NACIONES
UNIDAS

A

Asamblea General

Distr. GENERAL
A/CN.9/437
12 de marzo de 1997

ESPAÑOL
Original: INGLÉS

COMISIÓN DE LAS NACIONES UNIDAS PARA EL
DERECHO MERCANTIL INTERNACIONAL
30º período de sesiones
Viena, 12 a 30 de mayo de 1997

INFORME DEL GRUPO DE TRABAJO SOBRE COMERCIO ELECTRÓNICO ACERCA DE LA LABOR DE SU 31º PERÍODO DE SESIONES
(Nueva York, 18 a 28 de febrero de 1997)

ÍNDICE

V.97-21493

ÍNDICE (continuación)

INTRODUCCIÓN

1. Tras la aprobación de la Ley Modelo de la CNUDMI sobre Comercio Electrónico (en adelante denominada "Ley Modelo"), la Comisión en su 29º período de sesiones (1996), hizo un examen de la labor futura en la esfera del comercio electrónico, sobre la base de 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 Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) debía continuar su labor de preparación de un régimen jurídico que introdujera un elemento de previsibilidad en el comercio electrónico, aumentando de esa manera el comercio en todas las regiones.

2. Se hicieron nuevas propuestas en cuanto a los posibles temas y prioridades de la labor futura. Una de ellas fue que la Comisión iniciara la preparación de un régimen jurídico para la firma numérica. Se dijo que en muchos países se consideraba que era indispensable para el desarrollo del comercio por vía electrónica que se definiera el régimen jurídico de la firma numérica y que se diera reconocimiento legal a las decisiones de las "autoridades de certificación" (denominadas en adelante "autoridades certificadoras") o de otras personas autorizadas para emitir certificados electrónicos u otras formas de garantía del origen y de la imputabilidad de los mensajes "firmados" numéricamente. Se observó que la fiabilidad de la firma numérica sería un factor decisivo para el desarrollo de la contratación por vía electrónica, así como para la transferibilidad por esa vía de los derechos sobre mercancías y de derechos de otra índole. En algunos países, se estaban preparando nuevas leyes sobre la firma numérica que, según se dijo, adolecían ya de falta de uniformidad. Si la Comisión decidiera emprender alguna labor en esa esfera, tendría la oportunidad de armonizar el nuevo régimen de la firma electrónica o al menos de establecer ciertos principios comunes al respecto, lo que proporcionaría una infraestructura internacional para la actividad comercial por vía electrónica.

3. Esta propuesta obtuvo considerable apoyo. Ahora bien, se opinó en general que si la Comisión decidía emprender alguna labor en la esfera de la firma numérica, por conducto de su Grupo de Trabajo sobre intercambio electrónico de datos, debería dar a ese Grupo un mandato bien definido. Se opinó además que, dado que no era posible que la CNUDMI acometiera la preparación de normas técnicas, convendría que se mantuviera al margen de los aspectos técnicos de la firma numérica. Se recordó que el Grupo de Trabajo había reconocido, en su 30º período de sesiones, que tal vez fuera preciso llevar a cabo alguna labor respecto de las autoridades certificadoras, y que era probable que esa labor debiera efectuarse en torno a la cuestión de los registros y de los proveedores de servicios. Ahora bien, el Grupo de Trabajo fue también entonces del parecer que no se debería tratar de los aspectos técnicos de la conveniencia de una u otra norma técnica que fuera aplicable en la materia (ibid., párr. 111). Se expresó la inquietud de que la labor relativa a la firma numérica se saliera del ámbito estricto del derecho mercantil, al afectar también a cuestiones más generales de derecho civil o administrativo. A ello se respondió que lo mismo cabía decir del régimen de la Ley Modelo, pero que la Comisión no debería abstenerse de preparar una normativa de utilidad reconocida por la mera razón de que su utilidad se extendiera más allá de las relaciones propiamente comerciales.

4. Otra propuesta basada en las deliberaciones preliminares del Grupo de Trabajo, fue la de que la labor futura se centrara en los proveedores de servicios. A ese respecto, se mencionaron como posible temas de estudio respecto de los proveedores de servicios: las normas de ejecución mínimas aplicables en ausencia de acuerdo entre las partes; el alcance del riesgo asumido por los destinatarios definitivos; la validez del régimen aplicable o de los acuerdos concertados frente a terceros; la asignación del riesgo de intusiones eventuales o de otros actos no autorizados; y el alcance de las garantías obligatorias, de haberlas, o de otras obligaciones contraídas al prestar servicios con valor añadido (ibid., párr. 116).

5. Muchos participantes opinaron que convendría que la CNUDMI examinara la relación entre los proveedores de servicios, los usuarios de esos servicios y los terceros interesados. Se dijo que sería importante dirigir esa actividad hacia el desarrollo de principios y normas internacionales de conducta comercial en esta esfera a fin de

favorecer el comercio por vía electrónica, en vez de adoptar como meta el establecimiento de un régimen reglamentario para los proveedores de servicios o de todo otro reglamento susceptible de ocasionar gastos inaceptables para las aplicaciones comerciales del intercambio electrónico de datos (EDI) (ibid., párr. 117). Sin embargo, algunos participantes opinaron que el tema de los proveedores de servicios tal vez fuera demasiado amplio y abarcara demasiados supuestos prácticos diferentes para ser tratado como un único tema de trabajo. Se convino en general en que las cuestiones relativas a los proveedores de servicios podrían ser tratadas como es debido en el marco de cada nueva esfera de su labor de que se ocupara el Grupo de Trabajo.

6. Se propuso además que la Comisión iniciara la preparación del nuevo régimen general necesario para aclarar cómo cabía tramitar por vía electrónica ciertas funciones tradicionales del contrato. Se dijo que el significado de "ejecución", "entrega" y otros términos estaba plagado de incertidumbres en el contexto del comercio electrónico, en el que la oferta y la aceptación de un contrato y la entrega de mercancías podían efectuarse en el mundo entero por vía de redes informáticas abiertas. El rápido crecimiento del comercio por vía informática y de las operaciones por internet y otras redes o circuitos similares explican que el tema haya pasado a ser prioritario. Se sugiere que la Secretaría aclare en un estudio el alcance de esa labor. De decidir la Comisión, una vez que haya examinado este estudio, proseguir esta tarea, una de las posibilidades sería la de incorporar el régimen así elaborado a la sección de "Disposiciones especiales" de la Ley Modelo.

7. También se propuso que la Comisión se ocupara de la incorporación por remisión. Se recordó que el Grupo de Trabajo había convenido en que este tema podría ser tratado adecuadamente en el marco más general de la labor que se emprendiera sobre los registros y los proveedores de servicios (ibid., párr. 114). La Comisión se mostró de acuerdo en que cabría tratar esta cuestión en el marco de la labor sobre las autoridades certificadoras.

8. Tras su deliberación, la Comisión convino en que sería conveniente colocar el tema de las firmas numéricas y de las autoridades certificadoras en el programa de la Comisión, con tal de que ello sirviera también de ocasión para examinar los otros temas que el Grupo de Trabajo había sugerido para su futura labor. Se convino igualmente en definir mejor el mandato del Grupo de Trabajo respecto del régimen uniforme que había de preparar que abarcaría las siguientes cuestiones: el fundamento jurídico de los procedimientos de certificación, incluidas las nuevas técnicas de certificación y autenticación numérica; la aplicabilidad de estos procedimientos de certificación; la asignación de los riesgos y de la responsabilidad entre los usuarios, los proveedores de servicios y los terceros eventualmente interesados, en el marco del empleo de estas técnicas de certificación; la problemática peculiar al empleo de registros para los fines de la certificación; y la incorporación por remisión.

9. La Comisión pidió a la Secretaría que preparara un estudio de antecedentes sobre las cuestiones relativas a la firma numérica y a los proveedores de servicios, a partir de un análisis de las leyes que se estaban preparando al respecto en diversos países. El Grupo de Trabajo examinaría, a la luz de ese estudio, la conveniencia y viabilidad de preparar un régimen uniforme sobre los mencionados temas. Se convino en que el Grupo de Trabajo se ocupara en su 31º período de sesiones de la preparación de algunos proyectos de regla sobre determinados aspectos de esos temas. Se pidió al Grupo de Trabajo que presentara a la Comisión suficientes elementos de juicio para adoptar una decisión fundada respecto del alcance del régimen uniforme que se había de preparar. En vista de la amplitud de las actividades objeto de la Ley Modelo y de la labor futura eventual en el campo del comercio electrónico, se decidió que el Grupo de Trabajo sobre intercambio electrónico de datos pasaría a denominarse "Grupo de Trabajo sobre comercio electrónico"[1]

10. El Grupo de Trabajo sobre Comercio Electrónico, integrado por todos los Estados miembros de la Comisión, celebró su 31º período de sesiones en Nueva York del 18 al 28 de febrero de 1997. Asistieron al período de sesiones

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

representantes de los siguientes Estados miembros del Grupo de Trabajo: Alemania, Argentina, Australia, Austria, Bulgaria, China, Egipto, Eslovaquia,
España, Estados Unidos de América, Federación de Rusia, Finlandia, Francia, Hungría, India, Irán (República Islámica del), Italia, Japón, Kenya, México, Polonia, Reino Unido de Gran Bretaña e Irlanda del Norte, Singapur, Tailandia y Uganda.

11. Asistieron al período de sesiones observadores de los siguientes Estados: Canadá, Colombia, Dinamarca, Gabón, Indonesia, Irlanda, Kuwait, Mauritania, Mongolia, República Checa, República de Corea, Suecia, Suiza y Turquía.

12. Asistieron al período de sesiones observadores de las siguientes organizaciones internacionales: Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD), Comisión Europea, Asociación Internacional de Abogados, Cámara de Comercio Internacional (CCI) y Unión Internacional de Abogados.

13. El Grupo de Trabajo eligió a los siguientes miembros de la Mesa:

Presidente: Sr. Mads Bryde ANDERSEN (Dinamarca);

Vicepresidente: Sr. PANG Khang Chau (Singapur);

Relator: Sr. Piotr AUSTEN (Polonia).

14. El Grupo de Trabajo tuvo ante sí los siguientes documentos: el programa provisional (A/CN.9/WG.IV/WP.70) y una nota de la Secretaría (A/CN.9/WG.IV/WP.71).

15. El Grupo de Trabajo aprobó el siguiente programa:

1. Elección de la Mesa.

2. Aprobación del programa.

3. Planificación de la labor futura sobre los aspectos jurídicos del comercio electrónico: firmas digitales, autoridades certificadoras y cuestiones jurídicas conexas.

4. Otros asuntos.

5. Aprobación del informe.

I. DELIBERACIONES Y DECISIONES

16. El Grupo de Trabajo deliberó acerca de las cuestiones relativas a la firma numérica, las autoridades certificadoras y otras cuestiones jurídicas conexas a la luz de la nota preparada por la Secretaría (A/CN.9/WG.IV/WP.71). Las deliberaciones y conclusiones del Grupo de Trabajo con respecto a esas cuestiones se consignan la sección II infra. El Grupo de Trabajo hizo asimismo un examen preliminar de las cuestiones involucradas en la incorporación por remisión y de su futura labor. En las secciones III y IV del presente informe puede verse reflejado ese examen.

II. CUESTIONES JURÍDICAS Y POSIBLE CONTENIDO DEL RÉGIMEN UNIFORME PARA LA FIRMA NUMÉRICA

A. Observaciones generales

17. Antes de examinar el posible contenido del régimen uniforme para la firma numérica y las cuestiones jurídicas conexas, el Grupo de Trabajo intercambió opiniones sobre el alcance de su labor y estudió las iniciativas nacionales en curso relativas a las cuestiones jurídicas que planteaban las firmas digitales y las autoridades legalizadoras.

18. El Grupo de Trabajo recibió información sobre las medidas nacionales en curso relativas a las cuestiones jurídicas planteadas por las firmas digitales. En varios países se estaba examinando cuál era el régimen jurídico adecuado para los instrumentos capaces de realizar, en un medio de documentación electrónico, funciones análogas a las de la firma manuscrita en un medio de documentación escrita. Aunque en algunos países el examen de esta cuestión estaba todavía en una fase preliminar, según los informes recibidos otros países ya habían aprobado leyes relativas a las firmas digitales o estaban elaborando normas sobre esa materia basándose en la Ley Modelo de la CNUDMI sobre el Comercio Electrónico. Muchas de esas leyes basaban la utilización de las firmas digitales en el cifrado de claves públicas y en autoridades legalizadoras. En cuanto a su ámbito y grado de detalle esas leyes podían ser generales, concebidas para permitir la utilización de las firmas digitales como forma de autenticar mensajes electrónicos, o ser más detalladas y establecer las bases jurídicas del funcionamiento de las autoridades legalizadoras. También podían abarcar diversas cuestiones de política oficial, como la creación del marco administrativo que precisaba una infraestructura de claves públicas; la utilización de la criptografía para las firmas digitales o para garantizar el carácter confidencial de los documentos; la protección de los consumidores; y la posibilidad de que los poderes públicos controlasen el acceso a la información cifrada mediante, por ejemplo, un depósito de claves bloqueado. El Grupo de Trabajo fue informado también de las iniciativas regionales de armonización que se estaban llevando a cabo en varias organizaciones internacionales.

19. Se consideró que el régimen jurídico de los instrumentos utilizados para realizar funciones equivalentes a las de las firmas manuscritas, como las firmas digitales y otras firmas electrónicas, era una de las principales cuestiones que había que abordar para fortalecer las bases jurídicas del comercio electrónico. Existía el convencimiento generalizado de que la falta de una regulación jurídica de las firmas digitales y otras firmas electrónicas podía obstaculizar las transacciones económicas efectuadas por medios electrónicos. También existía el convencimiento de que la diversidad de planteamientos y posibles soluciones que se estaban examinando en el plano nacional justificaba la labor armonizadora de la CNUDMI. Se consideró que la CNUDMI, además de ofrecer orientación sobre las bases jurídicas en que debían apoyarse los Estados para aprobar leyes sobre firmas digitales y otras firmas electrónicas, debería concentrarse en los requisitos para el reconocimiento de la legalización efectuada por autoridades extranjeras. Se dijo que la CNUDMI podría también facilitar ese proceso estableciendo unos requisitos mínimos, admitidos internacionalmente, para habilitar a las autoridades legalizadoras.

20. El Grupo de Trabajo debatió si debía ocuparse exclusivamente de las firmas digitales (es decir, las técnicas en que se utilizaba el cifrado de claves públicas, también llamado cifrado de doble clave) o si debía ocuparse también de otras firmas electrónicas. Se observó que, además, se estaban desarrollando técnicas distintas del cifrado de claves públicas, conocidas generalmente como firmas electrónicas, con la finalidad de cumplir las funciones habituales de las firmas manuscritas. Esas técnicas comprendían la utilización de códigos o "contraseñas" o instrumentos de identificación biométrica y podían coexistir con un sistema de firmas digitales basado en una infraestructura de claves públicas. Se destacó que en el medio de documentación escrita las formalidades y requisitos de autenticación y legalización no eran necesarios en determinadas transacciones. Se afirmó que las firmas digitales basadas en una infraestructura de claves públicas entrañaban una mayor seguridad jurídica, pero que podía haber otras técnicas útiles de identificación y autenticación para los casos en que fuese menor el grado de seguridad jurídica requerido. Se dijo que el Grupo de Trabajo no debía dar la impresión errónea de que era contrario a la utilización de esas otras técnicas por el hecho de concentrarse únicamente en las firmas digitales. A este respecto, se afirmó que la utilización de las firmas digitales basadas en el cifrado de claves públicas no suponía necesariamente la obtención de la máxima seguridad jurídica. Las técnicas relativas a las firmas digitales tenían la flexibilidad suficiente para ofrecer también un menor grado de seguridad a un costo menor.

21. El sentir general fue que el propósito de las normas uniformes sobre firmas electrónicas debía ser mostrar al legislador la gran variedad de funciones de autenticación que podían realizarse en un medio de documentación electrónico. Esas funciones se ordenaban en lo que se denominó una "escala móvil": desde el máximo grado de seguridad (análogo a la legalización notarial y otras legalizaciones escritas) al mínimo grado de seguridad de las señales manuscritas o los sellos. Sin embargo, una de las dificultades de la labor en el campo de las firmas electrónicas era el hecho de que, para proporcionar el grado de orientación necesario a los efectos de aplicar los principios del artículo 7 de la Ley Modelo, las futuras normas uniformes tal vez tendrían que apartarse de un planteamiento puramente funcional y centrarse con cierto detalle en la forma en que una técnica determinada podía cumplir las funciones mencionadas.

