párrafo 8 supra). Antes de iniciar el examen de las cuestiones relativas a las firmas digitales, el Grupo de Trabajo quizá desee estudiar la conveniencia y viabilidad de limitar el alcance de su labor a las firmas digitales o ampliarla para cubrir también otros mecanismos de autentificación que ya estuvieran disponibles en el mercado o que pudieran elaborarse en fecha próxima para su utilización en el comercio electrónico (véanse los párrafos 15 a 17 supra). Cabe recordar que durante la preparación de la Ley Modelo, el Grupo de Trabajo tuvo conciencia de la necesidad de establecer normas jurídicas que no estuvieran amarradas a una etapa determinada del desarrollo técnico y comercial, sino que fueran más bien principios de carácter general que pudieran seguir siendo aplicables durante un cierto número de años, independientemente de los posibles cambios que se produzcan en las tecnologías.

47. El uso difundido de las firmas digitales y el riesgo de que se aprueben criterios legislativos diferentes en los diversos países, parece indicar que se necesitan disposiciones legislativas uniformes

como marco jurídico específico para esas técnicas de autentificación. Ahora bien, en consonancia con el enfoque neutral respecto del medio adoptado para la preparación de la Ley Modelo, el Grupo de Trabajo quizá desee examinar si es conveniente iniciar la preparación de normas uniformes que se aplicarían a las firmas digitales solamente o si dichas normas uniformes debieran abarcar también otras técnicas de autentificación. Si el Grupo de Trabajo llegase a la conclusión de que es particularmente apremiante el riesgo antes mencionado de que diversos países adopten leyes diferentes, que esto apunta hacia la necesidad de contar con normas uniformes aplicables a las firmas digitales, el Grupo de Trabajo quizá desee también examinar la mejor forma de redactar las normas uniformes sobre firmas digitales para evitar el riesgo de que pudieran interpretarse en el sentido de que alientan el empleo de las firmas digitales en detrimento de otras técnicas competitivas, lo que también podría interpretarse como una aplicación aceptable del concepto del "método fiable" consagrado en el artículo 7 de la Ley Modelo.

48. Con respecto a las autoridades certificadoras, el Grupo de Trabajo quizá desee también tener en cuenta que, en muchas situaciones prácticas, las actividades de una entidad comercial como autoridad certificadora son sólo una de la amplia gama de actividades que puede realizar dicha entidad comercial en su carácter de proveedora de servicios. Por lo tanto, el Grupo de Trabajo quizá desee estudiar la cuestión de si las normas uniformes sobre autoridades de certificación se deben limitar al establecimiento de normas de conducta aplicables sólo en el contexto de las actividades de un proveedor de servicios en calidad de autoridad certificadora, o si sería conveniente y viable desarrollar normas aplicables a una gama más amplia de actividades de los proveedores de servicios o "terceros de confianza" en el comercio electrónico.

B. Esfera de aplicación de las normas uniformes sobre firmas digitales y disposiciones de carácter general

49. La presente nota fue preparada partiendo del supuesto de que las posibles normas sobre firmas digitales se derivarían directamente del artículo 7 de la Ley Modelo, y se deben considerar como una forma de proporcionar información detallada sobre el concepto del "método [fiable] para identificar" a una persona y "para indicar que esa persona aprueba" la información contenida en un mensaje de datos. Al considerar las disposiciones generales para su posible inclusión en un conjunto de normas uniformes sobre firmas digitales, el Grupo de Trabajo quizá desee examinar en forma más general la relación entre dichas normas uniformes y la Ley Modelo de la CNUDMI sobre Comercio Electrónico. En particular, el Grupo de Trabajo quizá desee hacer propuestas a la Comisión sobre la cuestión de si las normas uniformes sobre firmas digitales deben constituir un instrumento jurídico separado o si se deben incorporar en una versión ampliada de la Ley Modelo, por ejemplo como un capítulo separado de la parte II de esa Ley Modelo.

50. Ya sea que las normas uniformes sobre firmas digitales se preparen como instrumento separado o como una adición a la Ley Modelo, se sugiere que las normas uniformes se basen en disposiciones similares a las de los artículos 1 (Ámbito de aplicación), 2 a), c) y e) (Definiciones de "mensajes de datos", "iniciador" y "destinatario"), 3 (Interpretación), 4) (Modificación mediante acuerdo), 6 (Escrito) y 7 (Firma) de la Ley Modelo. Si bien estas disposiciones no se producen en la presente nota, cabe señalar que el proyecto de normas uniformes sobre firmas digitales ha sido preparado por la Secretaría en base al supuesto de que dichas disposiciones de la Ley Modelo forman parte de las normas uniformes. A este respecto, cabe tener presente que hay disposiciones similares a las de los artículos 2, 4, 6 y 7 de la Ley Modelo en la legislación sobre firmas digitales que están preparando algunos países, y que también se hace referencia a la Ley Modelo en textos como el de las directrices sobre firmas digitales de la ABA.

51. Además de las disposiciones arriba mencionadas, el Grupo de Trabajo quizá desee considerar si en un preámbulo se podría aclarar la finalidad de las normas uniformes, es decir, promover la

utilización eficaz de las comunicaciones digitales estableciendo un marco de seguridad y dando a los mensajes digitales un estatuto igual al de los mensajes escritos en cuanto a sus efectos jurídicos.

