



Asamblea General

Distr.
LIMITADA

A/CN.9/WG.IV/WP.76
25 de mayo de 1998

ESPAÑOL
Original: INGLÉS

COMISIÓN DE LAS NACIONES UNIDAS PARA
EL DERECHO MERCANTIL INTERNACIONAL
Grupo de Trabajo sobre Comercio Electrónico
33º período de sesiones
Nueva York, 29 de junio a 10 de julio de 1998

PROYECTO DE RÉGIMEN UNIFORME PARA LAS FIRMAS ELECTRÓNICAS

Nota de la Secretaría

ÍNDICE

	<u>Párrafos</u>	<u>Página</u>
INTRODUCCIÓN	1 - 8	3
I. OBSERVACIONES GENERALES	9 - 11	5
II. PROYECTOS DE DISPOSICIÓN SOBRE FIRMAS NUMÉRICAS, OTRAS FIRMAS ELECTRÓNICAS, AUTORIDADES CERTIFICADORAS Y CUESTIONES JURÍDICAS CONEXAS	12 - 50	5
CAPÍTULO I. ESFERA DE APLICACIÓN Y DISPOSICIONES GENERALES	12 - 15	5
CAPÍTULO II. FIRMAS ELECTRÓNICAS	16 - 38	6
Sección I. Firmas electrónicas en general	16 - 22	6
Artículo 1. Definiciones	16 - 20	6
Artículo 2. Efectos de la firma electrónica	21	9
Sección II. Firmas electrónicas [seguras] [refrendadas]	22 - 30	10
Artículo 3. Presunción de firma	22 - 23	10

	<u>Párrafos</u>	<u>Página</u>
Artículo 4. Presunción de atribución	24	11
Artículo 5. Presunción de integridad	25 - 26	11
Artículo 6. Predeterminación de la firma electrónica [segura] [refrendada]	27	12
Artículo 7. Responsabilidad respecto de la firma electrónica [segura] [refrendada]	28 - 30	12
Sección III. Firmas numéricas respaldadas por certificados	31 - 38	13
Artículo 8. Contenido del certificado [seguro] [refrendado]	31	13
Artículo 9. Efectos de las firmas numéricas respaldadas por certificados	32 - 38	14
CAPÍTULO III. AUTORIDADES CERTIFICADORAS Y CUESTIONES CONEXAS	39 - 47	16
Artículo 10. Declaración al emitir un certificado	39	16
Artículo 11. Responsabilidad contractual	40	17
Artículo 12. Responsabilidad de la entidad certificadora frente a las partes que se fian de los certificados	41	18
Observación general relativa a los proyectos de artículo 13 a 16	42	19
Artículo 13. Revocación de certificados	43	19
Artículo 14. Suspensión de certificados	44	21
Artículo 15. Registro de certificados	45 - 46	21
Artículo 16. Relaciones entre las partes que se fian de los certificados y las autoridades certificadoras	47	22
CAPÍTULO IV. FIRMAS ELECTRÓNICAS EXTRANJERAS	48 - 50	23
Artículo 17. Prestación de servicios por autoridades certificadoras extranjeras	48	23
Artículo 18. Homologación de certificados extranjeros por autoridades certificadoras nacionales	49	24
Artículo 19. Reconocimiento de certificados extranjeros	50	25

INTRODUCCIÓN

1. La Comisión, en su 29º período de sesiones (1996), decidió incluir en su programa las cuestiones de las firmas digitales y las autoridades certificadoras. Se pidió al Grupo de Trabajo sobre Comercio Electrónico que examinase la conveniencia y viabilidad de preparar normas uniformes sobre los temas mencionados. Se convino en que la labor que había de llevar a cabo el Grupo de Trabajo en su 31º período de sesiones podía incluir la preparación de proyectos de normas sobre ciertos aspectos de dichos temas. Se pidió al Grupo de Trabajo que proporcionara a la Comisión elementos suficientes para adoptar una decisión informada acerca del ámbito de las normas uniformes que habían de elaborarse. Se convino además, como mandato más preciso para el Grupo de Trabajo, que las normas uniformes que había de preparar se refirieran a cuestiones tales como la base jurídica que sustentaba los procesos de certificación, incluida la tecnología incipiente de autenticación y certificación digitales; la aplicabilidad del proceso de certificación; la asignación del riesgo y la responsabilidad de los usuarios, proveedores y terceros en el contexto del uso de técnicas de certificación; las cuestiones concretas de certificación mediante el uso de registros y la incorporación por remisión¹.