22. Existía el convencimiento generalizado de que, habida cuenta de la neutralidad de la Ley Modelo en cuanto a los medios, las normas uniformes que había de preparar el Grupo de Trabajo no debían oponerse a la utilización de ninguna técnica que ofreciera un método con la seguridad necesaria como alternativa a las firmas manuscritas y otras firmas escritas con arreglo al artículo 7 de la Ley Modelo. Sin embargo, para facilitar sus deliberaciones, el Grupo de Trabajo decidió que su labor se centrara inicialmente en las cuestiones relativas a las firmas digitales, que eran más conocidas que otras técnicas a causa de la legislación y la doctrina jurídica. Se interpretó en general que, cuando conviniera, el examen podría adoptar un planteamiento más general y que también se podrían considerar cuestiones relativas a otras técnicas de firma electrónica.

23. En cuanto al ámbito de su labor, se generalizó la idea de que el Grupo de Trabajo no debía ocuparse de las cuestiones relativas a la utilización de la criptografía con fines de seguridad. Estas cuestiones, que ya se estaban examinando en otros foros internacionales, como la Organización de Cooperación y Desarrollo Económicos (OCDE), eran muy complejas, no estaban directamente relacionadas con la ejecución de un programa de firmas digitales y podían retrasar el examen del Grupo de Trabajo, que debía centrar su labor en facilitar el comercio electrónico. Se consideró en general que las futuras normas uniformes no debían ocuparse de ninguna de las cuestiones de seguridad nacional, política pública o derecho penal o administrativo que pudiera suscitar la ejecución de los programas de firmas digitales.

24. Se expresaron diversas opiniones acerca de si el Grupo de Trabajo debía ocuparse también de la protección de los consumidores. Según una opinión, esas cuestiones debían excluirse del ámbito de trabajo, que debía referirse exclusivamente a las transacciones comerciales. Según otra opinión, aunque las cuestiones principales que había que examinar no se relacionaban intrínsecamente con los consumidores, convenía estudiar, al preparar las normas uniformes sobre firmas digitales, si era necesario establecer normas diferentes para las transacciones realizadas por consumidores. Se acordó, previo debate, que el Grupo de Trabajo se centraría fundamentalmente en las transacciones comerciales, pero que tendría en cuenta los posibles efectos de las cuestiones examinadas en las transacciones realizadas por consumidores.

B. Cuestiones jurídicas específicas y proyectos de disposición sobre la firma numérica

25. Se expresaron diversas opiniones con respecto a la clase de labor que realizaría el Grupo de Trabajo. Según una de ellas, sería prematuro que la labor del Grupo de Trabajo sobre las cuestiones relativas a las firmas digitales y cuestiones conexas diese como producto una legislación modelo. Según otra opinión, el Grupo de Trabajo debería considerar, al menos hipotéticamente, la posibilidad de que su labor futura sobre las cuestiones relacionadas con las firmas digitales y cuestiones conexas diese como producto una adición a la Ley Modelo. Como se recordará, en su 29º período de sesiones, la Comisión había pedido al Grupo de Trabajo que examinara la conveniencia y la viabilidad de preparar unas normas uniformes sobre las cuestiones relacionadas con las firmas digitales y las autoridades certificadoras. La Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) había

convenido en que la labor del Grupo de Trabajo en el presente período de sesiones podría entrañar la elaboración de proyectos de normas sobre determinados aspectos de los citados temas (véase párr. supra).

26. Tras el correspondiente debate, el Grupo de Trabajo aplazó su decisión con respecto al producto de su labor futura hasta que hubiera acabado de examinar las cuestiones jurídicas de fondo pertinentes. Aplazó también el estudio de la relación precisa que habría entre el producto de su labor futura y la Ley Modelo. Se convino en que las posibles normas uniformes en materia de firmas digitales deberían emanar del artículo 7 de la Ley Modelo y servir de ejemplo de aplicación de un método fiable "para identificar a una persona" y "para indicar que esa persona aprueba" la información que figura en un mensaje de datos. En un plano más general, la labor futura sobre firmas digitales debería atenerse a los principios expresados en la Ley Modelo y a su terminología.

27. El Grupo de Trabajo partió de la hipótesis de que el producto de su labor futura en ese ámbito consistiría en un proyecto de disposiciones reglamentarias. Sin embargo, algunos opinaron que el Grupo de Trabajo podría considerar necesario dar explicaciones adicionales, tal vez mediante un preámbulo, mediante una guía de aplicación de las disposiciones reglamentarias uniformes o mediante la elaboración de unas directrices independientes, sobre todo en lo que respecta a las cuestiones que no se prestaran a unificación. Por ejemplo, se dijo que la CNUDMI podría formular observaciones de utilidad educativa sobre las diversas cuestiones suscitadas por la creación de infraestructuras públicas esenciales.

28. Se decidió que el Grupo de Trabajo prosiguiera sus deliberaciones tomando como base el proyecto de disposiciones uniformes que figura en la nota de la Secretaría (A/CN.9/WG.IV/WP.71, párrs. 52 a 76). Se señaló que ese proyecto de disposiciones tenía un carácter muy provisional y hubo acuerdo general en que, en lugar de centrarse en la redacción de cada artículo particular, debería aprovecharse el examen de ese proyecto de disposiciones para debatir el marco conceptual en que podrían basarse las normas uniformes sobre firmas digitales. Hubo consenso general en que, al debatir las cuestiones tratadas en el proyecto de disposiciones, el Grupo de Trabajo debería plantearse lo siguiente: a) si la uniformidad era necesaria; b) si la cuestión se trataba de manera suficientemente exhaustiva en la Ley Modelo o si sería deseable elaborar unas disposiciones más detalladas; c) si la cuestión era una cuestión propia de las firmas digitales o si podría tratarse en un plano más general; d) si la cuestión afectaba directamente al derecho mercantil internacional, al mandato de la CNUDMI y a su ámbito de competencia, y e) si era necesario promulgar unas normas vinculantes o debería prevalecer la autonomía de las partes.

1. Definiciones

29. Se consideró inicialmente que el Grupo de Trabajo debería considerar la posibilidad de adoptar otras definiciones aparte de los proyectos de definición de "firma digital", "autoridades certificadoras autorizadas" y "certificados" indicados en la nota de la Secretaría (A/CN.9/WG.IV/WP.71, párrs. 52 a 60). Se propusieron las siguientes definiciones: "'clave privada' es la clave del par de claves utilizada para crear una firma digital"; "'clave pública' es la clave del par de claves utilizada para verificar una firma digital"; "'Par de claves' designa, en un código criptográfico asimétrico, una clave privada y su correspondiente clave pública, relacionada matemáticamente con ella; con la característica de que la clave pública sirve para verificar la firma digital creada por la clave privada". El Grupo de Trabajo tomó nota de la propuesta. Hubo quien opinó que las definiciones propuestas eran, en cierta medida, redundantes. En un plano más general, se previno contra la introducción de una multiplicidad de definiciones en unas normas uniformes de carácter reglamentario, que podría ir en contra de la tradición legislativa de muchos países. Tras el correspondiente debate, se llegó a un acuerdo general sobre la posibilidad de reconsiderar, en una etapa posterior, la adición de un número limitado de definiciones.

a) Firma numérica

30. El Grupo de Trabajo debatió la definición de "firma digital" sobre la base del siguiente proyecto de disposiciones:

"Proyecto de artículo A

1) Una firma numérica es un valor numérico que se consigna en un mensaje de datos y que, gracias al empleo de 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 numéricas autorizadas a tenor de [la presente Ley] [las presentes Reglas] se basan en el cifrado de la clave pública. Aplicados a un mensaje de datos, esos procedimientos matemáticos operan una transformación del mensaje que permite que una persona, que disponga del mensaje inicial y de la clave criptográfica pública del iniciador, determine con exactitud.

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) Toda firma numérica consignada en un mensaje de datos se considerará autorizada si se puede verificar de conformidad con los procedimientos establecidos por una entidad certificadora autorizada con arreglo a [la presente Ley] [las presentes Reglas].

4) [La autoridad competente del Estado que promulgue la presente Ley o las presentes Reglas] reglamentará en detalle los requisitos técnicos que se deberán observar al consignar una firma numérica y al verificarla."

Párrafos 1) y 2)

31. Se expresó la opinión de que la definición de "firma digital" debería ampliarse para incluir no sólo la clave criptográfica pública sino también otros tipos de firma electrónica. No obstante, la opinión predominante fue que no sería apropiado tratar de crear una definición de "firma digital" que se alejara de los usos existentes. Se convino en que, si bien el concepto de "firma digital" debería limitarse a fin de incluir solamente la criptografía asimétrica, quizá sería necesario contar con otras definiciones para incluir otras técnicas a las que podría aludirse en términos amplios dentro del concepto de "firmas electrónicas".

32. En relación con el párrafo 1), se sugirió que la expresión "determinar que este valor numérico se ha obtenido exclusivamente" debería reemplazarse por la expresión "determinar que este valor numérico se ha obtenido de manera inequívoca sólo". El Grupo de Trabajo decidió que, en una etapa tan temprana de sus deliberaciones, no debería examinar en detalle la redacción del texto. Se consideró en general que los párrafos 1) y 2) reflejaban adecuadamente el fondo del concepto de "firma digital" en la forma que podría emplearse para delimitar el alcance de la labor futura. Finalizado el debate, el Grupo de Trabajo consideró en general aceptable el fondo de los párrafos 1) y 2).

Párrafo 3)

33. Se plantearon varios interrogantes en relación con el propósito del párrafo 3). Se expresó la opinión de que el párrafo no era adecuado para introducir las nociones de infraestructura de clave pública y verificación de firmas digitales y que, en cambio, abordaba cuestiones de fondo que no correspondían a la definición de "firma digital". Se dijo que se podría interpretar que el párrafo 3) introducía un procedimiento de verificación como requisito para la validez de la firma digital. Se sugirió que sería preferible eliminar el párrafo 3) y reemplazarlo por una definición descriptiva de la "verificación" de las firmas.

34. Se señaló que se podría interpretar que el párrafo 3) abordaba únicamente la validez de las firmas digitales que se empleaban en el contexto de una infraestructura de clave pública a cargo de las autoridades estatales. Se consideró que, en su redacción actual, la disposición era excesivamente rígida, ya que podría excluir el reconocimiento del uso de firmas digitales en cualquier otro contexto, como el de las infraestructuras de clave pública a cargo de entidades que no fuesen autoridades estatales. Se consideró en general que no sería conveniente afectar las transacciones que se podrían realizar en círculos cerrados entre partes que no considerasen necesario emplear los servicios de una autoridad certificadora. En un momento en que los Estados estaban todavía examinando varias opciones para la infraestructura de clave pública, se señaló que sería prematuro formular en las normas uniformes un sistema particular de infraestructura de clave pública en detrimento de los demás.

35. Se expresó la opinión de que, si bien el párrafo 3) debía leerse junto con el artículo 7 de la Ley Modelo, quizá las dos disposiciones no fueran totalmente coherentes entre sí. Por ejemplo, el párrafo 3) calificaba el concepto de "firma digital" haciendo referencia a la firma digital "autorizada", expresión que no se empleaba en el contexto del artículo 7 de la Ley Modelo. Igualmente, el artículo 7 de la Ley Modelo hacía referencia al uso del método de firma "tan fiable como sea apropiado para los fines para los que se generó o comunicó el mensaje de datos", admitiendo en consecuencia que existen distintos niveles de fiabilidad, según los propósitos para los cuales se generó o comunicó el mensaje de datos, incluidos los acuerdos celebrados entre las partes. Se señaló que, de conformidad con el artículo 7 de la Ley Modelo, si las partes en una transacción tenían suficiente confianza mutua podían convenir en un nivel de seguridad que consideraran adecuado para las circunstancias, sin necesidad de recurrir a una autoridad certificadora. Desde el punto de vista de las partes, la consideración esencial era si consideraban fiable el sistema empleado. Se dijo que había varios factores pertinentes para determinar la fiabilidad del equipo, los programas de computadora y los procedimientos utilizados por las partes (por ejemplo, si eran relativamente seguros desde el punto de vista de la invasión y el uso indebido; si tenían un nivel razonable de disponibilidad, fiabilidad y funcionamiento correcto; si eran razonablemente adecuados para cumplir la función prevista; y si se los utilizaba de conformidad con los principios de seguridad generalmente aceptados. En consecuencia, correspondía a las partes decidir si en

las normas de fiabilidad que exigían se debería incluir un procedimiento de verificación aplicado por una autoridad certificadora. En el párrafo 3) se da a entender que las firmas digitales sólo serían fiables si se pudiesen certificar con la asistencia de una autoridad certificadora. En consecuencia, se consideró que era más restrictivo que el artículo 7 de la Ley Modelo. Se dijo que sería necesario revisar a fondo el párrafo 3) para armonizarlo con el artículo 7 de la Ley Modelo.

36. También se plantearon algunas cuestiones en relación con la referencia que se hace en el párrafo 3) a la verificación de la firma digital de conformidad con los procedimientos establecidos por la autoridad certificadora. Se manifestó que la referencia a esos procedimientos planteaba la cuestión de las instrucciones técnicas aplicadas para la verificación de las firmas digitales y de otros criterios operativos observados por la autoridad certificadora, o de los efectos jurídicos que se producirían si en un caso determinado no se aplicaran esos procedimientos. No obstante, se trataba de cuestiones de fondo que no se podían abordar adecuadamente dentro del alcance limitado del proyecto de artículo A. En consecuencia, se sugirió que se debería suprimir del párrafo 3) la referencia a los procedimientos de verificación.

37. Tras haber examinado las distintas opiniones, el Grupo de Trabajo decidió suprimir el párrafo 3). Se convino en que sería necesario reabrir el debate sobre las distintas posibilidades para la infraestructura de clave pública después de haber examinado los efectos jurídicos de las firmas digitales.

Párrafo 4)

38. Se expresó la opinión de que, en la medida en que este artículo exigía que el Estado estableciera normas técnicas para las firmas digitales, excluía aparentemente las infraestructuras de clave pública a cargo de entidades que no fuesen estatales. Para ser coherente con su decisión de eliminar el párrafo 3) y habida cuenta de la relación lógica existente entre las dos disposiciones, el Grupo de Trabajo decidió que también debía eliminarse el párrafo 4).

b) Autoridades certificadoras autorizadas

39. El Grupo de Trabajo examinó la definición de "autoridad certificadora autorizada" tomando como base el siguiente proyecto de disposición:

"Proyecto de artículo B

1) El ... [Estado que promulgue la presente Ley o las presentes Reglas designará al órgano o a la autoridad competente para facultar a las autoridades certificadoras] podrá conceder a toda autoridad certificadora una autorización para actuar en cumplimiento de [la presente Ley] [las presentes Reglas]. Esta autorización será revocable.

2) El ... [Estado que promulgue la presente Ley o las presentes Reglas designará al órgano o a la autoridad competente para promulgar reglamentos relativos a las autoridades de certificación autorizadas] podrá reglamentar las condiciones para la concesión de dichas autorizaciones, y promulgar el reglamento de funcionamiento de las autoridades certificadoras.

3) Las autoridades certificadoras autorizadas podrán emitir certificados relativos a las clave criptográficas de personas naturales o jurídicas.

4) Las autoridades certificadoras autorizadas podrán prestar o facilitar servicios de inscripción registral y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones respecto de toda comunicación.

5) El ... [el Estado que promulgue la presente Ley o las presentes Reglas designará al órgano o a la autoridad competente para reglamentar en detalle las funciones que deben cumplir las autoridades de certificación autorizadas] podrá reglamentar más en detalle las funciones que deben cumplir las autoridades de certificación autorizadas en relación con la emisión de certificados a personas jurídicas o naturales."

40. El Grupo de Trabajo realizó un intercambio general de opiniones sobre el planteamiento que debería de adoptarse en relación con las autoridades certificadoras. Según una opinión, el proyecto de artículo B, tal como estaba formulado, parecía prescribir un método concreto para establecer una infraestructura de clave pública, siendo así que sería preferible dejar que cada uno de los Estados que incorporasen el nuevo régimen adoptase sus propias normas al respecto. Se indicó que, si bien las autoridades certificadoras podían desempeñar una función fundamental de fomento de la confianza en las firmas digitales, no resultaba inconcebible que los sistemas de firma digital operasen cuando no hubiese autoridades certificadoras. Por otra parte, se manifestó que el establecimiento de un mecanismo de derecho público para autorizar la actuación de las autoridades certificadoras no fomentaría necesariamente la confianza en las firmas digitales, objetivo éste que sería más fácil de alcanzar recurriendo a autoridades certificadoras de designación privada o a otros instrumentos de mercado. Según otra opinión, el proyecto de artículo B era aceptable en términos generales a los efectos de definir el concepto de autoridades certificadoras, dada su permisiva redacción, particularmente en su párrafo 2, que no impedía que el Estado que incorporase el nuevo régimen recurriera a otros métodos para poner en marcha su infraestructura de clave pública.