C. Cuestiones jurídicas específicas y proyectos de disposiciones sobre firmas digitales

1. Definiciones

52. Las leyes, los reglamentos y las directrices que ya se aplican o que se están preparando en la esfera de las firmas digitales y las autoridades certificadoras varían considerablemente en cuanto al número de definiciones en que se basan. Según cual sea la tradición jurídica del Estado que promulgue estas leyes, las cuestiones de las firmas digitales pueden resolverse principalmente por medio de definiciones o no contener definición alguna.

53. En consonancia con el criterio adoptado para la preparación de la Ley Modelo, el Grupo de Trabajo quizá desee examinar un número limitado de definiciones de conceptos esenciales, como "firma digital", "autoridades certificadoras" y "certificados".

54. El Grupo de Trabajo quizá desee utilizar los siguientes proyectos de definiciones como base para sus deliberaciones.

a) Firma digital

55. "Proyecto de artículo A

1) Una firma digital es un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido vinculado a la clave criptográfica privada del iniciador, permite determinar que este valor numérico se ha obtenido exclusivamente con la clave criptográfica privada del iniciador.

2) Los procedimientos matemáticos utilizados para generar firmas digitales autorizadas en virtud de [esta Ley] [estas Normas] se basan en la codificación de clave pública. Aplicados a un mensaje de datos, esos procedimientos matemáticos transforman el mensaje de modo que una persona que tenga el mensaje inicial y la clave criptográfica pública de un iniciador pueda determinar con precisión

a) Si la transformación se efectuó utilizando la clave criptográfica privada que corresponde a la clave criptográfica pública del iniciador; y

b) Si el mensaje inicial fue modificado después de efectuada la transformación.

3) Una firma digital adherida a un mensaje de datos se considera autorizada si se puede verificar de conformidad con los procedimientos establecidos por una autoridad certificadora autorizada en virtud de [esta Ley] [estas Normas].

4) La [autoridad pertinente del Estado que promulga la ley o la norma] establecerá normas específicas relativas a los requisitos técnicos que deberán cumplir las firmas digitales y la verificación de las mismas".

Observaciones

56. En consonancia con el criterio funcional utilizado en la preparación de la Ley Modelo, los párrafos 1) y 2) de la disposición sugerida hacen hincapié en una breve descripción de las funciones técnicas de la codificación de clave pública. En los párrafos 3) y 4) se refleja el principio de que las firmas digitales sólo son válidas si se utilizan en el contexto de una infraestructura de claves públicas (PKI) aplicada por las autoridades públicas.

b) Autoridades certificadoras autorizadas

57. "Proyecto de artículo B

1) El ... [Estado que promulga la ley o la norma especifica el órgano o autoridad competente para conceder la autorización a las autoridades de certificación] puede conceder a las autoridades de certificación una autorización para actuar en cumplimiento de [esta ley] [estas normas]. Esta autorización puede ser revocada.

2) El ... [Estado que promulga la ley o la norma especifica el órgano o autoridad competente para promulgar reglamentos relativos a las autoridades de certificación autorizadas] puede establecer normas que rijan las condiciones en que se pueden conceder dichas autorizaciones, y promulgar reglamentos para las operaciones de las autoridades certificadoras.

3) Las autoridades certificadoras autorizadas pueden emitir certificados en relación con las claves criptográficas de personas jurídicas o naturales.

4) Las autoridades certificadoras autorizadas pueden ofrecer o facilitar servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales.

5) El ... [el Estado que promulga la ley o la norma especifica el órgano o la autoridad competente que pueden establecer reglas específicas respecto de las funciones que deben cumplir las autoridades de certificación autorizadas] puede establecer reglas más específicas relativas a las funciones que deben cumplir las autoridades de certificación autorizadas en relación con la emisión de certificados a personas jurídicas o naturales."

Observaciones

58. El Grupo de Trabajo quizá desee examinar si las normas uniformes que se han de preparar deben mencionar expresamente el criterio que se debe tener en cuenta al autorizar el funcionamiento de autoridades certificadoras. Cabe recordar que, en el contexto de la preparación de la Ley Modelo, se decidió incluir esos criterios en las Directrices de Aplicación.

c) Certificados

59. "Proyecto de artículo C

El certificado emitido por una autoridad certificadora autorizada, en forma de mensaje de datos o en otra forma, debe indicar por lo menos:

a) El nombre del usuario [y la dirección o el lugar donde realiza su comercio];

b) [El día y año de nacimiento] [identificación suficiente] del usuario, si éste es una persona natural;

c) Si el usuario es una persona jurídica, el nombre de la empresa y toda otra información pertinente para identificarla;

e) El nombre, la dirección o el lugar donde realiza sus actividades comerciales la autoridad certificadora;

f) La clave criptográfica pública del usuario;

g) Toda otra información necesaria que indique de qué forma el receptor de la firma digital dada de conformidad con el certificado puede verificar la clave criptográfica pública del usuario;

h) El número de serie del certificado; e

i) La [fecha de emisión y la fecha de expiración] [el período de validez] del certificado."