2. En su 30º período de sesiones (1997), la Comisión tuvo ante sí el informe del Grupo de Trabajo acerca de la labor de su 31º período de sesiones (A/CN.9/437). En lo que se refiere a la conveniencia y la viabilidad de preparar normas uniformes sobre cuestiones relacionadas con las firmas numéricas y las autoridades certificadoras, el Grupo de Trabajo indicó a la Comisión que había logrado un consenso en relación con la importancia y la necesidad de proceder a la armonización de la legislación en ese ámbito. Aunque no había adoptado una decisión firme respecto de la forma y el contenido de su labor al respecto, había llegado a la conclusión preliminar de que era viable emprender la preparación de un proyecto de normas uniformes, por lo menos sobre cuestiones relacionadas con las firmas numéricas y las autoridades certificadoras y posiblemente sobre asuntos conexos. El Grupo de Trabajo recordó que, al margen de las cuestiones de las firmas numéricas y las autoridades certificadoras, también podía ser necesario que se examinaran 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 (A/CN.9/437, párrs. 156 y 157). Con respecto a la cuestión de la incorporación por remisión, el Grupo de Trabajo llegó a la conclusión de que no era necesario realizar ningún nuevo estudio de la Secretaría, dado que las cuestiones fundamentales eran bien conocidas y quedaba claro que muchos aspectos de la cuestión de la batalla de los formularios 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 otras consideraciones de orden público. El Grupo de Trabajo fue del parecer de que la cuestión debería examinarse como primer tema sustantivo de su programa, al comienzo de su período de sesiones siguiente (A/CN.9/437, párr. 155).

3. La Comisión expresó su reconocimiento por la labor ya efectuada por el Grupo de Trabajo en su 31º período de sesiones, hizo suyas las conclusiones del Grupo y le encomendó la preparación de un régimen uniforme sobre las cuestiones jurídicas relacionadas con las firmas numéricas y las autoridades certificadoras (denominado en adelante "el Régimen Uniforme").

4. Con respecto a la forma y al alcance exactos del Régimen Uniforme, la Comisión convino en que no era posible adoptar una decisión al respecto en una etapa tan temprana. Se opinó que, si bien el Grupo de Trabajo podría concentrar su atención en las cuestiones de las firmas numéricas, en vista de la función predominante aparentemente desempeñada por la criptografía de clave pública en la práctica más reciente en materia de comercio electrónico, el Régimen Uniforme que se preparara debería atenerse al criterio de neutralidad adoptado en la Ley Modelo de la CNUDMI sobre Comercio Electrónico. Por ello, el Régimen Uniforme no debería desalentar el recurso a otras técnicas de autenticación. Además, al ocuparse de la criptografía de clave pública, tal vez fuera preciso que el Régimen Uniforme acomodara diversos grados de seguridad y reconociera diversos efectos jurídicos y grados de responsabilidad según cuales fueran los servicios prestados en el contexto de las

firmas numéricas. Respecto de las autoridades certificadoras, si bien la Comisión reconoció el valor de las normas de fiabilidad o seguridad fijadas por el mercado, predominó el parecer de que el Grupo de Trabajo podría considerar el establecimiento de un juego de normas mínimas que las autoridades certificadoras habrían de respetar estrictamente, particularmente en casos en los que se solicitara una certificación de validez transfronteriza².