41. Con objeto de que se examinaran los posibles enfoques que debían adoptarse para abordar la cuestión de las autoridades certificadoras, se invitó al Grupo de Trabajo a considerar dos posibles objetivos que podrían alcanzarse mediante la adopción de una definición de "autoridad certificadora". Uno de esos objetivos podría ser facilitar orientaciones a los Estados que incorporasen el nuevo régimen en relación con elementos fundamentales que habrían de tenerse en cuenta al poner en marcha las infraestructuras nacionales de clave pública. Se indicó que el proyecto de artículo B carecía de la suficiente precisión para facilitar las debidas orientaciones al respecto. Otro posible objetivo sería permitir que la puesta en marcha de las infraestructuras de clave pública corriese a cargo de cada Estado, en tanto que en la definición de "autoridad certificadora" se determinarían los criterios que tendría que aplicar cada Estado para reconocer los certificados expedidos por las autoridades certificadoras extranjeras. Se dijo que, en caso de que el Grupo de Trabajo desease que el proyecto de normas uniformes persiguiese únicamente este último objetivo, habría que añadir un párrafo inicial al proyecto de artículo B, redactado en términos similares a los siguientes: "Las presentes disposiciones uniformes se aplicarán a los certificados expedidos de conformidad con un régimen jurídico que reúna las características siguientes:". No obstante, se consideró que, si se aprobase, esa propuesta exigiría una revisión a fondo de las restantes disposiciones del proyecto de artículo B. Según otra opinión, no se debería establecer ningún criterio concreto en el proyecto de artículo B, cuyo límite sería, a ese respecto, la declaración general del párrafo 2. Podrían formularse otras reservaciones, en una guía para la incorporación del proyecto de normas uniformes que incluiría una lista ilustrativa de los posibles criterios que podrían tener en cuenta los Estados.

42. El Grupo de Trabajo convino en que podría ser necesario examinar posteriormente la cuestión de determinar si era preciso que se definiera el concepto de "autoridad certificada" en el proyecto de normas uniformes a efectos distintos de definir los criterios que habrían de aplicar los Estados que incorporasen el nuevo régimen para reconocer los certificados expedidos por las autoridades certificadoras extranjeras. En general se consideró que, aunque la adopción de normas o criterios podría ser de utilidad a las autoridades certificadoras para generar el grado de confianza necesario en su actuación, tal vez fuera preciso distinguir entre la cuestión general de la confianza en las autoridades certificadoras, que podía estar en función del instrumento jurídico constitutivo de esas autoridades, y las cuestiones más concretas del grado de confianza en los certificados concretos que expidiese la autoridad certificadora.

43. Se expresó la opinión de que las disposiciones relativas a las funciones y obligaciones de las autoridades certificadoras, como las que figuraban en el proyecto de artículo B, tenían importancia no sólo porque constituían

elementos estructurales de un sistema de autoridades certificadoras (por ejemplo, la infraestructura de clave pública), sino también porque servían para determinar los efectos que había que atribuir a las firmas digitales y los actos conexos o que entrañasen utilización de firmas digitales. A la vista de esas circunstancias, se indicó que, al examinar el tema, podría ser útil que el Grupo de Trabajo tuviese en cuenta una serie de factores necesarios para determinar los efectos jurídicos que había que atribuir a las firmas digitales. A este respecto se manifestó que el Grupo de Trabajo debería examinar los factores siguientes, habida cuenta de su valor como instrumento de análisis: a) los tipos de firma (que, en orden decreciente de generalidad, incluían las firmas electrónicas; las firmas digitales; la firma digital certificada y la firma digital certificada por una autoridad certificadora oficialmente autorizada); b) las partes afectadas (es decir, las partes directamente contratantes, incluidas las autoridades certificadoras; las terceras partes, como los expedidoras y bancos; las entidades gubernamentales; y otros agentes como las empresas de servicios y las empresas de comunicaciones); c) los actos o circunstancias a los que había que atribuir efectos jurídicos (es decir, la utilización de la firma digital; la expedición de un certificado, incluida la expedición sin autorización; la expiración de un certificado; la revocación de un certificado; la revocación de una autorización concedida a una autoridad certificadora; d) el alcance de la labor de la CNUDMI en ese ámbito (alcance internacional únicamente; alcance internacional y formulación de propuestas para su incorporación al derecho interno; formulación de propuestas para su incorporación al derecho interno); e) los efectos jurídicos (es decir, la validez; las obligaciones del órgano expedidor de certificados y de las personas que hiciesen valer esos certificados; los recursos; la responsabilidad, incluidos sus límites; y la prueba); f) las técnicas de redacción (es decir, la determinación de normas; los efectos jurídicos en caso de que se cumpliesen las normas; los efectos jurídicos en caso contrario). El Grupo de Trabajo consideró que la lista de factores propuesta era un instrumento útil para facilitar su análisis del objetivo y las consecuencias de las disposiciones relativas a las autoridades certificadoras.

44. En sus siguientes debates, el Grupo de Trabajo examinó la cuestión de si sería conveniente que el proyecto de normas uniformes incluyese criterios de actuación de las autoridades certificadoras, con independencia de que estuviesen o no estuviesen autorizadas.

45. Se dijo que, al margen de las disposiciones que ya contenía, el proyecto de artículo B debería complementarse con normas uniformes en las que se indicasen concretamente los criterios que habría que tener en cuenta para autorizar la actuación de las autoridades certificadoras o, en su defecto, definir los criterios mínimos que deberían reunir esas autoridades para que se reconociesen jurídicamente los certificados que expidiesen. La referencia a esos criterios era necesaria para que en el proyecto de normas uniformes se regulase la cuestión de las autoridades certificadoras. Se recordó que en el párrafo 44 de la nota de la Secretaría (A/CN.9/WG.IV/WP.71) figuraba una lista de factores que podrían tenerse en cuenta al determinar si una autoridad certificadora era digna de confianza. En general, se consideró que esa lista constituía un punto de partida adecuado en caso de que el Grupo de Trabajo desease examinar más detenidamente la cuestión. Se manifestó que algunos de esos criterios podrían hacerse extensivos a factores como la competencia del personal a nivel administrativo o la separación de la función certificadora de otras operaciones que pudiese realizar la autoridad certificadora.

46. Se formularon objeciones a la inclusión en el proyecto de normas uniformes en relación con los criterios de actuación de las autoridades certificadoras. Se recordó al Grupo de Trabajo que, en su debate anterior, había examinado el papel de las autoridades públicas en la puesta en marcha de infraestructuras de clave pública y la posibilidad de que, en algunos Estados, las entidades privadas desempeñasen funciones certificadoras sin necesidad de la previa autorización de la administración pública (véanse los párrafos __). Además, se podrían considerar otras alternativas aceptables a los criterios aprobados por la administración pública, como los usos y prácticas mercantiles reconocidos internacionalmente o criterios de competencia establecidos por entidades no gubernamentales dignas de confianza, como ocurría en determinados ámbitos mercantiles. Se consideró que la propuesta de incluir criterios que habría que tener en cuenta al autorizar a actuar a las autoridades certificadoras no sería pertinente ni adecuada en el caso de las autoridades certificadoras que no actuasen amparadas por una autorización de la administración pública. Además, la inclusión de esos criterios exigiría determinar cuál era la entidad o autoridad competente para

resolver si una autoridad certificadora se ajustaba a los criterios indicados. Ese sistema daría lugar a dificultades en el caso de las autoridades certificadoras que actuasen al margen de la infraestructura de clave pública que hubiese establecido la administración.

47. En respuesta a esas objeciones, se recordó que la adopción de criterios comúnmente aceptados en lo concerniente a la actuación de las autoridades certificadoras podría ser una medida importante con miras a generar confianza en las firmas digitales. Esos criterios tal vez no fuesen necesarios siempre que las transacciones electrónicas tuviesen lugar entre partes que actuasen dentro de un sistema cerrado al que considerasen suficientemente digno de confianza. Los socios que actuasen dentro de esos sistemas cerrados podrían, de hecho, prescindir de los certificados expedidos por las autoridades certificadoras. No obstante, con objeto de propiciar una mayor utilización de las firmas digitales, sería necesario fomentar la confianza de la opinión pública en general respecto de la autenticidad de las firmas y de la fiabilidad de los métodos utilizados para verificarlas. Un importante método para lograr ese objetivo era asegurar a la opinión pública que las entidades encargadas de certificar la autenticidad de una clave pública tenían que ajustarse a determinados criterios establecidos para garantizar su fiabilidad. Aunque el Grupo de Trabajo no debería descartar la función que podían desempeñar los usos y prácticas mercantiles o las entidades no gubernamentales con miras al establecimiento de normas aceptables de actuación para un determinado ámbito de actividad mercantil, se destacó que no se contaba aún con ninguna práctica arraigada para establecer criterios aceptables de actuación de las autoridades certificadoras.

48. Se manifestó que tal vez no fueran mutuamente excluyentes las dos alternativas que se examinaban, a saber, el establecimiento de criterios para la concesión de autorizaciones administrativas a las autoridades certificadoras y el reconocimiento de criterios de actuación de las autoridades certificadoras que operasen fuera de una infraestructura de clave pública puesta en marcha por la administración pública. La diferencia entre esas dos situaciones podía estribar en los efectos jurídicos atribuidos a las firmas digitales en uno u otro caso. En el caso de las autoridades certificadoras autorizadas por la administración pública, el cumplimiento de los criterios de actuación aplicables por una autoridad certificadora constituiría un requisito previo para proceder a la autorización de una autoridad certificadora; a su vez, ese requisito constituiría una condición para el reconocimiento de la eficacia jurídica de los certificados expedidos por esa autoridad certificadora. En la segunda situación, una autoridad certificadora no tendría que demostrar que se ajustaba a los criterios de actuación antes de comenzar a desempeñar sus funciones. No obstante, en caso de que se impugnaran los certificados expedidos por ella (por ejemplo, en un litigio o en un proceso de arbitraje), el órgano encargado de pronunciarse sobre la impugnación tendría que juzgar el grado de fiabilidad del certificado, para lo cual tendría que determinar si fue expedido por una autoridad certificadora que se ajustaba a esos criterios.

49. Se expresó el parecer de que el grado de fiabilidad de un certificado pudiera depender de los actos de la entidad certificadora respecto de ese certificado en particular, y no de factores institucionales. Esta fiabilidad "operacional" no dependería necesariamente de la índole autorizada o no de la entidad certificadora o del reconocimiento internacional de los usos y prácticas observados por esa entidad. Se sugirió que el criterio de la fiabilidad dependería del motivo para el que se hubiera de determinar esa fiabilidad (por ejemplo, la certificación recíproca, la concesión de una licencia, la determinación de la responsabilidad).

50. Habida cuenta de la etapa inicial en que se encontraban las deliberaciones del Grupo de Trabajo y las opiniones contrapuestas expresadas al respecto, se apoyó en general la propuesta de que el Grupo de Trabajo siguiese considerando ambas alternativas como posibles hipótesis de trabajo y volviese a ocuparse de ellas una vez que hubiese examinado otras cuestiones intrínsecamente relacionadas con el tema, como la cuestión de la responsabilidad de las autoridades certificadoras y la cuestión de la certificación transfronteriza.

2. Responsabilidad

51. El Grupo de Trabajo basó su examen de la responsabilidad de las autoridades certificadoras en el siguiente proyecto de disposición:

"Proyecto de artículo H

1) Una entidad certificadora autorizada será responsable ante toda persona que haya actuado de buena fe en la confianza inspirada por un certificado emitido por ella, respecto de cualquier pérdida debida a algún defecto de inscripción que le sea imputable a ella, o que sea debida a alguna avería técnica o circunstancia similar, [aun cuando la pérdida no sea imputable] [cuando la pérdida sea imputable] a negligencia de la entidad certificadora.

2) Variante X La responsabilidad por cada pérdida no excederá de [cantidad]. ... [el Estado que incorpore a su derecho interno la presente Ley o las presentes Reglas designará al órgano o a la autoridad competente para revisar la cantidad máxima] podrá revisar esta cantidad cada dos años con miras a reflejar en ella la evolución de los precios.

Variante Y ... [el Estado que incorpore la presente Ley o las presentes Reglas designará al órgano o a la autoridad competente para reglamentar la cuestión de la responsabilidad] podrá promulgar reglamentos sobre la responsabilidad de las entidades certificadoras.

3) Cuando la parte que sufrió la pérdida haya contribuido a ella por algún acto deliberado o negligente, la indemnización podrá ser reducida o denegada.

[4) De serle notificada la revocación de un certificado, la entidad certificadora autorizada deberá inscribir al instante dicha revocación. De no hacerlo así, la entidad adjudicadora será responsable de toda pérdida que por ese motivo pueda sufrir el usuario.]"

Párrafos 1) y 2)

Observaciones generales

52. El Grupo de Trabajo procedió a un debate acerca del ámbito y las consecuencias de las normas propuestas sobre la responsabilidad de las autoridades certificadoras. Se señaló que esta cuestión se refería a dos tipos distintos de responsabilidad: una responsabilidad "estructural", resultante del incumplimiento por la autoridad certificadora de su mandato y una responsabilidad "funcional", resultante de la negligencia de la autoridad certificadora al expedir, suspender o revocar un certificado. En el primer caso, la autoridad certificadora quebranta la confianza pública depositada en ella y sería procedente que la entidad pública autorizada impusiera multas u otras sanciones acordes con la gravedad de la transgresión. En el segundo caso, la autoridad certificadora incumple sus obligaciones profesionales respecto de su propio cliente. Sin embargo, sufriría el perjuicio quien contratase con el cliente, que en la mayoría de los casos no tendría una relación contractual con la autoridad certificadora. En esas circunstancias, se preguntó si correspondería que la parte agraviada tuviese un recurso directo contra la autoridad certificadora o si debía simplemente tener un derecho de recurso contra la persona con quien contrataba únicamente, la cual, a su vez, podría tener un recurso contra la autoridad certificadora. Se dijo que sería difícil establecer un régimen apropiado de responsabilidad en el cual el usuario de un certificado tuviese un recurso directo contra la autoridad certificadora.

53. Se señaló que sería preferible que el Grupo de Trabajo evitase la cuestión de la responsabilidad de las autoridades certificadoras, ya que era delicada y compleja y no sería posible resolverla debidamente en el proyecto de normas uniformes. Se recordó que, en el contexto de la Ley Modelo se había decidido soslayar por completo la cuestión de la responsabilidad de los terceros que eran proveedores de servicios. Se dijo que la cuestión de la responsabilidad guardaba estrecha relación con la de los daños y perjuicios, que tal vez no se prestase fácilmente a la armonización internacional. Se invitó al Grupo de Trabajo a considerar si no sería más procedente excluir las dos cuestiones del alcance del proyecto de normas uniformes y dejarlas libradas al derecho interno aplicable. De

proceder de esa forma, cabría considerar las siguientes posibilidades: dejar librada a las normas nacionales sobre conflicto de leyes la determinación de la ley aplicable a las cuestiones de la responsabilidad y los daños y perjuicios; redactar una norma uniforme concreta sobre conflictos de leyes o determinar directamente qué norma sobre conflictos de leyes habría que aplicar (la del país en que la autoridad certificadora estuviese registrada o autorizada para funcionar, por ejemplo). En favor de esa sugerencia, se señaló que la cuestión de la responsabilidad consistía básicamente en las garantías que proporcionaba la autoridad certificadora y cuya regulación era preferible dejar librada a las partes contratantes o habría que determinar de conformidad con la legislación nacional que fuese aplicable a su relación contractual.

54. En todo caso, contó con gran apoyo la idea de incluir en el proyecto de normas uniformes disposiciones sobre la responsabilidad de las autoridades certificadoras. Se dijo que la cuestión de la responsabilidad era demasiado importante para dejarla totalmente librada a las partes, particularmente en vista del hecho de que tal vez no todos los usuarios de certificados tuviesen una relación contractual directa con la autoridad certificadora. De limitar los derechos del usuario únicamente al de pedir una reparación a la parte con quien contrate por las transgresiones cometidas por la autoridad certificadora, se dejaría sin protección a quienes fuesen víctimas de actos fraudulentos en que se empleasen nombres o entidades ficticias a sabiendas de la autoridad certificadora o por su negligencia. Además, la falta de normas uniformes sobre la responsabilidad de las autoridades certificadoras podría llevar a una situación inconveniente en la cual algunos países fijarían únicamente un grado mínimo de responsabilidad a fin de atraer o promover el establecimiento en su territorio de autoridades certificadoras. La posibilidad de "refugios" en este contexto podría hacer que los contratantes fuesen renuentes a la posibilidad de utilizar firmas digitales, situación que no sería acorde con el objetivo de promover el comercio electrónico. Por difícil que fuese el tema, que comprendía aspectos de responsabilidad contractual y extracontractual, la opinión predominante era que las normas uniformes debían incluir una disposición relativa a la cuestión de la responsabilidad de las autoridades certificadoras.