Observaciones

60. Los proyectos de ley sobre firma digital que se están preparando en ciertos países incluyen todos o algunos de los elementos mencionados en el proyecto de artículo C, como la información mínima que se debe suministrar en todos los certificados emitidos por una autoridad certificadora. Ahora bien, de conformidad con la decisión adoptada por el Grupo de Trabajo en la preparación de la Ley Modelo, de no inmiscuirse en las cuestiones relativas a la protección de los datos personales, el Grupo de Trabajo quizá desee tener en cuenta que, en muchos países, la información relativa, por ejemplo, a la fecha de nacimiento de una persona podría estar protegida como dato personal y podrían necesitarse normas específicas para reglamentar su transmisión por medios electrónicos.

2. Firmas de personas jurídicas y naturales

61. "Proyecto de artículo D

1) Tanto las personas naturales como las jurídicas pueden obtener la certificación de las claves públicas criptográficas usadas exclusivamente con fines de identificación.

2) Una persona jurídica puede identificar un mensaje de datos adhiriendo a ese mensaje la clave criptográfica privada certificada para esa persona jurídica. Sólo se considerará que la persona jurídica [es la iniciadora] [ha aprobado la transmisión] del mensaje si éste ha sido también firmado en forma digital por una persona natural autorizada a actuar en nombre de esa persona jurídica."

Observaciones

62. La disposición precedente tiene por objeto aclarar las condiciones en que las firmas digitales se pueden utilizar para vincular a personas jurídicas. Se basa en una distinción entre las dos funciones cumplidas por la "firma" en virtud apartado a) del párrafo 1 del artículo 7 de la Ley Modelo, es decir, identificar al autor de un mensaje e indicar que esa persona aprueba la información contenida en el mensaje. En tanto que las dos funciones normalmente se cumplirían mediante el empleo de una clave única certificada para una persona natural, las claves públicas certificadas para personas jurídicas se utilizarían solamente para dar seguridades en cuanto a la identidad de la persona jurídica remitente del

mensaje. La "firma digital" de una persona jurídica tendría, por lo tanto, un efecto limitado. Toda aprobación de un mensaje requeriría, además de la "firma digital" (es decir, la identificación) de la persona jurídica, la firma digital de una persona natural, que identifique a esa persona e indique, en nombre de la persona jurídica, la intención de aprobar el contenido del mensaje.

63. Si bien el proyecto de disposición contiene una referencia a "una persona natural autorizada para actuar en nombre" de una persona jurídica, no se tiene el propósito de dejar de lado la ley nacional de representación. Por lo tanto, la cuestión de si una persona natural tiene, de hecho y con arreglo a la ley, la autoridad para actuar en nombre de la persona jurídica se deja a las disposiciones jurídicas apropiadas distintas de las normas uniformes.

3. Atribución de los mensajes firmados digitalmente

64. "Proyecto de artículo E

1) El originador de un mensaje de datos al que está adherida su firma digital queda obligado por el contenido del mensaje como si éste hubiera existido en un formulario firmado [en forma manuscrita], de conformidad con la ley aplicable al contenido del mensaje.

2) El destinatario de un mensaje de datos al que está adherida una firma digital tiene derecho a considerar que ese mensaje proviene del originador, y a actuar en base a ese supuesto si:

a) para determinar si el mensaje de datos provenía del originador, el destinatario aplicó correctamente la clave pública del originador al mensaje de datos recibido y ello reveló: que el mensaje de datos recibido fue codificado con la clave criptográfica privada del originador, y que el mensaje inicial no fue alterado después de haber sido codificado, usando para ello la clave criptográfica pública del originador;

o

b) el mensaje de datos recibido por el destinatario resulta de las acciones de una persona cuya relación con el originador, o con cualquier agente del originador, permite a esa persona tener acceso a la clave criptográfica privada del originador.

3) El párrafo 2 no se aplica:

a) desde el momento en que el destinatario supo o debió haber sabido, si hubiera solicitado información a la autoridad certificadora autorizada o si hubiera tomado otras precauciones razonables, que la validez de la clave criptográfica pública del originador había expirado, o que el certificado expedido por la autoridad certificadora había sido revocado o suspendido;

o

b) en un caso comprendido en el apartado b) del párrafo 2, en cualquier momento en que el destinatario supo o debió haber sabido, su hubiera tomado precauciones razonables o hubiera utilizado cualquier procedimiento convenido, que el mensaje de datos no provenía del originador."

Observaciones

65. El Grupo de Trabajo quizá desee considerar si la cuestión de la atribución de los mensajes firmados digitalmente se podría resolver haciendo referencia sencillamente al artículo 13 de la Ley Modelo. El proyecto de artículo E, que se ajusta al artículo 13 de la Ley Modelo, tiene por objeto aclarar los principios contenidos en el artículo 13 en el contexto de las firmas digitales. Se basa en la necesidad de dar certidumbre en cuanto a los efectos jurídicos de las firmas digitales, que actualmente se consideran como un procedimiento muy seguro de autentificación. El proyecto de disposición impone una pesada carga al originador de un mensaje que lleva su firma digital. Cabe recordar que, en virtud del apartado c) del artículo 2 de la Ley Modelo, por "originador" se entiende toda persona que, a tenor del mensaje, haya actuado por su cuenta o en cuyo nombre se haya actuado para enviar el mensaje de datos. El proyecto de disposición ilustra la necesidad de que todo usuario de una firma digital proteja su clave privada, la cual, aplicada para codificar un mensaje, creará un presunción irrefutable de que el mensaje proviene del supuesto originador.