5. El Grupo de Trabajo comenzó la preparación del Régimen Uniforme en su 32º período de sesiones sobre la base de una nota preparada por la Secretaría (A/CN.9/WG.IV/WP.73). Se pidió a la Secretaría que preparase, sobre la base de las deliberaciones y conclusiones del Grupo de Trabajo, un juego de disposiciones revisadas, con posibles variantes, para que pudiera examinarlo el Grupo de Trabajo en un período de sesiones futuro (el informe sobre la labor del mencionado período de sesiones figura en el documento A/CN.9/446). En cuanto a la incorporación por remisión, el Grupo de Trabajo adoptó el texto de un proyecto de disposición, decidió que dicho texto debía presentarse a la Comisión para que lo examinase y posiblemente lo añadiese como nuevo artículo 5 bis de la Ley Modelo de la CNUDMI sobre Comercio Electrónico, y pidió a la Secretaría que preparase una nota explicativa para añadirla a la Guía de aplicación de la Ley Modelo (A/CN.9/446, párr. 24).

6. La presente nota contiene proyectos de disposición revisados que se prepararon de conformidad con las deliberaciones y decisiones del Grupo de Trabajo, así como con las deliberaciones y decisiones de la Comisión en su 30º período de sesiones, antes mencionadas. En particular, los proyectos de disposición se basan en la hipótesis de trabajo del Grupo de Trabajo de que su labor en el ámbito de las firmas numéricas adoptaría la forma de un proyecto de disposiciones legales (A/CN.9/437, párr. 27). Obedecen además al propósito de reflejar la decisión tomada por el Grupo de Trabajo en su 31º período de sesiones de que las posibles normas uniformes en el ámbito de las firmas numéricas deberían emanar del artículo 7 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico (denominada en adelante "la Ley Modelo") y que había que considerar que fijaban la manera en que se podía utilizar un método fiable "para identificar a una persona" y "para indicar que esa persona aprueba" la información contenida en un mensaje de datos.

7. En la preparación de la presente nota, la Secretaría fue asistida por un grupo de expertos que comprendía expertos invitados por la Secretaría y expertos designados por gobiernos interesados y organizaciones internacionales.

8. En consonancia con las instrucciones aplicables acerca de la limitación y el control más estrictos de los documentos de las Naciones Unidas, las observaciones explicativas referentes a los proyectos de disposición se han formulado de la forma más breve posible. En el período de sesiones se proporcionarán más explicaciones orales.

I. OBSERVACIONES GENERALES

9. La finalidad del Régimen Uniforme, según se refleja en los proyectos de disposición que figuran en la parte II de la presente nota, es facilitar la utilización cada vez mayor de las firmas electrónicas en las operaciones comerciales internacionales. Inspirándose en los múltiples instrumentos legislativos ya en vigor o en curso de elaboración en varios países, estos proyectos de disposición se proponen impedir la desarmonía en las reglas jurídicas aplicables al comercio electrónico proporcionando un conjunto de normas sobre cuya base puedan reconocerse los efectos jurídicos de las firmas numéricas y otras firmas electrónicas, con el posible auxilio de autoridades certificadoras, para las cuales se ofrecen también varias reglas básicas.

10. Centrado en los aspectos de derecho privado de las operaciones comerciales, el Régimen Uniforme no intenta resolver todas las cuestiones que pueden plantearse en el contexto de la mayor utilización de las firmas electrónicas. En particular, el Régimen Uniforme no trata los aspectos de orden público, derecho administrativo, protección del consumidor o derecho penal que quizá los legisladores nacionales tengan que tener presentes al establecer un marco jurídico completo para las firmas electrónicas.

11. Sobre la base de la Ley Modelo, el Régimen Uniforme se propone reflejar en particular: el principio de la neutralidad en lo relativo a los medios técnicos; un enfoque conforme al cual no se discrimine contra los equivalentes funcionales de los conceptos y prácticas tradicionales en un medio de documentación escrita; y un amplio recurso a la autonomía de la voluntad de las partes. Está pensado para utilizarlo a la vez como normas mínimas en un entorno "abierto" (es decir, en que las partes se comunican electrónicamente sin acuerdo previo) y como normas supletorias en un entorno "cerrado" (es decir, donde las partes están vinculadas por normas y procedimientos contractuales preexistentes que se han de observar en la comunicación por medios electrónicos).