55. Tras un debate, el Grupo de Trabajo decidió que, en principio, el proyecto de normas uniformes incluyese disposiciones relativas a la responsabilidad de las autoridades certificadoras en el contexto de su participación en transacciones con firmas digitales.

Índole de la responsabilidad

56. Se plantearon cuestiones en cuanto a la índole de la responsabilidad de la autoridad certificadora, particularmente si esa responsabilidad dependería de la negligencia o si sería definida como "responsabilidad estricta" concepto también llamado "responsabilidad objetiva". Se formularon objeciones a la inclusión de disposiciones por las cuales la responsabilidad de la autoridad certificadora fuese estricta. Se señaló que la responsabilidad estricta constituía una excepción al principio general de la responsabilidad extracontractual por el cual una persona era responsable únicamente de su propia negligencia y, como tal, era aceptada en el derecho nacional por razones excepcionales de interés público, como era el caso de algunos regímenes de responsabilidad estricta para quienes llevaran a cabo actividades excesivamente peligrosas. No había una razón apremiante para someter a las autoridades certificadoras a un régimen de responsabilidad estricta. Además, ese régimen tendría la consecuencia negativa de desalentar la incipiente industria de las autoridades certificadoras y, de esa forma limitar las posibilidades de utilización de firmas digitales. Se señaló además que las autoridades certificadoras podrían ofrecer distintos tipos de servicios a sus clientes y al público en general, que iban desde la simple enumeración de los nombres de titulares de claves públicas y sus respectivas claves a servicio más detallados que incluyeran garantías de la autenticidad de las claves públicas y de la identidad de sus titulares. La obligación que contraían las autoridades certificadoras, y los derechos que cobraban, dependían del tipo de servicio que prestaran y, teniendo ello presente, no sería razonable imponer a las autoridades certificadoras el mismo grado de responsabilidad en todas las circunstancias posibles. Se señaló, entonces, que el régimen de responsabilidad aplicable a las autoridades certificadoras debía basarse en la negligencia, según una de las opciones previstas en el párrafo 1) del proyecto de artículo H.

57. Se señaló en respuesta que no sería justo exigir que recayese sobre la parte agraviada la carga de demostrar la negligencia de la autoridad certificadora. Habida cuenta del alto grado de avance tecnológico que cabría esperar de las autoridades certificadoras y del alto grado de confianza que deben generar, en circunstancias normales habría que imputar responsabilidad a las autoridades certificadoras cada vez que la expedición de certificados defectuosos causase un perjuicio. Se señaló que, en algunos ordenamientos jurídicos, ciertas categorías profesionales (los notarios públicos en algunos países de derecho románico, por ejemplo) estaban obligados a contratar un seguro de responsabilidad civil o a participar en un fondo común para indemnizar a las partes que sufriesen perjuicios como resultado de sus actos. Se dijo que se facilitaría el establecimiento de un fondo común de indemnización si las autoridades certificadoras quedasen organizadas en algún tipo de estructura institucional, como un sistema de licencias por ejemplo.

58. Se señaló que se podría superar la divergencia de opiniones manifestada en el Grupo de Trabajo si, en lugar de enunciar una norma positiva en que se indicaran las circunstancias en las cuales las autoridades certificadoras serían responsables, el proyecto de normas uniformes estableciese una presunción juris tantum de responsabilidad. Según esa propuesta, en el caso de identificación errónea de una persona o de atribución errónea de una clave pública a una persona, por ejemplo, la autoridad certificadora sería responsable por el perjuicio sufrido por cualquier parte agraviada a menos que pudiese demostrar que había hecho todo lo posible por evitar el error. La autoridad certificadora podía impugnar la presunción demostrando, por ejemplo, que su conducta se había ajustado a lo establecido en las normas uniformes. Se señaló que un sistema de esa índole, similar a lo previsto en algunas legislaciones nacionales respecto de la responsabilidad por los productos, serviría de protección adicional a los usuarios de servicios sin imponer, en todo caso, una responsabilidad estricta a la autoridad certificadora. El Grupo de Trabajo recibió bien esta propuesta, que fue calificada en general de planteamiento viable para resolver el difícil problema de la responsabilidad de las autoridades certificadoras.

59. El Grupo de Trabajo procedió luego a examinar las circunstancias que podían eximir de responsabilidad a la autoridad certificadora. Se dijo que, en el sistema propuesto, la autoridad certificadora debería quedar exenta de responsabilidad si podía demostrar que había ejercido diligencia razonable al identificar al titular de la clave pública o ejercer sus funciones de autentificación, que los errores eran consecuencia de culpa del propio usuario, como se indicaba en el párrafo 3) del proyecto de artículo H o que el error era imputable a circunstancias ajenas a su voluntad. Se señaló en general que sería aceptable establecer circunstancias eximentes de esa índole.

Las declaraciones sobre prácticas de certificación y la autonomía de las partes

60. Se señaló que, para examinar la cuestión de la responsabilidad era importante tener presentes las expectativas y los intereses tanto del usuario como de la autoridad certificadora. Cabía prever que ésta hiciese una declaración sobre prácticas de certificación en la que pusiese en conocimiento de los usuarios, entre otras cosas, los métodos y procedimientos que aplicaba para identificar al titular de una clave pública. Era de suponer que el usuario cobraría conocimiento razonable de un documento de esa índole. Además, los usuarios deberían quedar obligados a cerciorarse de la validez de un certificado (de que no hubiese sido revocado, por ejemplo) antes de aceptarlo como tal. Por último, cabía prever que los usuarios actuasen razonablemente sobre la base de la información de que dispusieran. En respuesta a preguntas relativas a la forma en que los usuarios podían verificar la validez de un certificado, se dijo que se podía exigir a las autoridades certificadoras que mantuviesen bases de datos de certificados válidos, como ya hacían algunas, que estarían a disposición de las partes interesadas a los efectos de verificar la validez. Respecto de esta propuesta se dijo que, por más que pudiese ser procedente alentar a los usuarios a que actuaran con diligencia en el caso de los certificados, la responsabilidad primaria por la autenticidad y validez de un certificado incumbía a la autoridad certificadora y había que tener mucho cuidado antes de imponer a los usuarios obligaciones que pudiesen hacerles compartir esa responsabilidad. En la mayoría de los casos, normalmente los usuarios no estarían en condiciones de cerciorarse de diversos factores relacionados con la validez del certificado, como los procedimientos de identificación empleados por la autoridad certificadora o si el titular de la clave pública

tenía también la clave privada correspondiente. No sería razonable traspasar al usuario ninguna de esas obligaciones.

61. El Grupo de Trabajo procedió a un debate acerca del papel que cabía a las declaraciones sobre prácticas de certificación y la medida en que podían servir para limitar o definir el alcance de la responsabilidad contraída por las autoridades certificadoras. A los efectos de proteger los intereses de los usuarios, se podía exigir a las autoridades certificadoras que indicasen el grado de esa responsabilidad mediante disposiciones a ese efecto en las declaraciones sobre prácticas de certificación que emitieran. Desde el punto de vista tecnológico, quienes recurrieran a los servicios de una autoridad certificadora podían tener acceso electrónico a las declaraciones sobre prácticas de certificación. Se señaló que la parte que recabara los servicios de una autoridad certificadora tenía que aceptar que, al recurrir a esos servicios, quedaba obligada por lo dispuesto en la declaración sobre la práctica de certificación. Las cláusulas contractuales concertadas entre las partes debían tener preferencia sobre las normas dimanadas de otras fuentes y, en ese contexto, era importante asegurar que se pudiesen hacer cumplir.

62. El Grupo de Trabajo sostuvo en general que, al enunciar un régimen de responsabilidad para las autoridades certificadoras, había que tener debidamente en cuenta la necesidad de preservar la autonomía de las partes. Sin embargo, se expresaron reservas en cuanto a la posibilidad de que una autoridad certificadora se eximiera de responsabilidad por su propia culpa en virtud de cláusulas de exención de la responsabilidad o de descargos de responsabilidad incluidos en la declaración sobre prácticas de certificación o en cualquier otro documento expedido por ella. Se señaló que quien recibiera un mensaje en que se utilizase un certificado para verificar la autenticidad de una firma digital normalmente no tendría una relación jurídica directa con la autoridad certificadora y, por lo tanto, no estaría en condiciones de negociar con ella las cláusulas de responsabilidad de esa índole. Incluso quien emitiera el mensaje, que sí tendría una relación con la autoridad certificadora, no siempre podría negociar esas cláusulas que, en muchos casos, revestirían la forma de condiciones comerciales prefijadas que no admitirían enmienda. En algunos ordenamientos jurídicos, la exención unilateral de la responsabilidad sería contraria al orden público. De instituir límites o exenciones en la responsabilidad, habría que hacerlo de conformidad con la ley o con la aprobación de las autoridades públicas.

Limitación de la responsabilidad

63. El Grupo de Trabajo examinó si la responsabilidad de las autoridades certificadoras debía estar limitada y de qué forma. Se adujo en contra de limitar la responsabilidad de las autoridades certificadoras que solía haber límites en actividades sujetas a alguna forma de monopolio, como los servicios de correos y teléfonos en varios países, pero que en otras actividades donde la competencia era libre no había razón para limitar la responsabilidad.
64. No obstante, se expresaron varias opiniones en favor de limitar de alguna forma la responsabilidad de las autoridades certificadoras. Se señaló lo siguiente: a) la certificación era una actividad reciente, cuyo desarrollo podría resultar frenado por una responsabilidad ilimitada; b) era importante que las autoridades certificadoras pudieran determinar el grado de responsabilidad que estaban dispuestas a asumir y que podría ser una condición previa para poder contratar un seguro que cubriera suficientemente sus actividades y c) podría suceder que, en relación con las firmas digitales, la función de la autoridad certificadora se limitase a expedir un certificado, lo cual en sí mismo podría tener poco o ningún valor cuantificable. Se observó además que cuando se expedía un certificado para establecer una conexión entre una clave pública y una persona determinada, éste podía agregarse a varios mensajes en diversas operaciones, cuya cantidad total sería, la mayoría de las veces, imprevisible por parte de la autoridad certificadora. Se indicó que en el caso de las operaciones realizadas con tarjeta de crédito, había medios para autorizar cada operación individualmente, de forma que la empresa expedidora pudiera, cada vez que se utilizar la tarjeta para realizar una operación por encima de una cantidad determinada, calcular su posible responsabilidad en caso de utilización no autorizada de la tarjeta de crédito. Las autoridades certificadoras no tenían esta posibilidad ya que normalmente desconocían las condiciones de las operaciones realizadas por sus clientes. Por ello, sería difícil fijar un umbral o límite de responsabilidad por remisión al importe de la operación para la cual se hubiera utilizado una firma digital. Dado el número indefinido de las operaciones a las que se podría adjuntar un mismo certificado,

era difícil que las autoridades certificadoras pudieran contratar un seguro de responsabilidad civil a un precio razonable.

65. En cuanto a la forma de limitar la responsabilidad de las autoridades certificadoras, el Grupo de Trabajo examinó varias propuestas. Una de ellas era establecer una cantidad fija, según se proponía en la variante X del párrafo 2) del proyecto de artículo H. Otra consistía en limitar la responsabilidad según un multiplicador de los derechos que paga el suscriptor, un porcentaje del valor de la operación o un porcentaje del perjuicio efectivamente sufrido por el tercero agraviado. Se observó, sin embargo, que los perjuicios derivados de la actuación de la autoridad certificadora no eran fácilmente cuantificables como para servir de criterio objetivo para determinar la cuantía de la responsabilidad. Además, los servicios y honorarios de la autoridad certificadora no solían guardar relación con el valor de las operaciones correspondientes ni con el perjuicio sufrido por las partes. Otras limitaciones, como las previstas en el Convenio de las Naciones Unidas sobre el Transporte Marítimo de Mercancías (Reglas de Hamburgo) o en la Ley Modelo de la CNUDMI sobre transferencias internacionales de créditos, se referían a operaciones con elementos cuantificables (el valor de los bienes, el importe del crédito transferido por ejemplo) que podían no existir en el caso que se examinaba.

66. Otra posible limitación de la responsabilidad consistía en excluirla respecto de determinados daños, como el daño emergente. A este respecto se indicó que el concepto de daño emergente, también llamado indirecto, podía interpretarse de manera diferente en los distintos ordenamientos jurídicos. Por ello se señaló que sería preferible hacer referencia expresa a los prejuicios comprendidos en este concepto y respecto de los cuales la autoridad certificadora estaría exenta de responsabilidad. Aunque hubo opiniones en favor de excluir la responsabilidad por daños indirectos, solución adoptada en la Ley Modelo de la CNUDMI sobre Transferencias Internacionales de Créditos, se advirtió que ella tal vez no fuera apropiada en el contexto de las firmas digitales y las autoridades certificadoras. Se adujo que el daño rara vez resultaba directamente de la expedición de, por ejemplo, un certificado fraudulento, sino más bien de que un tercero aceptase una firma digital dudosa porque había tal certificado. Por esta razón la mayor parte de los daños causados por actos de las autoridades certificadoras podían considerarse "emergentes" o "indirectos". Se propuso también utilizar la "previsibilidad" como criterio para limitar la responsabilidad de las autoridades certificadoras. Se dijo que tal vez habría que examinar más detenidamente como posible referencia el régimen de responsabilidad aplicable al vendedor según la Convención de las Naciones Unidas sobre los contratos de compraventa internacional de mercaderías.

67. En vista de las diversas opciones propuestas, el Grupo de Trabajo pidió a la Secretaría que preparara un informe sucinto sobre los regímenes jurídicos vigentes y las formas de limitar la responsabilidad, sobre todo los previstos en los convenios internacionales aplicables al transporte de mercancías y viajeros, en el que podría hacerse también referencia al régimen de responsabilidad establecido en algunas legislaciones internas para los profesionales que ejercen respecto de la documentación escrita funciones análogas a las de las autoridades certificadoras.

Norma de responsabilidad mínima

68. Se observó que en la etapa en curso de sus deliberaciones, el Grupo de Trabajo estaba estudiando aún si las autoridades certificadoras debían contar con la autorización previa de un organismo público. Se propuso que el Grupo de Trabajo, al retomar el asunto en la continuación del examen del proyecto de artículo B, considerase si el organismo público habilitante debía ser subsidiariamente responsable por los actos de la autoridad certificadora.

69. En cuanto a los párrafos 1) y 2), el Grupo de Trabajo manifestó a título de conclusión provisional que el régimen de responsabilidad aplicable a las autoridades certificadoras debía ser doble, esto es, debía reconocer que el origen de la responsabilidad podía variar según que la autoridad certificadora hubiera sido habilitada por un organismo público o hubiera actuado exclusivamente en virtud de cláusulas contractuales privadas.

70. Como denominador común de ambos regímenes de responsabilidad se propuso que la autoridad certificadora, al expedir un certificado, quedase sujeta a una obligación que podría expresarse en los términos siguientes:

"Al emitir un certificado, la entidad certificadora declara confirmar que:

1) Ha cumplido con todos los requisitos aplicables, a tenor de las presentes Reglas, para la emisión de un certificado, y caso de publicar el certificado o de ponerlo por cualquier otro medio a disposición de alguna persona que razonablemente se fíe de su contenido o de toda firma numérica comprobable mediante la clave pública indicada en el certificado, declara asimismo que el titular indicado en el certificado ha aceptado que así se hiciera;

2) El titular designado en el certificado tiene en su poder la clave privada correspondiente a la clave pública indicada en el certificado;

3) La clave pública y la clave privada del titular funcionan a modo de juego conjunto;

4) Toda la información que figura en el certificado es exacta, salvo que la entidad certificadora haya declarado en el certificado [o en otro lugar al que éste remita] que no confirma la exactitud de algún dato determinado;

y

5) No tiene constancia de que en el certificado se hayan omitido datos sustanciales que, de conocerse, restarían fiabilidad a las declaraciones que anteceden."

Hubo acuerdo en general en que la redacción propuesta era admisible en lo fundamental como norma mínima de la que las partes no podrían substraerse mediante disposiciones contractuales. Así, no debía reconocerse validez a una cláusula limitadora de la responsabilidad de las autoridades certificadoras que fuera contraria a las normas expuestas. Cuando se hiciera valer la responsabilidad de una autoridad certificadora, ésta se presumiría responsable de las consecuencias de la expedición del certificado salvo que demostrara haber cumplido las normas expuestas. No obstante, si una autoridad certificadora quisiera contraer obligaciones mayores que las expuestas, debía tener la posibilidad de hacerlo mediante cláusulas incluidas en una declaración sobre prácticas de certificación o por otros medios.