4. Revocación de certificados

66. "Proyecto de artículo F

1) El tenedor de un par de claves certificado puede revocar el certificado correspondiente. La revocación es efectiva desde el momento en que es [registrada] [recibida] por la autoridad certificadora.

2) El tenedor de un par de claves certificado tiene la obligación de revocar el certificado correspondiente si toma conocimiento de que la clave criptográfica se ha perdido, ha resultado expuesta o corre peligro de se la utilice indebidamente de otra forma. Si el tenedor no revoca el certificado en esa situación, será responsable de cualquier pérdida en que incurran los terceros que confiaron en el contenido del mensaje a raíz de que el tenedor no revocó el certificado."

Observaciones

67. El Grupo de Trabajo quizá desee tener presente que, si en las normas uniformes sobre firmas digitales se dispone que la revocación de un certificado es efectiva desde el momento en que es recibida por la autoridad certificadora, se podría suprimir el párrafo 4 del proyecto de artículo H (responsabilidad) dado que no habría ninguna base para hacer responsable a la autoridad certificadora por incumplimiento o negligencia en el registro de esa revocación.

5. Registro de certificados

68. "Proyecto de artículo G

1) Toda autoridad certificadora autorizada deberá llevar un registro electrónico de certificados expedidos, al que tenga acceso el público, indicando la fecha en que se expidió cada certificado, la fecha de expiración y la fecha en que fue suspendido o revocado.

2) El registro será mantenido por la autoridad certificadora por lo menos durante [10] años después de la fecha de revocación o la expiración del período operacional de cualquier certificado expedido por esa autoridad certificadora."

Observaciones

69. El Grupo de Trabajo quizá desee considerar si el registro de certificados debe ser del dominio público o si el acceso a él debe estar limitado de alguna manera a las partes interesadas. En cuanto al período durante el cual se deberán mantener ese registro, el Grupo de Trabajo quizá desee examinar si conviene establecer un período fijo como norma uniforme, si la determinación de dicho período se debe dejar al arbitrio de cada Estado, o si se debe tratar de establecer un criterio más flexible, por ejemplo, indicando que el registro debe estar disponible para verificar certificados durante el período operacional de cada uno de ellos y hasta el final del período en que los mensajes firmados digitalmente con certificados de la autoridad certificadora se puedan utilizar o se deban verificar, lo que podría hacer necesario el establecimiento de varios períodos, según las disposiciones de las leyes sobre prescripción vigentes.

6. Responsabilidad

70. "Proyecto de artículo H

1) La autoridad certificadora será responsable ante toda persona que haya actuado de buena fe basándose en un certificado expedido por ella, respecto de cualquier pérdida debida a defectos en el registro de la autoridad certificadora, fallos técnicos o circunstancias similares [aun si la pérdida no se debe][si la pérdida se debe] a negligencia de la autoridad certificadora.

2) Variante X La responsabilidad por cada pérdida no excederá de [cantidad]. El...[el Estado que promulga la ley o la norma especificará el órgano o la autoridad competente para revisar la cantidad máxima] puede revisar esta cantidad cada dos años para tener en cuenta la evolución de los precios.

Variante Y El...[el Estado que promulga la ley o la norma especificará el órgano o la autoridad competente para promulgar reglamentos sobre responsabilidad] podrá promulgar reglamentos sobre la responsabilidad de las autoridades certificadoras.

3) En caso de que la parte que sufrió la pérdida haya contribuido a ella por su propia voluntad o negligencia, la indemnización podrá reducirse o no adjudicarse.

[4) Cuando una autoridad certificadora autorizada haya recibido una notificación de la revocación de un certificado, la autoridad registrará dicha revocación de inmediato. Si no lo hace, la autoridad será responsable de cualquier pérdida que por ese motivo pueda sufrir el usuario.]

Observaciones

71. El Grupo de Trabajo quizá desee examinar si la disposición sobre responsabilidad debería ampliarse para abarcar otros casos, además de la negligencia de la autoridad certificadora. Quizá desee también determinar si corresponde aplicar el principio de la autonomía de las partes, y en qué medida, para permitir que las autoridades certificadoras controlen, por acuerdo privado con los usuarios, el alcance de su responsabilidad.

72. El Grupo de Trabajo quizá desee estudiar la posibilidad de incluir una disposición de "refugio" con el siguiente texto:

"Toda autoridad certificadora que cumpla con [la presente Ley][estas normas] y con toda ley o contrato aplicable, no será responsable de ninguna pérdida

1) en que incurra el tenedor de un certificado expedido por esa autoridad certificadora, como resultado de haber confiado en ese certificado, o

2) que resulte de haber confiado en un certificado emitido por esa autoridad certificadora, con una firma digital verificable por referencia a la clave pública indicada en un certificado emitido por esa autoridad certificadora, o a información contenida en ese certificado."

7. Cuestiones relativas a las certificaciones recíprocas

73. "Proyecto de artículo I

1) Los certificados emitidos por autoridades certificadoras extranjeras pueden ser usados a los fines de la firma digital en las mismas condiciones que las firmas digitales sujetas [a la presente Ley][a estas normas], si son reconocidos por una autoridad certificadora autorizada, y si ésta última garantiza, en la misma medida que respecto de sus propios certificados, la regularidad de los detalles del certificado, así como su validez y vigencia.