II. PROYECTOS DE DISPOSICIÓN SOBRE FIRMAS NUMÉRICAS, OTRAS FIRMAS ELECTRÓNICAS, AUTORIDADES CERTIFICADORAS Y CUESTIONES JURÍDICAS CONEXAS

CAPÍTULO I. ESFERA DE APLICACIÓN Y DISPOSICIONES GENERALES

12. Al examinar el proyecto de disposiciones que se propone se incluyan en el Régimen Uniforme, el Grupo de Trabajo tal vez desee considerar en términos más generales la relación entre el Régimen Uniforme y la Ley Modelo. En particular, el Grupo de Trabajo podría quizá formular propuestas a la Comisión sobre si el Régimen Uniforme para las firmas numéricas debería constituir un instrumento aparte o si habría que incorporarlo en una versión ampliada de la Ley Modelo, por ejemplo como nueva Parte III de la Ley Modelo.

13. Si el Régimen Uniforme se prepara como instrumento aparte, se supone que tendrá que contener disposiciones acordes con el artículo 1 (Ámbito de aplicación), los incisos a), b) y c) del artículo 2 (Definiciones de "mensaje de datos" "iniciador" y "destinatario"), y los artículos 3 (Interpretación), 7 (Firma) y 13 (Atribución de mensajes de datos) de la Ley Modelo. Aunque esos artículos no se reproducen en la presente nota, cabe observar que el proyecto de disposiciones del Régimen Uniforme ha sido preparado por la Secretaría basándose en el supuesto de que esas disposiciones formarían parte del Régimen Uniforme. Con respecto al ámbito de aplicación de este último, hay que tener presente que, según el artículo 1 de la Ley Modelo, las operaciones en que participen consumidores, por más que no sean objeto particular del Régimen Uniforme, no serían excluidas de su ámbito de aplicación a menos que la ley aplicable a las operaciones en que intervengan consumidores del Estado promulgante estén en conflicto con el Régimen Uniforme.

14. En cuanto a la cuestión de la autonomía de la voluntad de las partes, la mera referencia al artículo 4 (Modificación mediante acuerdo) de la Ley Modelo no basta para obtener una solución satisfactoria en vista del hecho de que el artículo 4 establece una distinción entre las disposiciones de la Ley Modelo que pueden ser libremente modificadas por contrato y las que deben considerarse imperativas a menos que la modificación mediante acuerdo esté autorizada por la ley aplicable fuera de la Ley Modelo. Con respecto a las firmas electrónicas, la importancia práctica de las redes "cerradas" hace necesario prever un amplio reconocimiento de la autonomía de la voluntad de las partes. No obstante, posiblemente haya que tener también en cuenta las restricciones de orden público a la libertad contractual, incluidas las leyes que protegen a los consumidores de contratos de adhesión exorbitantes. El Grupo de Trabajo podría, pues, querer incluir en el Régimen Uniforme una disposición análoga al párrafo 1) del artículo 4 de la Ley Modelo al efecto de que, salvo disposición en contrario del Régimen Uniforme u otra ley aplicable, las firmas electrónicas y los certificados emitidos, recibidos o aceptados como válidos de conformidad con los procedimientos acordados entre las partes en una operación tienen la eficacia especificada en el acuerdo. Además, el Grupo de Trabajo podría examinar la posibilidad de establecer una regla de interpretación en el sentido de que, al determinar si un certificado, una firma electrónica o un mensaje de datos verificados con referencia a un certificado, es suficientemente fiable para un fin particular, han de tenerse en cuenta todos los acuerdos pertinentes entre las partes, la conducta observada entre ellas y los usos mercantiles pertinentes.