71. El Grupo de Trabajo decidió que la norma mínima expuesta debía aplicarse a la expedición de certificados relativos a las firmas digitales, definidas en el proyecto de artículo A. Hubo acuerdo general en que el proyecto de normas uniformes no debía tratar de abarcar otros actos o servicios de las autoridades certificadoras, los cuales podrían ser objeto de cláusulas del contrato entre las autoridades certificadoras y sus clientes y de las demás leyes aplicables (por ejemplo, normas jurídicas imperativas sobre la admisibilidad de las cláusulas de exención de la responsabilidad).

Párrafos 3) y 4)

72. El Grupo de Trabajo consideró aceptables en general los elementos de fondo de los párrafos 3) y 4). En relación con el párrafo 3) se estimó en general que, aunque tal vez habría que tener en cuenta el principio de culpa concurrente al preparar la versión revisada del proyecto de artículo H, la norma concreta contenida en el párrafo 3) tal vez ya no fuese necesaria en vista de la decisión del Grupo de Trabajo de que el régimen de responsabilidad aplicable a las autoridades certificadoras no debía basarse exclusivamente en la negligencia. En relación con el párrafo 4) se decidió que la expresión "que ... pueda sufrir el usuario" debía suprimirse para que la norma comprendiera los perjuicios sufridos por cualquier interesado.

73. Tras un debate, el Grupo de Trabajo pidió a la Secretaría que, teniendo presentes las deliberaciones y decisiones que anteceden, preparara un proyecto revisado de artículo H.

74. El Grupo de Trabajo basó sus deliberaciones sobre las cuestiones relativas a las certificaciones recíprocas en el siguiente proyecto de artículo:

"Proyecto de artículo I

1) Los certificados emitidos por entidades certificadoras extranjeras podrán ser utilizados para los fines de una firma numérica en las mismas condiciones que las firmas numéricas sujetas [a la presente Ley] [a las presentes Reglas], de ser reconocidos por una entidad certificadora autorizada, y de garantizar esta entidad, 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 Estado que promulgue la presente Ley o las presentes Reglas designará al órgano o a la autoridad competente para reglamentar la aprobación de certificados extranjeros] queda autorizado para aprobar certificados extranjeros, y para dictar el reglamento por el que se rija dicha aprobación."

75. Antes de dar comienzo a sus deliberaciones sobre las cuestiones relativas a las certificaciones recíprocas, se recordó al Grupo de Trabajo que, conforme al mandato que había recibido de la Comisión, debía asesorar a ésta en cuanto a la conveniencia y viabilidad de preparar unas normas uniformes sobre firmas digitales, autoridades certificadoras y cuestiones conexas (véase el párrafo _). Ese mandato no requería que el Grupo de Trabajo, en este momento, ultimara un proyecto de texto para su examen por la Comisión en su 30º período de sesiones.

76. Se recordaron también las anteriores deliberaciones del Grupo de Trabajo respecto de la función de las autoridades certificadoras en el marco del proyecto de artículo B, en particular las opiniones discrepantes expresadas en cuanto a si las autoridades certificadoras tendrían que obtener aprobación del Estado para cumplir su cometido (véanse los párrafos __). En general, el Grupo de Trabajo estimó que podría adelantar sus deliberaciones al respecto luego de examinar las cuestiones relativas a la responsabilidad de las autoridades certificadoras y a las certificaciones recíprocas. Al propio tiempo, se observó que la decisión respecto de las cuestiones planteadas por el proyecto de artículo B tendría también consecuencias para el régimen de certificación recíproca previsto en el proyecto de normas uniformes.

77. Con el carácter de observación general, se dijo que en los párrafos 1) y 2) se legislaba la relación entre los certificados expedidos por las autoridades certificadoras nacionales y los certificados extranjeros desde ángulos algo distintos. El párrafo 1) autorizaba a una autoridad certificadora nacional a garantizar, en la misma medida que respecto de sus propios certificados, la regularidad de los detalles del certificado extranjero, así como su validez y vigencia. Conforme al párrafo 2), al órgano o a la autoridad competente para autorizar a las autoridades certificadoras en el Estado promulgante se le daba la posibilidad de aprobar los certificados expedidos por las autoridades certificadoras extranjeras conforme a las condiciones que estipulara. Se sugirió que las cuestiones legisladas en el párrafo 1) caían dentro de lo que podría llamarse "certificación recíproca", en tanto que el párrafo 2) se refería a una situación a la que sería más exacto calificar de "reconocimiento recíproco". Se trataba de cuestiones diferentes que bien podrían examinarse por separado.

78. Se opinó que los párrafos 1) y 2) contenían dos opciones distintas respecto de un posible régimen de certificados extranjeros en el marco del proyecto de normas uniformes. Se expresó apoyo en favor de cada una de esas opciones. Con todo, el parecer general fue que ambas opciones no necesariamente habían de considerarse mutuamente excluyentes. Si bien se expresó apoyo en favor de consignar la esencia de los párrafos 1) y 2) en dos artículos separados, se sugirió que sus respectivos ámbitos de aplicación debían ser objeto de un análisis más a fondo. Se señaló que el párrafo 1) contenía esencialmente una disposición respecto de la determinación de

responsabilidad en el caso de que el certificado extranjero resultara irregular, responsabilidad que se derivaba del proyecto de artículo H. El párrafo 2), a su vez, no se refería a las cuestiones de la responsabilidad, sino a los efectos jurídicos que se podrían dimanar directamente de un certificado extranjero, cuando, por ejemplo, el certificado extranjero sirviera de prueba en un litigio ante los tribunales del Estado promulgante. Esos efectos jurídicos no dependían necesariamente de la existencia de la garantía prevista en el párrafo 1) ni se veían afectados por ésta.

79. Habida cuenta de la decisión adoptada por el Grupo de Trabajo de legislar en el proyecto de normas uniformes no sólo sobre las autoridades certificadoras autorizadas por entidades públicas, sino también por "autoridades certificadoras impulsadas por el mercado" (véanse los párrafos __), se estima en general que el proyecto de artículo I debía referirse al reconocimiento de los certificados extranjeros expedidos por ambos tipos de autoridades certificadoras.

80. Se sugirió que el Grupo de Trabajo considerara también la cuestión de las condiciones con arreglo a las cuales se podrían reconocer los certificados extranjeros. Esas condiciones podrían asumir la forma de requisitos establecidos por el Estado o estipularse en arreglos entre las autoridades certificadoras nacionales y extranjeras. Se explicaron las formas en que sería concebible estructurar esos arreglos entre autoridades certificadoras. Se recordó que la infraestructura de clave pública a menudo se sustentaba en diversos niveles jerárquicos de autoridad. Dentro de esas estructuras jerárquicas, era probable que hubiera dos fases de certificación recíproca. En una fase inicial era de esperar que la certificación recíproca quedara reservada exclusivamente a las "autoridades primarias" (esto es, las autoridades que certificaban la tecnología y las prácticas en relación con el uso de pares de claves y que registraban a las autoridades certificadoras subordinadas). En una etapa ulterior, a medida que se desarrollara este sector, las autoridades certificadoras subordinadas de nivel inferior a la autoridad "primaria" podrían también intervenir directamente en la expedición de la garantía de regularidad de los certificados expedidos por autoridades certificadoras extranjeras. Al formular normas respecto de las cuestiones de las cuestiones de certificación recíproca, sin embargo, el Grupo de Trabajo debería tener en cuenta la posibilidad de que, en particular respecto de las firmas digitales con mínimos grados de seguridad, acaso habría que dar efecto a certificados extranjeros en ausencia de un acuerdo específico entre las autoridades certificadoras. Por lo tanto, se sugirió que en esas circunstancias se podría requerir una norma supletoria para reconocer las firmas digitales extranjeras.

81. Se dijo que la inclusión de disposiciones relativas a las cuestiones del reconocimiento recíproco podría constituir un importante paso adelante para realzar la fiabilidad de los certificados. Sin embargo, el Grupo de Trabajo tendría que examinar cuidadosamente los métodos y los procedimientos de certificación o reconocimiento recíproco. Se señaló que, al evaluar la fiabilidad de un certificado extranjero, el receptor de un mensaje con firma digital acompañado por ese certificado debería considerar diversas cuestiones, como las relativas a saber si la autoridad certificadora que había expedido el certificado estaba autorizada a actuar en el extranjero; si la firma digital de la autoridad certificadora era auténtica; si había recursos legales contra la autoridad certificadora; si la firma digital había sido reconocida para surtir efectos jurídicos; y si la firma digital podría oponerse a su autor.

82. Desde esa perspectiva, se dijo también que en la certificación recíproca se podían básicamente reconocer cuatro niveles distintos de fiabilidad. En el nivel máximo, la autoridad certificadora nacional, a petición de la parte que invocara un certificado extranjero, garantizaría el contenido de ese certificado de acuerdo con su conocimiento declarado de los procedimientos que hubieran llevado a la expedición del certificado, asumiendo así plena responsabilidad por los errores u otras irregularidades del certificado. En el nivel inmediatamente inferior, la autoridad certificadora nacional garantizaría el contenido de un certificado extranjero sobre la base de la información que hubiera recibido en cuanto a la fiabilidad de la autoridad certificadora extranjera. En un grado inmediatamente inferior de fiabilidad, la autoridad certificadora nacional limitaría su responsabilidad a garantizar la fiabilidad de la autoridad certificadora extranjera, sin asumir responsabilidad alguna por el contenido del certificado extranjero. En el último nivel, la autoridad certificadora nacional sólo garantizaría la identidad de la autoridad certificadora extranjera, basada en la verificación de su clave pública y de su firma digital. Se sugirió que el Grupo de Trabajo

cuando llegara el momento de formular disposiciones sobre certificación o reconocimiento recíproco de certificados extranjeros, prestara atención al nivel de fiabilidad que interesaba al receptor del mensaje.

83. A ese respecto, se comparó la posición de la autoridad certificadora que garantizaba la exactitud y validez de un certificado extranjero con la de una institución financiera que garantizaba una carta de crédito otorgada por un banco extranjero. La admisibilidad de la carta de crédito por su beneficiario dependía de factores como la fiabilidad del banco extranjero que otorgara la carta de crédito y de la ejecutoriedad de ésta en el país del beneficiario. A veces el beneficiario podía insistir en obtener una contra-garantía de un banco local. El beneficiario de la carta de crédito determinaría el nivel de seguridad adecuado para una operación de conformidad con el nivel de riesgo que estuviera dispuesto a asumir. Análogamente, la parte en una operación en la que se utilizara un certificado extranjero bien podría considerar que era suficiente, por ejemplo, saber que el certificado había sido expedido por una autoridad certificadora extranjera fidedigna sin considerar necesario obtener la garantía de una autoridad certificadora de su país. Se expresó preocupación por que se interpretara que el proyecto de artículo I desaconsejaba o prohibía la utilización de certificados que no hubieran sido garantizados por una autoridad certificadora nacional, aun en el caso de operaciones en que las partes se hubieran sentido razonablemente seguras con un menor grado de seguridad o certeza jurídica. Era importante asegurar que el proyecto de artículo I se ocupara de las cuestiones de la certificación y el reconocimiento recíprocos de manera flexible.

84. En relación con la comparación antes expuesta entre la función de las autoridades certificadoras y la de los bancos que intervenían en los créditos documentados, se consideró en general que, al elaborar normas uniformes para el reconocimiento de certificados, debía tenerse en cuenta que las firmas digitales podían servir no solamente para transferir derechos sino también obligaciones, como por ejemplo cuando una firma digital se añadía a la notificación de una cesión de deuda. Por lo tanto, el riesgo de confiar en una firma digital podía atribuirse al receptor o al emisor de la firma digital, según la operación.

85. En cuanto al posible ámbito de la certificación y reconocimiento recíprocos, se dijo que, en cierta medida, las funciones desempeñadas por las autoridades certificadoras eran similares a las realizadas por los notarios en algunos ordenamientos jurídicos. Así, en varios de ellos algunas operaciones exigían que un notario u otro funcionario con funciones similares certificara determinados hechos (por ejemplo, la identidad de una de las partes) o elementos del acto (por ejemplo, la firma de las partes o la autenticidad de un documento). Sin embargo, las operaciones en que se exigía la certificación notarial variaban de un ordenamiento jurídico a otro, y no sería factible tratar de armonizar las soluciones nacionales relativas a los requisitos formales de las operaciones subyacentes.

86. Se opinó que los certificados extranjeros se reconocerían normalmente en régimen de reciprocidad y que, por ende, la facultad correspondiente se derivaría de acuerdos internacionales bilaterales o multilaterales. Se expresaron reservas a que en el proyecto de normas uniformes se hiciera referencia a la "reciprocidad", dados los diversos significados que ésta tenía en distintos ordenamientos jurídicos. Por otra parte, la propuesta de añadir una referencia a los acuerdos internacionales bilaterales o multilaterales provocó reacciones diversas. En apoyo de la propuesta se dijo que la referencia a los acuerdos internacionales bilaterales o multilaterales aclararía que el proyecto de normas uniformes no afectaba a las obligaciones internacionales que los Estados hubieran contraído, por ejemplo, en virtud de acuerdos regionales sobre integración o cooperación económica. No obstante, se dijo también que era innecesario referirse expresamente a esos acuerdos, pues el párrafo 1) en absoluto impedía que el Estado promulgante hiciera certificaciones recíprocas o reconociera certificados extranjeros en virtud de esos acuerdos. Se propuso además que, en lugar de referirse a los acuerdos internacionales en el proyecto de artículo I, el Grupo de Trabajo considerara la posibilidad de establecer normas sustantivas sobre el reconocimiento de los certificados extranjeros. Debía evitarse que en el artículo I se hiciera referencia a los acuerdos internacionales bilaterales o multilaterales, a no ser que: a) el Grupo de Trabajo llegara a la conclusión de que no era viable establecer unas normas de reconocimiento armonizadas; o b) la referencia fuera a acuerdos que ofrecieran un nivel de reconocimiento de los certificados extranjeros más favorable que el previsto en el proyecto de normas uniformes.

87. Se observó que los párrafos 1) y 2) ofrecían dos opciones diferentes al Estado promulgante, según que la intervención de la autoridad certificadora necesitara o no la autorización previa del Estado. No obstante, se expresó preocupación por que, considerado juntamente con el proyecto de artículo B que requería esa autorización previa respecto de las autoridades certificadoras establecidas en el Estado promulgante, pudiera interpretarse que el párrafo 1) permitía el reconocimiento de certificados expedidos por autoridades certificadoras extranjeras cuyo funcionamiento no hubiera sido autorizado por las normas internas, al mismo tiempo que negaba eficacia jurídica a los certificados expedidos por autoridades certificadoras nacionales que no hubieran recibido la autorización requerida en el Estado promulgante. En ese sentido se preguntó si el propósito del proyecto de artículo I era hacer posible que una autoridad certificadora autorizada por el Estado diera validez jurídica a los certificados expedidos por otras autoridades certificadoras nacionales o extranjeras no autorizadas. Si ésa era su finalidad, el proyecto de artículo I tal vez tendría que modificarse con arreglo a la decisión que el Grupo de Trabajo tomara en relación con el proyecto de artículo B.

88. Respecto de la garantía prevista en el párrafo 1), se señaló que en algunos ordenamientos jurídicos bien podría ser difícil regular la cuestión mediante una disposición general sin añadir más detalles, puesto que las garantías otorgadas por las autoridades certificadoras podían variar mucho de un país a otro. Sería difícil que las autoridades certificadoras internas aceptaran responsabilidad por certificados expedidos en el extranjero sin que hubiera uniformidad respecto de las garantías ofrecidas por las autoridades certificadoras.

89. Tras examinar las diversas opiniones expresadas en el Grupo de Trabajo, se consideró conveniente, en general, que el proyecto de normas uniformes se ocupase de las cuestiones de la certificación recíproca. Aunque los principios expuestos en el proyecto de artículo I se consideraron admisibles en general, sería prematuro que el Grupo de Trabajo tratara de establecer normas detalladas sobre esas cuestiones en una fase tan precoz de sus deliberaciones. Se pidió a la Secretaría que preparara un proyecto de artículo I revisado teniendo en cuenta las opiniones antes expresadas y la necesidad de que fuera aplicable a las autoridades certificadoras, autorizadas o no por el Estado. Se pidió a la Secretaría que distinguiera entre las condiciones y efectos del reconocimiento de una firma digital y un certificado, por un lado, y el reconocimiento de una autoridad certificadora por otro, y que hiciera las propuestas oportunas, posiblemente en forma de variantes, para legislar respecto de esas dos cuestiones diferentes.