2) El...[el Estado que promulga la ley o la norma especifica el órgano o la autoridad competente para establecer las normas relativas a la aprobación de certificados extranjeros] está autorizado para aprobar certificados extranjeros, y también las normas específicas para dicha aprobación."

Observaciones

74. El proyecto de artículo I se basa en la noción de que el reconocimiento de certificados extranjeros se debe autorizar bajo la responsabilidad de una autoridad certificadora local con arreglo a la reciprocidad. Al examinar las cuestiones de las certificaciones recíprocas, el Grupo de Trabajo quizá desee considerar si se debe exigir reciprocidad plena o si las garantías en cuanto a la regularidad y validez de los certificados extranjeros no tienen que ser suministradas necesariamente al mismo nivel por todas las partes que formen parte de un plan de certificaciones recíprocas. El Grupo de Trabajo quizá desee considerar también si se debe requerir necesariamente la intervención del gobierno para el reconocimiento de certificados extranjeros.

75. El Grupo de Trabajo podría considerar, como posible alternativa al proyecto de artículo I, el criterio utilizado en los proyectos de legislación de ciertos países, en virtud del cual los certificados extranjeros sólo se pueden reconocer sobre la base de acuerdos internacionales bilaterales o multilaterales.

8. Relaciones entre los usuarios y la autoridad certificadora

76. "Proyecto de artículo J

1) La autoridad certificadora sólo puede pedir la información que sea necesaria para identificar al usuario.

2) A petición de personas jurídicas o naturales, la autoridad certificadora entregará información sobre lo siguiente:

a) las condiciones para el uso del certificado;

b) las condiciones a que está sujeto el uso de firmas digitales;

c) las tarifas de los servicios de las autoridades certificadoras;

d) las políticas o prácticas de la autoridad certificadora con respecto al uso, almacenamiento y comunicación de datos personales;

e) las especificaciones técnicas de la autoridad certificadora relativas al equipo de comunicaciones del usuario;

f) las condiciones en que la autoridad certificadora envía advertencias a los usuarios en caso de irregularidades o fallos en el funcionamiento del equipo de comunicaciones;

g) toda limitación de la responsabilidad de la autoridad certificadora;

h) cualquier restricción impuesta por la autoridad certificadora respecto del uso del certificado;

i) las condiciones en que el usuario tiene derecho a imponer restricciones al uso del certificado.

2) La información indicada en el párrafo 1 se entregará al usuario antes de la concertación de un acuerdo final. [Esa información puede ser entregada por la autoridad certificadora en forma de declaración sobre prácticas de certificación].

3) Con sujeción a un preaviso [de un mes], el usuario podrá dar por terminado el acuerdo de vinculación a la autoridad certificadora. Ese aviso de terminación tiene efecto desde el momento en que lo recibe la autoridad certificadora.

4) Con sujeción a un preaviso [de tres meses], la autoridad certificadora puede dar por terminado el acuerdo de vinculación a la autoridad certificadora. Ese aviso de terminación tiene efecto desde el momento de su recepción.

III. INCORPORACIÓN POR REMISIÓN

A. Exámenes anteriores

77. En el 28º período de sesiones del Grupo de Trabajo, se presentó una propuesta de incluir en el proyecto de Ley Modelo de la CNUDMI sobre los Aspectos Jurídicos del Intercambio Electrónico de Datos (EDI) y Medios Afines de Comunicación de Datos una disposición por la que se reconociera que ciertas cláusulas y condiciones que pudieran ser incorporadas en un registro de datos por simple referencia gozaran de idéntica validez jurídica que si hubieran sido enunciadas en su integridad en el texto del registro de datos. Se dijo que la incorporación por remisión de ciertas cláusulas a los mensajes

EDI era una cuestión esencial para los usuarios del EDI y que la certeza era muy necesaria para el empleo de este método. Se dijo que, por cierto, el EDI era intrínsecamente un sistema de incorporación por remisión, ya que los mensajes EDI perderían sentido y serían de escaso valor contractual sin la incorporación por remisión de las normas técnicas de comunicación pertinentes. Se decidió que el Grupo de Trabajo abordaría, en un futuro período de sesiones, la cuestión de la incorporación de cláusulas y condiciones en un mensaje de datos mediante una mera referencia a dichas cláusulas y condiciones (A/CN.9(406, párrafos 90 y 178).