1. Definiciones (continuación)

B. Entidades certificadoras autorizadas

90. Habiendo completado su examen preliminar de las cuestiones relativas a la responsabilidad y la certificación recíproca de conformidad con los proyectos de artículos H e I, el Grupo de Trabajo reanudó sus deliberaciones acerca de las cuestiones planteadas por la definición de la "autoridad de certificadora" con arreglo al proyecto B (véanse los párrafos ...). Se recordó que, a fin de dar cabida tanto a la situación en que la autoridad certificadora actúa con carácter exclusivamente privado y la situación en que la autoridad certificadora debe estar licenciada o autorizada de alguna manera por las autoridades públicas antes de que se les permita operar, el Grupo de Trabajo había decidido adoptar un "criterio dual" (véase el párrafo ...), que sugería la necesidad de una definición amplia de "autoridad certificadora" para abarcar ambos tipos de situaciones. A ese respecto se sugirió que el Grupo de Trabajo podría considerar la posibilidad de reemplazar la idea de "autoridad certificadora" por la de "entidad certificadora" para evitar la posible consecuencia de que las funciones de certificación fueran realizadas necesariamente por autoridades públicas. Si bien hubo apoyo en favor de esa sugerencia, se recordó que la idea de "autoridad certificadora" ya se usaba ampliamente, tanto por entidades públicas como privadas. Se instó al Grupo de Trabajo a que obrara con cautela al adoptar terminología que pudiera contradecir la práctica de certificación que estaba surgiendo.

91. Se indicó que las disposiciones que actualmente incorporaba el proyecto de artículo B se referían a diversos aspectos de las autoridades certificadoras. Si bien algunos párrafos, como el párrafo 3, tenían solo el carácter de definición, otras disposiciones, como el párrafo 4, eran más operacionales y descriptivos de las funciones que realizaban las autoridades certificadoras. De esa manera se sugirió que podría ser necesario dividir el proyecto

de artículo B en diferentes artículos, que se ocuparan de la definición y de las funciones de las autoridades certificadoras, respectivamente. Se consideró ampliamente que, al reestructurar el proyecto de artículo B, podría ser apropiado referirse a funciones que pudieran realizar las autoridades certificadoras además del estampado cronológico, como la emisión de pares de claves, la mantención de directorios, la conservación de registros y otros servicios, que se describían como "secundarios" respecto de las funciones principales de las autoridades certificadoras relativas a las firmas digitales. Sin embargo, hubo acuerdo en general en que el efecto de referirse a esos servicios secundarios no debía ampliar el ámbito de las normas uniformes, como se definían en referencia con las "firmas digitales" en el proyecto de artículo A.

92. Como posible distinción entre los regímenes jurídicos aplicables a las autoridades certificadoras licenciadas o autorizadas de otra manera por el Estado promulgante y a las autoridades certificadoras no autorizadas, se sugirió que el proyecto de norma uniformes expresara los efectos jurídicos concretos que podrían esperarse de la emisión de certificados por la autoridad certificadora autorizada. En respuesta a una pregunta que se planteó en cuanto a los efectos jurídicos que podrían derivar de la emisión de certificados por las autoridades certificadoras no autorizadas, se sugirió que podría tratarse el asunto con una referencia simple al artículo 7 de la Ley Modelo. Si bien hubo apoyo en favor de esa propuesta, se dijo que tal vez sería apropiado que las normas uniformes abundaran en los efectos jurídicos de los certificados que emanaran de las autoridades certificadoras exclusivamente privadas. Otra sugerencia fue que podría basarse una distinción entre autoridades autorizadas y no autorizadas en las diferentes funciones que podrían realizar los dos tipos de autoridades. En general se consideró que esas cuestiones merecerían mayor consideración del Grupo de Trabajo en un período de sesiones futuro.

93. En el contexto del examen del párrafo 3 se planteó la cuestión de si la referencia a las "claves de personas naturales y jurídicas" daba suficiente orientación en las situaciones en que las claves criptográficas se emitieran directamente a los mecanismos electrónicos, o los usaran esos mecanismos, en ausencia de intervención humana directa. El Grupo de Trabajo recordó que se había examinado la cuestión en el contexto de la preparación de la Ley Modelo, y en general se concordó en que tal vez sería necesario examinarlo mayormente en una etapa posterior con respecto a la cuestión de las firmas digitales.

94. En cuanto a la posible estructura de un proyecto revisado de artículo B, se señaló a la atención del Grupo de Trabajo el método seguido respecto de la Ley Modelo, que se basaba en una combinación de disposiciones estatutarias con una guía para promulgar esas disposiciones. La adopción de ese método haría posible incluir explicaciones e ilustraciones más pormenorizadas en cuanto al contenido de las disposiciones estatutarias, con lo cual se facilitaría su consideración futura por los legisladores. Se sugirió que podría seguirse el mismo criterio respecto de las normas uniformes. Particularmente al ocuparse de las diversas funciones realizadas por las autoridades certificadoras sería apropiado incluir material explicativo en el contexto de una guía de la promulgación. El Grupo de Trabajo, aunque postergó su decisión en cuanto a la forma definitiva de las normas uniformes, encontró en general aceptable esa sugerencia.

95. Después del debate el Grupo de Trabajo decidió que se reubicaran las disposiciones que actualmente se hallaban en el proyecto de artículo B en dos artículos distintos que se ocuparían de una definición ampliada de "autoridad certificadora" y de las funciones de las autoridades certificadoras, respectivamente. Se decidió que la definición general de "autoridad certificadora" se basara en el texto del párrafo 3 del proyecto de artículo B. Se convinó en que la referencia a las "personas naturales o jurídicas" se complementara con una referencia a los "mecanismos electrónicos", que debía colocarse entre corchetes, en tanto lo examinaba el Grupo de Trabajo. Además de una definición general de "autoridad certificadora" el artículo revisado de definición debía contener una definición de las autoridades certificadoras "licenciadas", "autorizadas" o "acreditadas", que podría basarse en el párrafo 1 del proyecto de artículo B. En cuanto a los elementos que figuraban en los párrafos 2 y 5 del proyecto de artículo, debían reflejarse en la parte de la guía de promulgación del proyecto de normas uniformes correspondiente a la definición de autoridades certificadoras "autorizadas".

96. En general hubo acuerdo en que el artículo separado, que debía ocuparse de las diversas funciones de las autoridades certificadoras, podía basarse en el párrafo 4 del proyecto de artículo B. Se convino además en que el alcance de un artículo futuro relativo a las funciones de las autoridades certificadoras podría ampliarse de manera de abarcar otras funciones. En tal sentido, podrían extraerse elementos de la legislación, las directrices y los contratos modelo actualmente en uso o en examen con respecto a las autoridades certificadoras. Como cuestión de redacción en general se consideró que podría ser necesario enmendar la referencia a las "comunicaciones basadas en las firmas digitales" en el párrafo 4 para evitar la sugerencia de consecuencias particulares en cuanto a la aceptabilidad de los métodos de seguridad usados por las autoridades certificadoras.

97. Se pidió a la Secretaría que preparara un proyecto revisado artículo B, tomando en cuenta las deliberaciones y decisiones anteriores.

c) Certificados

98. El Grupo de Trabajo examinó la definición de certificados sobre la base del proyecto de disposición siguiente:

"Proyecto de artículo C

Todo certificado emitido por una entidad certificadora autorizada, en forma de mensaje de datos o en alguna otra forma, deberá indicar por lo menos:

a) El nombre del usuario [y su dirección o establecimiento];

b) [La fecha de nacimiento] [Datos personales suficientes] del usuario, caso de ser éste una persona natural;

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

d) El nombre, la dirección o el establecimiento de la entidad certificadora;

e) La clave criptográfica pública del usuario;

f) Toda otra información necesaria para dar a conocer la manera por la cual el destinatario de la firma numérica dad de conformidad con el certificado podrá verificar la clave criptográfica pública del usuario;

g) El número de serie del certificado; y

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

99. Al comenzar el debate, se recordó al Grupo de Trabajo que, en el curso de sus deliberaciones sobre la definición de autoridad certificadora, había decidido, como hipótesis de trabajo, adoptar un planteamiento flexible que comprendiera tanto los certificados expedidos por autoridades certificadoras autorizadas por el gobierno como los expedidos por autoridades certificadoras que funcionaran fuera de una infraestructura de clave pública organizada por el gobierno y que, por el momento, no había de excluir ninguna de esas posibilidades. Con arreglo a esa hipótesis de trabajo, había que suprimir la palabra "autorizada" que figuraba en el encabezamiento del proyecto de artículo C.

100. Se hicieron observaciones generales en cuanto a la terminología del proyecto de artículo C, en particular el empleo de la palabra "usuario" en relación con el titular de la clave privada de un par de claves criptográficas. Se señaló que esa palabra se prestaba a confusión con el receptor del mensaje, al que cabía considerar "usuario" del certificado o de la clave pública utilizada para verificar la firma digital. Se sugirieron varias variantes, entre ellas las expresiones "propietario del par de claves", "titular del certificado" o "titular de la clave privada". Se decidió que la Secretaría revisara la terminología empleada en el proyecto de artículo C y en las demás disposiciones del proyecto de normas uniformes y presentase propuestas para evitar posibles ambigüedades.

101. Hubo acuerdo generalizado en que era necesario definir en el proyecto de artículo C el término "certificado" antes de mencionar cuál debía ser su contenido. Se propuso la siguiente definición: "Certificado es un mensaje electrónico enviado con la intención de certificar, en el que se identifica a la autoridad certificadora, se incluye la clave pública del usuario, se identifica al usuario y se pone la firma digital de la autoridad certificadora". Según otra propuesta, la definición debía basarse en los elementos de un certificado que se indicaban en una nota de la Secretaría, en la que se hacía referencia al certificado como registro electrónico que indicaba una clave pública junto con el nombre del suscriptor del certificado como "sujeto" del certificado y confirmaba que el posible firmante identificado en el certificado poseía la clave privada correspondiente (A/CN.9/WG.IV/WP.71, párr. 36). Se señaló

que una definición similar a la de esta última propuesta sería generalmente aceptable. Sin embargo, en ella habría que indicar que la autoridad certificadora debía poner su firma digital en el certificado a fin de asegurar la autenticidad de éste tanto respecto de su contenido como de su fuente.

102. Se preguntó si las palabras "por lo menos" que figuraban en el encabezamiento del proyecto de artículo C en relación con el contenido de un certificado significaban que el que no contuviera todos los datos enumerados en el proyecto de artículo no sería considerado certificado en el sentido del proyecto de normas uniformes. Se respondió que, en su texto actual, el artículo C mencionaba diversos elementos que necesariamente debía contener un certificado para ser considerado tal con arreglo al proyecto de normas uniformes. En aras de la claridad, se sugirió que la definición de "certificado" fuese una disposición independiente y la información que había que indicar en el certificado constase en una disposición separada.

103. El Grupo de Trabajo debatió cuánta información debía contener el certificado. Como observación general, se dijo que los elementos obligatorios debían mantenerse en un mínimo e incluir esencialmente la información necesaria para que el usuario del certificado pudiera verificar la firma digital empleada en un mensaje electrónico. Se señaló que la inclusión de elementos innecesarios en la información que había de contener un certificado podía surtir el efecto no deseado de excluir del ámbito del proyecto de normas uniformes diversos certificados que, de lo contrario, serían suficientes a los fines para los que habían sido expedidos. Se señaló que era importante tener presente la diferencia que había entre la información contenida en un certificado y las medidas que debía adoptar la autoridad certificadora para cerciorarse de que esa información fuese exacta. Cuanta más información contuviese un certificado, mayor era el riesgo de que la autoridad certificadora incurriera en responsabilidad. Se sugirió en consecuencia que no se fijaran en el proyecto de normas uniformes requisitos mínimos en cuanto al contenido de un certificado.

104. Se sugirió otra posibilidad sobre la base del examen de la cuestión de la responsabilidad de las autoridades certificadoras, en el contexto del cual se había entendido que, en caso de error en la identificación de una persona o en la atribución de una clave pública a una persona, la autoridad certificadora sería responsable por los perjuicios sufridos por la parte agraviada a menos que pudiera demostrar que había hecho lo que estaba a su alcance para evitar el error (véase el párrafo _____). La opinión generalizada fue que de poco serviría al objetivo de proteger al usuario final exigir que la autoridad certificadora aplicase procedimientos adecuados para verificar la exactitud de la información o identificar debidamente a los titulares de claves privadas y, al mismo tiempo, permitir que esa autoridad soslayara su responsabilidad expidiendo certificados que no contuvieran el mínimo de información necesario.

105. Se indicó que, si el certificado debía cumplir un cierto número de requisitos obligatorios en cuanto a su contenido, la autoridad certificadora no estaría en condiciones de soslayar su responsabilidad en la forma que se había dicho. En ese contexto, se recordó que en el debate de la cuestión de la responsabilidad de las autoridades certificadoras, se había propuesto que éstas, al expedir un certificado, quedasen obligadas a declarar que habían confirmado una cantidad de elementos (véase el párrafo ___). Esta sugerencia suscitó amplio apoyo. Tras un debate, el Grupo de Trabajo decidió que no era posible examinar minuciosamente la cuestión en el período de sesiones en curso y que habría que reanudar las deliberaciones a la brevedad posible sobre la base de las variantes de texto que preparase la Secretaría con arreglo al debate que antecede.

106. En cuanto a los datos que habría que exigir para identificar al titular de la clave privada, se sugirió refundir los apartados a), b) y c) en una disposición. En ese contexto, se señaló que en muchos países la información relativa a la fecha de nacimiento de una persona, por ejemplo, estaba protegida como dato personal y podía haber normas concretas que rigieran su divulgación por medios electrónicos. Se dijo por lo tanto que no había que exigir que un certificado contuviera información personal de esa índole. Se respondió que, en algunas circunstancias, quien pidiera un certificado podía aceptar la divulgación de algunos tipos de datos personales o fuentes de información adicional o incluso tener interés en ello. El proyecto de normas uniformes no debía obstar a esa posibilidad en los casos en que la divulgación consensual de datos personales no fuese incompatible con las normas aplicables sobre protección

de datos o con la política pública del Estado en que se hiciera la solicitud o se expidiera el certificado. La opinión generalizada fue que las cuestiones relativas a la protección de datos no quedaban comprendidas en el ámbito del proyecto de normas uniformes y que en el proyecto de artículo C había que exigir únicamente que se proporcionara identificación suficiente en forma compatible con las normas aplicables en materia de protección de los datos.

107. Se sugirió hacer referencia en el apartado a) al "nombre o identificación" del usuario de manera de dejar comprendidas las situaciones en que el usuario no estaría identificado por su nombre sino por otro medio, como un número de cuenta, como ocurriría en el caso de certificados relativos a transacciones con tarjetas de crédito. Se expresaron objeciones a esa sugerencia porque podría alentar la utilización de mensajes y certificados anónimos, situación que no sería compatible con el objetivo de promover una mayor certeza jurídica en el comercio electrónico. Se instó al Grupo de Trabajo a que mantuviese la referencia al nombre del titular de la clave privada como elemento esencial de un certificado.

108. A los efectos de la debida identificación del titular de la clave privada, se sugirió que el proyecto de artículo C hiciera referencia a elementos adicionales de identificación como la dirección, en el caso de las personas naturales, o el número de registro en el caso de las entidades jurídicas, ya que el nombre de una persona o empresa tal vez no bastara por sí solo para identificarla.

109. Se señaló que, en algunos casos, la utilización de una firma digital podría estar limitada a ciertos tipos de transacciones como resultado, por ejemplo, de limitaciones a la autoridad del firmante para obligar a la compañía en cuyo nombre se hacía la transacción. Por ello, se dijo que el certificado debía incluir información acerca de esas restricciones o limitaciones o una referencia a su fuente. Se respondió que la cuestión de los límites dentro de los cuales podía hacerse fe en una firma digital planteaba diversos y difíciles problemas jurídicos, que no eran propios del comercio electrónico únicamente. En una transacción ordinaria, no electrónica, tal vez no fuese obligatorio que la firma manuscrita fuese acompañada de una declaración de las limitaciones a que estuviesen sometidas las atribuciones de su autor. Se instó al Grupo de Trabajo a que no instituyera en relación con las firmas digitales requisitos más estrictos que los aplicables a las firmas manuscritas.

110. Se recordó al Grupo de Trabajo su debate anterior acerca de las cuestiones relativas al consumidor y la responsabilidad de una autoridad certificadora, así como de las posibles limitaciones y exclusiones de la responsabilidad de conformidad con la legislación nacional o con la declaración de las prácticas de certificación de la autoridad certificadora. Se señaló que había que exigir que la autoridad certificadora expusiera esas limitaciones o hiciese referencia a un documento que el usuario pudiese consultar y en el que constasen ellas. Se señaló también que el proyecto de normas uniformes debía consignar las consecuencias que entrañaría la falta de esa indicación en el certificado. Se dijo igualmente que, en los casos en que el período de validez de un certificado fuese limitado, habría que mencionar en el certificado la fecha de expiración o el período de vigencia. Se sostuvo que era importante para proteger a los usuarios del certificado proporcionarles información en cuanto a la validez de ellos, así como que no corrieran el riesgo de que se expidiera un certificado sin esa indicación. Por lo tanto, el proyecto de normas uniformes debía contener una disposición supletoria en que se especificara el período de validez que regiría de no hacerse tal indicación. Se señaló, sin embargo, que podría interpretarse la existencia de una norma de esa índole en el sentido de que la autoridad certificadora tenía la opción de no mencionar el período de validez de un certificado.

111. Se formularon preguntas en cuanto al tipo de información que las autoridades certificadoras podían proporcionar a los usuarios de sus servicios en alguna forma a la que tuvieran acceso con la tecnología existente. Se respondió que la tecnología existente permitía a las autoridades certificadoras adjuntar de alguna forma información adicional a los certificados que expedían, como su propia declaración de prácticas de certificación o la información que, a título facultativo, facilitasen para esos efectos los titulares de claves privadas. Sin embargo, muchos sistemas informáticos que actualmente utilizaban los clientes de autoridades certificadoras todavía no podían tener acceso a toda esa información. Además de esas dificultades técnicas, era importante tener presente que parte de la información que se adjuntara a los certificados podía dimanar de los titulares de claves privadas y ser divulgada

por solicitud de ellos. Era importante distinguir en esos casos entre los elementos del certificado que la autoridad verificaba (la identidad del titular de la clave privada, por ejemplo) y otros elementos proporcionados por sus clientes y que ella no hubiese verificado (las limitaciones en cuanto a la utilización de claves privadas en una empresa, por ejemplo). No cabía imputar a las autoridades certificadoras la responsabilidad por la exactitud de esa información no verificada.

112. Hubo varias intervenciones en el sentido de que, sin perjuicio de la información de otra índole que la autoridad certificadora proporcionase a sus clientes, ésta tenía que garantizar que había verificado que la información que debía obligatoriamente constar en un certificado era exacta y cabal.

113. Tras examinar las opiniones expresadas respecto del proyecto de artículo 5, el Grupo de Trabajo decidió que había que agregarle una definición de certificado. El contenido obligatorio del certificado formaría parte de una disposición separada, que se referiría también a las consecuencias de la falta de elementos obligatorios en un certificado. Esa disposición tendría en cuenta los elementos a que se hacía referencia en los apartados a), b) y c), refundidos en una disposición revisada única, e incluiría también la información mencionada en los apartados d), e) y h) del proyecto de artículo C. Se consideró que la autoridad certificadora no estaba en condiciones de certificar la información a que se hacía referencia en el apartado f) y, en consecuencia, se decidió suprimirlo. Hubo acuerdo en dejar el apartado g) entre corchetes y examinarlo posteriormente como opción posible, ya que tal vez no todos los certificados estuviesen identificados con un número de serie. En el proyecto revisado de artículo C había que hacer referencia expresa a la aplicabilidad a la información contenida en un certificado de la legislación interna en materia de protección de los datos. Se pidió a la Secretaría que preparase una versión revisada del artículo C en que constaran, como posibles variantes, las diversas opiniones expresadas, así como las conclusiones a que había llegado el Grupo de Trabajo.

4. Firmas de personas jurídicas y naturales

114. El Grupo de Trabajo celebró un debate sobre el siguiente proyecto de disposición:

> "Proyecto de artículo D
>
> 1) Tanto las personas naturales como las jurídicas podrán obtener la certificación de una clave pública criptográfica utilizada exclusivamente con fines de identificación.
>
> 2) Toda persona jurídica podrá identificar un mensaje de datos consignando en ese mensaje la clave criptográfica pública certificada para esa persona jurídica. Sólo se considerará que esa persona jurídica [es la iniciadora] [ha dado su aprobación al envío] de ese mensaje, cuando el mensaje haya sido además firmado numéricamente por una persona natural autorizada para actuar en nombre de dicha persona jurídica."

115. Según una opinión muy difundida, se debería suprimir el artículo D. Se señaló que era improcedente distinguir entre personas jurídicas y naturales a los efectos de las firmas digitales, ya que no se hacía esa distinción en la Ley Modelo, en la que el término "persona" abarcaba tanto a las personas naturales como a las jurídicas. Además, se manifestó que el párrafo 2) podía constituir una injerencia indebida en otros conjuntos normativos, como, por ejemplo, en la legislación sobre representación y en las disposiciones del derecho societario relativas a la representación de las sociedades por personas naturales. Además, se manifestó que la norma que figuraba en el párrafo 2) parecía imponer a los usuarios de firmas digitales una carga que iba más allá de los requisitos existentes respecto de las firmas manuscritas.

116. No obstante, se manifestó la opinión de que era útil el proyecto de artículo D, y, en concreto, su párrafo 2). Particularmente, dado que en ninguna otra norma jurídica aplicable se indicaba la forma en que podía estamparse una firma vinculante en nombre de una persona jurídica, el hecho de contar con una norma subsidiaria como la del párrafo 2) podía servir para indicar en qué circunstancias podía considerarse que una firma digital que aparentemente era la de una persona jurídica correspondía a ésta. Se expresaron opiniones favorables a mantener el párrafo 2),

habida cuenta de que se había modificado su texto para incluir claramente que, aunque contenía una referencia a "una persona natural autorizada a actuar en nombre" de una persona jurídica, su objetivo no era reemplazar a la legislación nacional en materia de representación. Así pues, la cuestión de determinar si una persona natural estaba facultada de hecho y de derecho para actuar en nombre de una persona jurídica se resolvería en el marco de normas jurídicas pertinentes distintas de las normas uniformes.

117. Tras celebrar el correspondiente debate, el Grupo de Trabajo decidió que el proyecto de artículo D debería colocarse entre corchetes y ser examinado más detenidamente en un período de sesiones posterior.

5. Atribución de los mensajes firmados digitalmente

118. El Grupo de Trabajo examinó la cuestión sobre la base del proyecto de disposición siguiente:

"Proyecto de artículo E

1) El iniciador de un mensaje de datos, que lleve consignada su firma numérica, quedará obligado por el contenido del mensaje al igual que si éste figurara en un formulario firmado [a mano], de conformidad con la ley aplicable al contenido del mensaje.

2) El destinatario de un mensaje de datos que lleve consignada una firma numérica tendrá derecho a considerar que ese mensaje proviene del iniciador, y a actuar como si así fuera cuando:

a) para determinar que el mensaje de datos provenía del iniciador, el destinatario haya aplicado correctamente la clave pública del iniciador al mensaje de datos recibido y ello reveló: que el mensaje de datos recibido fue cifrado con la clave criptográfica privada del iniciador, y que el mensaje inicial no ha sido alterado después de haber sido cifrado con la clave criptográfica pública del iniciador;

o

b) el mensaje de datos recibido por el destinatario resultó de los actos de una persona que tuvo acceso a la clave criptográfica privada del iniciador por razón de sus relaciones con el iniciador o con algún agente del iniciador.

3) El párrafo 2) no será aplicable:

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

o

b) en el supuesto considerado en el inciso b) del párrafo 2), cuando el destinatario supo o hubiera sabido, de haber tomado precauciones razonables o de haber utilizado cualquier procedimiento convenido, que el mensaje de datos no provenía del iniciador."

119. Se dijo que había que suprimir el proyecto de artículo E. En apoyo de esa opinión se manifestó que el proyecto de artículo sólo establecía una versión específica del artículo 13 de la Ley Modelo y que quizás crearía incertidumbre en cuanto a la posible relación entre las dos disposiciones. Según otra opinión, había que suprimir el proyecto de artículo porque podría interpretarse erróneamente como una injerencia con la ley aplicable a la transacción comercial para la que se había usado la firma digital. Por ejemplo, se podría interpretar que las

disposiciones del párrafo 1) según las cuales el originador del mensaje de datos "queda obligado por el contenido del mensaje" se referían de manera improcedente al derecho general de los contratos.

120. La opinión predominante fue que, por más que hubiese que modificar la redacción del proyecto de artículo E, el principio contenido en el párrafo 1) era útil para establecer las consecuencias jurídicas del uso de las firmas digitales. En cuanto a la manera en que cabría expresar un principio de esa índole, se sugirió redactar nuevamente el párrafo 1) en la forma de una presunción juris et de jure de manera que se considerase que el titular de una firma digital era el firmante del mensaje electrónico en el que se había puesto la firma digital.

121. En cuanto a la posibilidad de resolver la cuestión de la atribución de los mensajes con firma digital mediante presunciones, fuesen juris et de jure o juris tantum, se sugirió que quizás habría que hacer nuevas distinciones según el tipo de transacción para la cual se utilizase la firma digital. Por ejemplo, no se deberían utilizar las mismas normas para transacciones exclusivamente
comerciales entre asociados comerciales de larga data que para la presentación de declaraciones impositivas ante la administración pública.

122. Se señaló que en una disposición como la del párrafo 1) habría que distinguir entre los distintos tipos de firma digital (por ejemplo, el diverso grado de seguridad logrado de los diversos algoritmos y la variación correspondiente en el costo de la firma digital) y las distintas circunstancias en que se usaban firmas digitales. Se sugirió que, en la preparación del proyecto revisado del párrafo 1), se tuvieran en cuenta las categorías siguientes: si la firma digital se utilizaba fuera de un contrato preexistente entre las partes; si la firma digital se utilizaba en el contexto de un marco contractual; si para la firma digital se necesitaba la expedición de un certificado por una autoridad certificadora no acreditada o si el certificado había sido expedido por una autoridad certificadora autorizada. También se sugirió que, en relación con los distintos grados de riesgo que entrañaba el proceso de la firma digital en casos de fraude, se prestara particular atención al caso en que el fraude se produjera antes de la emisión de un par de claves. En una situación de ese tipo, a falta de acuerdo entre las partes, la carga de establecer el vínculo entre la firma digital y el expedidor debería recaer en el receptor. Si se hubiese expedido un certificado, y éste fuese válido y en debida forma, tal vez cabría desplazar la carga de la prueba. También se sugirió que, en el caso de los mensajes certificados por una autoridad certificadora, la parte que la hubiese designado debería soportar el riesgo que entrañara el uso de los certificados expedidos por ella.

123. Se expresaron dudas acerca de si, al revisar el proyecto de artículo E, habría que tener en cuenta todas las categorías mencionadas precedentemente. En particular, se recordó que en el contexto del debate sobre las cuestiones de responsabilidad, el Grupo de Trabajo había decidido centrar su atención en los casos en que se expedía un certificado. No obstante, se consideró en general que habría que tener presentes algunas de las categorías sugeridas al preparar el proyecto revisado de artículo E que se examinaría en un futuro período de sesiones del Grupo de Trabajo o todas ellas.

124. Tras un debate, el Grupo de Trabajo decidió que era necesaria una disposición relativa a la atribución de los mensajes firmados digitalmente, la cual podría redactarse siguiendo la pauta del párrafo 1) del proyecto de artículo E. Se consideró en general que se necesitarían comentarios adecuados para aclarar la relación entre el artículo E y los artículos 7 y 13 de la Ley Modelo. Se pidió a la Secretaría que preparase un proyecto revisado de artículo E, con distintas variantes que tuviesen en cuenta el debate que antecede.

6. Revocación de certificados

125. El Grupo de Trabajo basó su debate acerca de la revocación de certificados en el proyecto de disposición siguiente:

"Proyecto de artículo F

1) El titular de un juego de claves certificado podrá anular el certificado correspondiente. Esa anulación será efectiva desde el momento en que haya sido [inscrita] [recibida] por la entidad certificadora.

2) El titular de un juego de claves certificado estará obligado a hacer anular el certificado correspondiente si llega a su conocimiento que la clave criptográfica privada se ha perdido, o corre peligro o está expuesta a ser de algún otro modo indebidamente utilizada. El titular que, llegada esa situación, no haga anular el certificado será tenido por responsable de toda pérdida en que incurra un tercero que se haya fiado del contenido de un mensaje por no haber cumplido el titular con su obligación de anular el certificado.

Párrafo 1)

126. Se hicieron observaciones generales en cuanto al significado del párrafo 1). Se indicó que el tenedor de la clave privada siempre debía tener derecho a pedir a la autoridad certificadora que revocara un certificado. El hecho de que esa revocación se hiciera efectiva al recibo o registro por la autoridad certificadora no debía interpretarse como una limitación de ese derecho. Además, el hecho de que esa revocación se hiciera efectiva al recibo o registro por la autoridad certificadora no debía interpretarse en el sentido de que los terceros tenían la obligación de cerciorarse de la validez de un certificado (por ejemplo, que el certificado no había sido revocado) antes de confiar en un certificado, proposición que había suscitado diversas objeciones en el Grupo de Trabajo (véanse los párrafos).

127. Se expresaron diversas opiniones en cuanto al momento a partir del cual se hacía efectiva esa revocación. Según una opinión la revocación debía hacerse efectiva desde el momento en que la registrara la autoridad certificadora, ya que podía resultar difícil determinar el momento de la recepción en algunos casos, lo que provocaría incertidumbre en cuanto al momento en que un certificado dejara de ser válido. Según otra opinión la autoridad certificadora debía tener la obligación de actuar prontamente al revocarse un certificado de manera de evitar toda pérdida que pudiera sufrir el tenedor de la clave privada o terceros, y que podría dar como resultado, por ejemplo, que un certificado fuera aceptado por inadvertencia después de que ese certificado hubiera sido repudiado por su tenedor. Por lo tanto, los efectos de la revocación de un certificado debían depender de medidas que había de adoptar la autoridad certificadora, sobre las cuales el tenedor de la clave privada no tendría control.

128. Se plantearon dudas en cuanto al posible efecto del registro de la revocación de un certificado. A ese respecto se opinó que el concepto de registro de la revocación de un certificado podría no ser completamente adecuado a los efectos pretendidos por el artículo F, que entre otras cosas, estaba encaminado a asegurar que los terceros conocieran, en la medida correspondiente, el hecho de que un certificado determinado había sido revocado. Se dijo que, al recibir una solicitud relativa a la revocación, la autoridad certificadora podría en algunos casos verse obligada a verificar la autenticidad de esa solicitud, procedimiento que, según las circunstancias, podría implicar una demora. El momento apropiado para que esa revocación fuera plenamente efectiva, por lo tanto, era el momento en que se daba a conocer al público en general poniéndolo en una base de datos generalmente accesible que mantuviera la autoridad certificadora o por otro método apropiado de publicación.

129. En vista de esos comentarios, se señaló que la recepción de la solicitud de revocación seguía siendo preferible al registro para los efectos de determinar el momento a partir del cual se consideraba que el certificado había sido revocado. No obstante, si se estimaba que el concepto de recepción de esas solicitudes no era suficientemente preciso, podía combinarse la recepción con alguna medida que habría de tomar posteriormente la autoridad certificadora para dar efecto a esa revocación, como dar publicidad a la revocación o hacer una notificación a ese respecto.

130. A fin de adelantar sus deliberaciones sobre el tema, se invitó al Grupo de Trabajo a que considerara las consecuencias generales de una selección con respecto al momento en que se hacía efectiva la revocación, así como las partes que podrían ser afectadas por esa revocación. El momento en que la revocación se hacía efectiva sería

fundamental para determinar las responsabilidades respectivas del tenedor de la clave privada y las autoridades certificadoras entre ellos y respecto de terceros. Se sugirió que podría ser conveniente que el Grupo de Trabajo considerara la posibilidad de ocuparse de cada una de esas situaciones por separado. En apoyo de esa propuesta se indicó que cada una de las alternativas que actualmente figuraba en el párrafo 1) tenía sus propios méritos. Entre el tenedor de la clave privada y la autoridad certificadora podría ser apropiado disponer que la revocación se hiciera efectiva al recibir la autoridad certificadora la solicitud de revocación hecha por el tenedor de la clave privada. Pero respecto de terceros podía ser más apropiado exigir el registro o publicación previa para que la notificación surtiera efectos.