78. En su 29º período de sesiones, el Grupo de Trabajo tuvo ante sí dos propuestas relativas a un proyecto de disposición sobre incorporación por remisión, una presentada por el Observador de la Cámara de Comercio Internacional (A(CN.9/WG.IV/WP.65) y otra presentada por el Reino Unido de Gran Bretaña e Irlanda del Norte (A/CN.9/WG.IV/WP.66). La opinión más difundida fue que la cuestión no estaba todavía madura para ser incluida en la Ley Modelo y que era necesario seguir estudiándola. Se dijo además que podía pensarse que ambas propuestas interferían con las normas generales del derecho contractual. Se afirmó además que la incorporación por remisión en un medio de documentación electrónica no tenía por qué abordarse en la Ley Modelo, ya que planteaba las mismas cuestiones que la incorporación mediante remisión en un medio de documentación escrita, las cuales ya habían sido abordadas en el derecho contractual general. Por último, se dijo que una disposición en la cual se distinguía entre la incorporación por remisión en un medio de documentación escrita y las comunicaciones del intercambio electrónico de datos sería incongruente con el criterio adoptado hasta el momento por el Grupo, que se proponía garantizar una "neutralidad con respecto al medio". En respuesta a esta posición, se dijo que existía entre los profesionales la percepción de que la cuestión de la incorporación mediante remisión era más compleja en el intercambio electrónico de datos que en un medio de documentación escrita debido, por ejemplo, a que el número de comunicaciones pertinentes era mucho mayor y sería mucho más difícil determinar cuáles habían sido las condiciones incorporadas mediante remisión si ellas adoptaban la forma de mensajes de datos. También se dijo que los profesionales sentían la necesidad de contar con disposiciones específicas relativas a la incorporación mediante remisión en el contexto de las comunicaciones electrónicas. Otro de los problemas planteados fue que, habida cuenta de la cantidad de mensajes de datos que podía abarcar una determinada relación contractual entablada mediante intercambio electrónico de datos, muy probablemente se suscitara el problema conocido con el nombre de "batalla de formularios" en el contexto de las comunicaciones electrónicas. El Grupo de Trabajo convino en que quizá fuera necesario estudiar más a fondo la cuestión de la incorporación por remisión en el contexto de la labor futura (A/CN.9/407, párrafos 100 a 105 y 117).

79. En su 30º período de sesiones, el Grupo de Trabajo estuvo en general de acuerdo en que era necesario abordar la cuestión de la incorporación por remisión en el contexto del EDI. Se expresó el parecer de que, en cualquier intento de establecer normas jurídicas para esa incorporación de cláusulas de remisión en los mensajes de datos, debían satisfacerse las tres condiciones siguientes: 1) la cláusula de remisión debía insertarse en el mensaje de datos; 2) el documento al que hiciera remisión, por ejemplo, condiciones y cláusulas generales, tenía que ser realmente conocido por la parte frente a la cual pudiera hacerse valer; y 3) el documento al que se hiciera referencia, además de ser conocido, tenía que ser aceptado por esa parte. Se convino en general en que la manera de tratar adecuadamente el punto de la incorporación por remisión era en el contexto de una labor más general sobre las cuestiones relativas a registros y proveedores de servicios (A/CN.9/421, párrafo 114). La Comisión, en su 29º período de sesiones, estuvo en general de acuerdo en que la cuestión podía considerarse en el contexto de la labor sobre autoridades de certificación (A/51/17, párrafo 222).

B. Posible necesidad de normas uniformes sobre incorporación por remisión

80. La incorporación por remisión es una forma concisa de referirse en forma genérica en un documento a disposiciones que están detalladas en otra parte, en lugar de reproducirlas en su totalidad.

Esto evita, por ejemplo, tener que reproducir extensos términos estándard cuando se negocian o conciertan contratos. De esta forma, esos términos se consideran incorporados en el documento o mensaje de datos en que se hace referencia a ellos, simplemente identificando los términos en forma suficiente e indicando la intención de incluirlos. En un medio de documentación electrónica, la incorporación por remisión se puede definir como el método para hacer que un mensaje o registro de datos (o parte de la información contenida en los mismos) pase a formar parte de otro mensaje o registro de datos separado haciendo en el primero una referencia al segundo, y declarando que el primero forma parte del segundo como si se lo hubiera incluido en él en su totalidad.

1. Normas tradicionales desarrolladas para un medio de documentación escrita

a) Incorporación por remisión

81. Las cuestiones jurídicas que plantea la incorporación por remisión son conocidas en el contexto de las comunicaciones basadas en documentación escrita, y en muchos sistemas jurídicos hay normas que establecen las condiciones jurídicas para que la información que no se ha incluido en su totalidad en un documento escrito pueda considerarse como que forma parte de ese documento. Por ejemplo, con arreglo a ciertas condiciones se puede incluir en un pedido o una factura, una referencia a uno o más INCOTERMS, como "porte pagado hasta" (CPT) o "porte y seguro pagados hasta" (CIP), con la consecuencia de que esos INCOTERMS se considerarán como una de las condiciones del contrato de compraventa sin que se incluya el texto completo de la definición de "CPT" o "CIP" en ninguno de los documentos contractuales. La incorporación por remisión de INCOTERMS puede verse facilitada por el hecho de que han sido preparados por la Cámara de Comercio Internacional (CCI) específicamente para su inclusión en contratos mediante el uso de acrónimos o designaciones abreviadas que son muy conocidas, y debido a que tanto la CCI como la CNUDMI recomiendan su uso. Otro ejemplo de un texto que se suele incorporar por remisión es el de las Reglas y Usos Uniformes relativas a los créditos documentarios (UCP 500), preparadas por la CCI. El argumento jurídico utilizado para permitir la incorporación por remisión en un contrato de un texto como el de las UCP 500 se suele basar en que ese texto registra prácticas muy conocidas y aceptadas en todo el mundo, y que se presume que todas las partes involucradas las conocen.