131. Se señaló que la fecha efectiva de la revocación tenía consecuencias significativas en cuanto a la responsabilidad de la autoridad certificadora y que ambas cuestiones debían tratarse en forma armónica. Se observó que el párrafo 4) del proyecto de artículo H disponía que, en los casos en que una autoridad certificadora autorizada hubiera recibido notificación de la revocación de un certificado, la autoridad debía registrar esa revocación inmediatamente. Si la autoridad certificadora no lo hacía, debía tener responsabilidad por toda pérdida que por ese motivo sufriera el usuario. De esta manera, si en el proyecto de normas uniformes se disponía que la revocación de un certificado fuera efectiva en el momento en que se recibiera, debía suprimirse el párrafo 4) del proyecto de artículo H por cuanto no podría dar base para la responsabilidad de la autoridad certificadora por culpa o negligencia en el registro de la revocación. No obstante, si la revocación de un certificado debía surtir efectos en el momento en que se registrara, podría no ser necesario una disposición además de la del párrafo 4) del artículo H.

132. En respuesta al comentario se observó que debía conservarse la norma que figuraba en el párrafo 4) del artículo H independientemente de la selección que hiciera el Grupo de Trabajo con respecto a las dos alternativas que actualmente figuraban en el párrafo 1) del artículo F. El registro tardío de una solicitud de revocación podría ser la causa de alguna pérdida, ya fuera para el propietario o para el tenedor, y, por lo tanto, sería necesario tener una norma relativa a la responsabilidad por las consecuencias del registro tardío.

133. A ese respecto se indicó que en las normas y directrices internacionales sobre certificación y autenticación electrónicas, como las directrices internacionales uniformes sobre prácticas de autenticación y certificación que estaba preparando la Cámara de Comercio Internacional, se reflejaba el principio de que una autoridad certificadora tenía que actuar prontamente respecto de una solicitud de revocación de un certificado. No obstante, como se había observado anteriormente, podría haber cierto retraso para dar efecto a esa solicitud, en particular en los casos en que, dadas las circunstancias, la autoridad certificadora tuviera que hacer alguna verificación, como confirmar las atribuciones de las personas que solicitaban la revocación en nombre del tenedor de la clave privada. A fin de evitar el uso por inadvertencia del certificado durante el período en que la autoridad certificadora estuviera verificando la revocación, se sugirió que se incluyera en el proyecto de normas uniformes una disposición en cuya virtud una autoridad certificadora debía suspender un
certificado prontamente al recibirse la solicitud de un tenedor de una clave privada. Se explicó que, a diferencia de la revocación, que ponía término a la validez del certificado, la suspensión sería una medida de carácter provisional que sólo retendría la validez del certificado durante un cierto período.

134. Se expresó apoyo a la introducción del concepto de suspensión del certificado a diferencia de la revocación abierta. No obstante, se sugirió que esa suspensión debía ser objeto de una disposición aparte, ya que el concepto y los efectos de una suspensión eran diferentes de los de una revocación.

135. Tras considerar las diferentes opiniones expresadas, el Grupo de Trabajo convino en que la cuestión de la revocación de los certificados era parte importante de un régimen jurídico adecuado de las firmas digitales y que merecía mayor consideración del Grupo de Trabajo. Se consideró en general que se necesitaban elementos adicionales en una disposición que tratara ese tema y se pidió a la Secretaría que preparara una disposición revisada en la que se tomaran en cuenta las deliberaciones del Grupo de Trabajo y se incluyeran posibles variantes relativas al momento en que debía hacerse efectiva la revocación. Se convino además en que el proyecto revisado debía contener disposiciones relativas a la suspensión de un certificado.

Párrafo 2)

136. Se sugirió que el uso de la palabra "obligación" en la primera oración del párrafo 2) no era del todo apropiado y que, en ese contexto, sería preferible usar palabras como "responsabilidad" o "deber".

137. Se sugirió que, además del tenedor de un par de claves certificadas, la autoridad certificadora también debía tener el deber de revocar el certificado correspondiente en los casos en que la autoridad certificadora se enterara de la pérdida de una clave criptográfica privada, de que estuviera expuesta o en peligro de ser utilizada indebidamente de otra manera. En apoyo de esa sugerencia se dijo que algunas normas y directrices internacionales sobre certificación y autenticación electrónicas, como las directrices internacionales uniformes sobre prácticas de autenticación y certificación que estaba preparando la Cámara de Comercio Internacional, preveían ese deber.

138. En respuesta a las preguntas relativas a la capacidad de la autoridad certificadora para cumplir ese deber, se indicó que la tecnología actualmente disponible permitía a un autoridad certificadora responder prontamente en esas situaciones. No obstante, el tiempo necesario para esa respuesta no era sólo una función de la tecnología disponible, sino que dependía además del nivel de los servicios prestados por una autoridad certificadora a sus clientes, en las condiciones de sus arreglos contractuales (por ejemplo, si la autoridad certificadora había designado funcionarios para encargarse de la pérdida, exposición o uso indebido de claves privadas; si la autoridad certificadora ofrecía servicios a los clientes en los fines de semana o sólo durante las horas normales de oficina).

139. El Grupo de Trabajo tomó nota de las opiniones expresadas y concordó en que debían tomarse en cuenta en sus futuras deliberaciones acerca de la emisión de la revocación de certificados.

5. Registro de certificados

140. El Grupo de Trabajo basó su examen del registro de certificados en el proyecto de disposición siguiente:

"Proyecto de artículo G

1) Toda entidad certificadora autorizada deberá llevar un registro electrónico de certificados emitidos, al que tenga acceso el público, indicando la fecha en que se emitió cada certificado, su fecha de expiración y la fecha en que fue suspendido o anulado.

2) La entidad certificadora deberá conservar esa inscripción en su registro por lo menos durante los [10] años siguientes a la fecha de anulación o de expiración del plazo de validez de todo certificado emitido por esa entidad certificadora."

141. Se pidió al Grupo de Trabajo que para empezar su examen del registro de certificados considerara la conveniencia de incluir una disposición sobre el particular en el proyecto de normas uniformes y que, en caso afirmativo, considerara también el contenido de ese registro y, si procedía, el período durante el cual se debía mantener.

142. Aunque no se plantearon objeciones de principio a la inclusión de una disposición sobre el registro de certificados, se indicó que el Grupo de Trabajo debía tener en cuenta si esa disposición era realmente necesaria en el contexto de las normas uniformes y si podía aplicarse a las diferentes clases de certificados que las autoridades certificadoras podían expedir.

143. En cuanto a la forma en que debía estructurarse el registro, se observó que tal vez fuera conveniente que las autoridades certificadoras pertenecientes a una misma infraestructura de claves públicas llevaran un registro centralizado donde anotaran los certificados expedidos, en lugar de llevar cada una su propio registro. La adopción de este sistema, cuyo propósito sería evitar la multiplicidad de registros, se estaba estudiando en algunos países. Se indicó que podría ser útil que el Grupo de Trabajo examinara esta posibilidad más detenidamente.

144. En relación con el párrafo 1 se observó que no era necesario que en el registro se indicase la fecha de expedición de los certificados y que, en consecuencia, la frase "indicando la fecha en que se expidió cada certificado" debía suprimirse. También se propuso que las autoridades certificadoras llevaran una base de datos separada en la que figuraran los certificados revocados a fin de facilitar las consultas de los interesados acerca de la validez de los certificados.

145. Hubo diversidad de opiniones en cuanto a la necesidad y suficiencia del período durante el cual debía mantenerse el registro según el párrafo 2. Se dijo que convenía establecer una duración mínima para asegurar el acceso de los interesados a la información, lo cual era especialmente importante en el contexto de los plazos establecidos por las leyes internas para ejercer o hacer valer los derechos o exigir el cumplimiento de las obligaciones. No obstante, las leyes internas establecen plazos diferentes para las distintas clases de derechos y obligaciones, así como diferentes plazos durante los cuales se deben mantener las inscripciones de los registros públicos y privados según su objeto. Dadas las circunstancias, tal vez sería preferible dejar al derecho interno la determinación de los plazos apropiados, en lugar de fijar arbitrariamente plazos que podrían no ser adecuados en todo caso. Además, el Grupo de Trabajo debía tener en cuenta el costo que suponía mantener un registro de certificados durante un plazo determinado. Dependiendo del servicio que la autoridad certificadora prestase y del método de registro que utilizase, tal vez no le resultara rentable comprometerse a mantener ciertos certificados más allá de un plazo determinado. No convendría tratar de fijar un plazo general sin recabar información sobre las consecuencias prácticas que esa disposición tendría para las empresas.

146. Según otra opinión, sin embargo, la cuestión del mantenimiento de los registros y de la información que permitiese a los interesados constatar la identidad y la autenticidad de las firmas de las personas con quienes negociaran tenía varias repercusiones de política pública que el Grupo de Trabajo no debía ignorar. El proyecto de normas uniformes debía regular esta cuestión. En cuanto al plazo de mantenimiento adecuado se propuso que las autoridades certificadoras no pudieran establecerlo unilateralmente sólo en razón de los costos. Además, el simple

costo del mantenimiento no debía ser un factor determinante para su reducción o supresión. Las autoridades certificadoras que anotaran los certificados expedidos en un mismo registro correspondiente a una infraestructura de claves públicas podían establecer un mecanismo para repartirse los costos.

147. Se propuso que los interesados que consultaran un registro de certificados tuvieran la obligación de dejar alguna constancia de que habían hecho la consulta. Se explicó que esa constancia podía ser importante si surgía una controversia entre la autoridad certificadora y el interesado en cuanto a si éste había comprobado la validez del certificado antes de confiar en un mensaje con firma digital.

148. El Grupo de Trabajo tomó nota de las distintas opiniones expresadas y pidió a la Secretaría que examinara las cuestiones planteadas y formulara proyectos de disposiciones alternativas teniendo en cuenta el debate desarrollado en el Grupo de Trabajo.

8. Relaciones entre los usuarios y la autoridad certificadora

149. El Grupo de Trabajo tuvo ante sí el siguiente proyecto de disposición:

"Proyecto de artículo J

"Proyecto de artículo J

1) La entidad certificadora sólo podrá pedir los datos que necesite para identificar al usuario.

2) A petición de personas jurídicas o naturales, la entidad certificadora dará a conocer los datos siguientes:

a) Las condiciones para la utilización del certificado;

b) Las condiciones a que está sujeto el empleo de una firma numérica;

c) Las tarifas de los servicios de la entidad certificadora;

d) La política o las prácticas de la autoridad certificadora con respecto a la utilización, el archivo y la comunicación de datos personales;

e) Las especificaciones técnicas de la entidad 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 de algún defecto de funcionamiento del equipo de comunicaciones;

g) Toda limitación de la responsabilidad de la entidad certificadora;

h) Cualquier restricción impuesta por la entidad certificadora respecto del empleo del certificado;

i) Las condiciones en las que el usuario tendrá derecho a poner restricciones al uso del certificado.

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

4) Con un preaviso [de un mes], el usuario podrá dar por terminado el acuerdo de vinculación a la entidad certificadora. Ese preaviso surtirá efecto al ser recibido por la autoridad certificadora.

5) Con un preaviso [de tres meses], la autoridad certificadora podrá dar por terminado ese mismo acuerdo. Ese preaviso surtirá efecto desde el momento de su recepción."

150. El Grupo de Trabajo observó que, en la medida en que el proyecto de artículo J se ocupaba de las relaciones entre los usuarios y la autoridad certificadora, presuponía decisiones sobre diversas cuestiones que el Grupo de Trabajo aún estaba examinando. Se acordó que todo el proyecto de artículo J fuera entre corchetes y que el Grupo de Trabajo lo examinara en una fase posterior.

III. INCORPORACIÓN POR REMISIÓN

151. Después de haber concluido su análisis preliminar de las cuestiones jurídicas y posibles disposiciones que se deben tener en cuenta en las normas uniformes sobre firmas digitales, análisis que se consigna en la parte II del presente informe, el Grupo de Trabajo consideró que, por falta de tiempo, no podía examinar detenidamente las cuestiones de la incorporación por remisión en el período de sesiones en curso.

152. El Grupo de Trabajo recordó que la cuestión de la incorporación por remisión se había examinado someramente en diferentes momentos durante la preparación de la Ley Modelo (véase). En el período de sesiones anterior, el Grupo de Trabajo llegó a la conclusión general de que era preciso examinar la incorporación por remisión en el contexto del comercio electrónico. Se expresó la opinión de que, en caso de que se intentaran establecer normas jurídicas para proceder a la incorporación de cláusulas de remisión en los mensajes de datos, deberían cumplirse las tres condiciones siguientes: a) la cláusula de remisión debería incluirse en el mensaje de datos; b) el documento al que se hiciera la remisión (por ejemplo, las condiciones y cláusulas generales) tenía que ser conocido de hecho por la parte contra la que podría hacerse valer el documento de remisión; y c) el documento de remisión tenía que ser no sólo conocido, sino también aceptado por esa parte. En términos generales, se consideró que el tema de la incorporación por remisión debería examinarse en el contexto de la labor general que se estaba realizando sobre las cuestiones relativas a los registros y proveedores de servicios (A/CN.9/421, párr. 114). En su 29º período de sesiones, la Comisión había considerado que la cuestión podía examinarse en el contexto de la labor sobre las autoridades certificadoras[1].

153. En el período de sesiones en curso, se extendió la opinión de que la aceptabilidad de la incorporación por remisión era de considerable importancia para el desarrollo del comercio electrónico en general. Aunque podía ser necesario que esa cuestión fuera examinada en el contexto de la labor sobre las firmas digitales y las autoridades certificadoras, también debería ser examinada a nivel más general. Aunque posteriormente se considerase adecuado establecer normas concretas para la incorporación por remisión en el contexto de las firmas digitales, era necesario celebrar un debate general y posiblemente establecer un conjunto general de normas.

154. Se expresó la opinión de que el establecimiento de normas para la incorporación por remisión en un entorno electrónico podía constituir una tarea difícil, habida cuenta de la complejidad de las cuestiones que se planteaban al respecto. La incorporación por remisión y las cuestiones conexas, como los contratos de adhesión y la "batalla de las formas", habían dado lugar a una amplia variedad de normas jurídicas en un medio de documentación escrita y no todas las cuestiones jurídicas conexas se habían resuelto de manera satisfactoria. El tema hacía necesario lograr un equilibrio entre intereses contrapuestos. Por una parte, era preciso reconocer la autonomía de las partes. Por otra, debían limitarse posibles abusos en los contratos de adhesión. Habida cuenta de las dificultades que se preveían en el ámbito de la incorporación por remisión, se sugirió que se considerasen con un mayor grado de prioridad otras cuestiones que también podían exigir un estudio más detenido en el contexto del comercio electrónico. Según otra opinión, sólo podía celebrarse un debate sobre la incorporación por remisión tomando como base nuevos estudios de la Secretaría relativos a los aspectos de los contratos de adhesión en el derecho comparado, la "batalla de las formas" y las cuestiones conexas de la responsabilidad.

155. Prevaleció la opinión de que no era necesario realizar un nuevo estudio, dado que las cuestiones fundamentales eran bien conocidas y quedaba claro que muchos aspectos de la cuestión de la "batalla de las formas" y los contratos de adhesión deberían precisarse en la legislación nacional aplicable, por consideraciones relacionadas, entre otras cosas, con la protección de los consumidores y las normas de actuación de los poderes públicos. Tras el correspondiente debate, el Grupo de Trabajo decidió que la cuestión debería examinarse como primer tema sustantivo de su programa, al comienzo de su período de sesiones siguiente.

IV. FUTURA LABOR

156. El Grupo de Trabajo recordó que la Comisión había pedido que examinase la conveniencia y la viabilidad de preparar normas uniformes sobre cuestiones relacionadas con las firmas digitales y las autoridades certificadoras. Al término de su período de sesiones, el Grupo de Trabajo consideró que en el informe que presentaría a la Comisión debería indicarse que había logrado un consenso en relación con la importancia y la necesidad de proceder a la armonización de la legislación en ese ámbito. El Grupo de Trabajo no había adoptado una decisión firme respecto de la forma y el contenido de su labor al respecto, si bien había llegado a la conclusión preliminar de que era viable emprender la preparación de un proyecto de normas uniformes sobre cuestiones relacionadas con las firmas digitales.

157. Al examinar la futura labor del Grupo de Trabajo, se recordó que, al margen de las cuestiones de las firmas digitales y las autoridades certificadoras, también podía ser necesario que se examinaran las cuestiones siguientes en el ámbito del comercio electrónico: alternativas técnicas a la criptografía de clave pública; cuestiones generales relacionadas con los terceros que eran proveedores de servicios; y la contratación electrónica.

Notas

[1] Documentos Oficiales de la Asamblea General, quincuagésimo primer período de sesiones, Suplemento No. 17 (A/51/17), párr. 222.