82. Cuando esa presunción no es aplicable, las condiciones establecidas por las leyes nacionales para validar la incorporación por remisión pueden incluir requisitos estrictos, por ejemplo, que todas las partes conozcan realmente la información incorporada por referencia, o hasta la aprobación expresa de esa información por las partes a las que se quiere exigir su cumplimiento. En virtud de ciertas leyes nacionales, en cambio, los requisitos para la validación de la incorporación por remisión pueden ser menos estrictos. Por ejemplo, ciertos requisitos jurídicos tradicionales de la incorporación por remisión pueden hacer hincapié en la claridad de la cláusula por la que se efectúa esa incorporación y en la facilidad de acceso a la información incorporada por remisión.

b) La "batalla de los formularios"

83. La cuestión de la incorporación por remisión no debe confundirse con la cuestión generalmente conocida como "la batalla de los formularios". Esta última puede ocurrir, por ejemplo, cuando los términos y condiciones generales del contrato propuesto por un comprador figuran en letra pequeña al dorso del formulario de pedido, mientras que en el dorso de la factura del vendedor figura un conjunto diferente de términos y condiciones generales del contrato. Cuando el comprador y el vendedor no hayan concertado un acuerdo específico acerca de los términos y condiciones que se aplicarán a un contrato dado, y haya dos conjuntos opuestos de esos términos y condiciones al dorso de sus respectivos documentos contractuales, será necesario eliminar la incertidumbre en cuanto al conjunto que regirá la transacción. En muchos países, se han desarrollado normas jurídicas de derecho contractual con el fin de resolver esa ambigüedad.

2. Cuestiones que se plantean en un medio de comercio electrónico

a) Uso difundido de la incorporación por remisión

84. La incorporación por remisión es esencial para el uso difundido del intercambio electrónico de datos (EDI), el correo electrónico, los certificados digitales y otras formas de comercio electrónico. Por ejemplo, las comunicaciones mediante mensajes EDI estándard, y las comunicaciones electrónicas en general, normalmente están estructuradas de tal forma que se intercambian grandes cantidades de mensajes, cada uno con información breve y recurriendo, con mucha más frecuencia que en las comunicaciones escritas, a la remisión a información que se puede encontrar en otras partes. El EDI y otros tipos sumamente estructurados y formateados de datos, invariablemente utilizan mucho la incorporación por remisión para mejorar la eficiencia en la elaboración de los datos. En períodos de sesiones anteriores del Grupo de Trabajo, se dijo que el EDI y diversas formas de comercio electrónico eran fundamentalmente sistemas de incorporación por remisión. Como cuestión de carácter práctico, cabe decir que es posible que los mensajes EDI tendrán una certeza jurídica reducida a menos que se aclaren la validez y la eficacia de la incorporación por remisión de los términos administrativos, técnicos y jurídicos pertinentes, y las condiciones, cláusulas, acuerdos, estándares, normas o directrices que pudieran ser aplicables a esos mensajes.

85. Con respecto a las situaciones en que pudiera ocurrir una "batalla de los formularios", cabe tener presente que los mensajes electrónicos no han sido concebidos, ni están preparados, para transmitir con cada mensaje textos como las condiciones y términos generales que suelen estar impresos al dorso de documentos escritos, y que su inclusión sería costosa e ineficiente, podría hacer más lentas y hasta interrumpir las comunicaciones electrónicas, y hasta podría reducir la efectividad de los avisos al obligar a las partes a imprimir o leer en pantalla esos extensos textos. Es por lo tanto necesario desarrollar normas sobre la forma en que esos textos podrían considerarse incorporados a un mensaje. El objetivo de esas normas, de ser posible, sería reducir en un medio electrónico las dificultades que plantean las batallas de los formularios en un medio de documentación escrita, o por lo menos asegurar que las soluciones incluidas en muchas leyes nacionales para resolver esas dificultades en un medio de comunicaciones por escrito se puedan aplicar también a un medio electrónico. Cabe señalar que la elaboración de dichas normas no implicaría necesariamente la modificación de las soluciones que puedan derivarse de las leyes nacionales existentes para resolver situaciones de "batallas de formularios".

86. Las normas para incorporar mensajes de datos por remisión en otros mensajes de datos, pueden también ser esenciales para el empleo de certificados de clave pública, dado que estos certificados suelen ser registros breves con un contenido estrictamente determinado de tamaño limitado. Sin embargo, es probable que el tercero de confianza que expide el certificado exija la inclusión de términos que limiten su responsabilidad. Por lo tanto, el alcance, la finalidad y el efecto de un certificado en la práctica comercial serían ambiguos e inciertos sin la incorporación por remisión de términos externos al mismo. Esto sucede particularmente en el contexto de las comunicaciones internacionales entre diversas partes que se rigen por prácticas y usos comerciales diferentes.

87. En anteriores períodos de sesiones del Grupo de Trabajo se dijo repetidas veces que el establecimiento de normas para incorporar mensajes de datos por remisión en otros mensajes de datos era fundamental para el crecimiento de una infraestructura comercial basada en computadoras. Sin la certidumbre jurídica que dan esas normas, las transacciones por computadora se verían sobrecargadas por la inclusión de grandes cantidades de material, lo que las haría muy inflexibles para las partes y para el sistema que facilita las comunicaciones. Sin esas normas uniformes, podría correrse el riesgo de que la aplicación de los métodos tradicionales para determinar la posibilidad de ejecutar los términos que se procura incorporar por remisión, fueran ineficaces cuando se los aplicase a términos comerciales electrónicos correspondientes, debido a diferencias entre los mecanismos tradicionales y electrónicos

del comercio. Por ejemplo, ciertos métodos jurídicos tradicionales aplicables a la incorporación por remisión pueden exigir pruebas de que los términos incorporados son "claros y conspicuos", que contienen "palabras de remisión adecuadas que demuestran la intención de incorporar" o que la intención de incorporar es "clara y convincente". Esos métodos pueden crear barreras no deseadas a la facilitación del comercio electrónico. Puede que se necesiten normas específicas, dado que los métodos usados para las notificaciones y para asegurar el acceso a la información pueden ser diferentes según que el medio de documentación para el comercio sea escrito o electrónico, con la posible consecuencia de que, en algunas jurisdicciones, las normas tradicionales sobre incorporación por remisión podrían dar lugar a una discriminación no justificada contra el comercio electrónico.

b) Accesibilidad del texto incorporado

88. El comercio electrónico se basa mucho en el mecanismo de la incorporación por remisión. Al mismo tiempo, el acceso al texto completo de la información a la que se hace referencia puede verse muy facilitado por el empleo de las comunicaciones electrónicas. Por ejemplo, un mensaje puede tener grabados localizadores de recursos uniformes (URL), que dirigen al lector al documento al que se hace referencia. Esos URL pueden proporcionar "enlaces de hipertexto" que permiten al lector apuntar un dispositivo como un ratón de computadora a una palabra clave asociada al URL y descargar el texto completo.

89. Los mismos métodos se pueden usar en un medio electrónico para asegurar el acceso fácil de todos los usuarios a diversos textos, por ejemplo: 1) textos que contienen prácticas comerciales establecidas (como la UCP 500); 2) normas técnicas que rigen la comunicación; 3) declaraciones de prácticas de certificación emitidas por autoridades certificadoras; y 4) información más concreta, como los términos y condiciones contractuales de una empresa. Sin embargo, no se puede confiar en los efectos jurídicos de estos métodos si no hay normas para incorporar mensajes de datos por remisión en otros mensajes de datos.

90. La necesidad de desarrollar normas para la incorporación por remisión en un medio electrónico resulta tanto de la frecuencia con que los mensajes de datos hacen referencia a información registrada en otra parte, como a la disponibilidad de los medios técnicos para que la verificación de esa información sea más fácil y más rápida que en un medio de comunicaciones escritas.

C. Posibles disposiciones

91. Al desarrollar disposiciones sobre incorporación por remisión para el comercio electrónico, el Grupo de Trabajo quizá desee tener presente que, en ciertas jurisdicciones, las normas existentes para un medio de comunicaciones escritas se basan en la preocupación por que los términos y demás información incorporada se señalen debidamente a la atención del remitente, o de un tercero, según sea el caso. Cuando existan dichas normas, puede ser conveniente aplicarlas indistintamente a la incorporación por remisión en un medio EDI o en cualquier otro tipo de comunicación.

92. No obstante, puede que sea posible formular un principio general que aclare que la incorporación por remisión es eficaz en el comercio electrónico, siempre que también se deje en claro que este principio no afecta a las normas que ya puedan existir acerca de: 1) la necesidad de que el contenido o la ubicación de los términos y otra información se señale a la atención de todas las partes a las que se aplique, o que se ponga a disposición de esas partes; o 2) cualquier requisito legal de que los términos sean aceptados antes de que puedan formar parte de un contrato. El principio esencial es que se reconozca el empleo de la incorporación por remisión, de modo que el hecho de que la información esté en otra parte no impida que sea incorporada en el mensaje de datos en el que se hace referencia a ella.

93. El Grupo de Trabajo quizá desee reanudar su examen de las cuestiones de la incorporación por remisión sobre la base de las dos variantes siguientes:

Variante A

A menos que se disponga otra cosa, cuando en un mensaje de datos se hace remisión total o parcial a directrices, normas, estándares, acuerdos, cláusulas, condiciones o términos [fácilmente][razonablemente] accesibles con la intención [aparente] de incorporarlos como parte del contenido, o de otra forma darle carácter jurídicamente vinculante, se presume que esos términos están incorporados por remisión a ese mensaje de datos. Entre las partes, esos términos serán tan vinculantes y jurídicamente efectivos como si se hubieran incorporado en su totalidad en el mensaje de datos, en la medida que lo permita la ley.

Variante B

1) El presente artículo se aplica cuando la información registrada o comunicada en un mensaje de datos hace remisión, o sólo se puede verificar plenamente por remisión a información registrada en otra parte ("la información restante").

2) Con sujeción a lo dispuesto en el párrafo 4, el mensaje de datos tendrá el mismo efecto que si la información restante estuviera plenamente expresada en él, y se pudiera determinar sólo por remisión a ella, siempre que el mensaje de datos:

a) identifique la información restante:

i) mediante un nombre o descripción colectiva; y

ii) indicando un registro, y las partes de ese registro, que contenga la información restante y, si ese registro no es del dominio público, el lugar donde se puede encontrar; y

b) indique expresamente o contenga una clara referencia a que el mensaje de datos tendrá el mismo efecto que si la información restante estuviese incluida en él en su totalidad.

3) Ninguna de las disposiciones del presente artículo afecta:

a) a ninguna norma jurídica que requiera la notificación adecuada del contenido de la información registrada en otra parte, o del registro o el lugar en que se puede encontrar dicha información, o que requiera que ese registro o lugar sean accesibles a otras personas; ni

b) a ninguna norma jurídica relativa a la aceptación de una oferta a los fines de la formación del contrato.