15. Además de las mencionadas disposiciones, el Grupo de Trabajo quizá desee ponderar si un preámbulo serviría para aclarar la finalidad del Régimen Uniforme, a saber, fomentar la eficiente utilización de la comunicación digital creando un marco de seguridad y otorgando a los mensajes escritos y numéricos igual condición por lo que se refiere a su eficacia jurídica.

CAPÍTULO II. FIRMAS ELECTRÓNICAS

Sección I. Firmas electrónicas en general

Artículo 1. Definiciones

Para los fines del presente Régimen:

- a) por "firma electrónica" se entenderá los datos en forma electrónica adjuntos a un mensaje de datos o lógicamente vinculados con él, y que [puedan utilizarse] se utilicen para [identificar al firmante del mensaje de datos e indicar que el firmante aprueba la información contenida en el mensaje de datos] [satisfacer las condiciones del inciso a) del párrafo 1 del artículo 7 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico];
- b) por "firma electrónica [segura] [refrendada]" se entenderá una firma electrónica que [se creó y que] [al tiempo en que se consignó] pueda verificarse mediante la aplicación de un procedimiento de seguridad o una combinación de procedimientos de seguridad que vele por que dicha firma electrónica:
 - i) sea exclusiva del firmante [para la finalidad para la que] [dentro del contexto en el que] se consigne;
 - ii) se pueda utilizar para identificar objetivamente al firmante del mensaje de datos;
 - iii) fue creada y añadida al mensaje de datos por el firmante o utilizando un medio bajo el control exclusivo del firmante; [y]

[iv) ha sido creada y está vinculada con el mensaje de datos a que se refiere de modo que, si el mensaje es alterado, quede revelada la alteración]

c) Variante A

por "firma numérica" se entenderá una firma electrónica creada mediante la transformación de un mensaje de datos utilizando una función que resuma mensajes, y codificando la transformación resultante con un sistema criptográfico asimétrico que use la clave privada del firmante, de forma que cualquier persona que tenga el mensaje de datos inicial no transformado, la transformación codificada, y la clave pública correspondiente del firmante pueda determinar [exactamente]:

- i) si la transformación se efectuó utilizando la clave privada que corresponde a la clave pública del firmante; y
- ii) si el mensaje inicial de datos ha sido alterado desde que se efectuó la transformación.

Variante B

por "firma numérica" se entenderá una transformación criptográfica (que utilice una técnica de criptografía asimétrica) de la representación numérica de un mensaje de datos, de forma que cualquier persona que tenga el mensaje de datos y la clave pública correspondiente pueda determinar:

- i) que la transformación se efectuó utilizando la clave privada correspondiente a la clave pública pertinente; y
- ii) que el mensaje de datos no ha sido alterado después de la transformación criptográfica.

d) por "autoridad certificadora" se entenderá toda persona o entidad que en el desempeño de sus funciones, extienda certificados [de identificación] en relación con las claves criptográficas utilizadas a efectos de las firmas numéricas. [Esta definición está subordinada a toda norma legislativa aplicable que requiera que una autoridad certificadora esté en posición de una licencia, o esté acreditada, u opere de la forma que se especifique en dicha norma.]

e) por "certificado [de identificación]" se entenderá un mensaje de datos u otra constancia que haya emitido una autoridad certificadora con la intención de confirmar la identificación [u otra característica importante] de una persona o entidad que tiene en su poder un juego determinado de claves.

f) por "certificado [seguro] [refrendado]" se entenderá un certificado [de identificación] emitido con objeto de refrendar firmas electrónicas [seguras] [refrendadas].

g) por "declaración sobre prácticas de certificación" se entenderá una declaración publicada por una autoridad certificadora en la que se especifiquen las prácticas que la autoridad certificadora emplee en la emisión y demás manipulaciones de certificados.

h) por "firmante" se entenderá la persona que consigna, o en cuyo nombre se consigne, [una firma electrónica] [una serie de datos como firma electrónica].

Referencias

A/CN.9/446, párrs. 27-46 (proyecto de artículo 1), 62-70 (proyecto de artículo 4), 113-131 (proyecto de artículo 8), 132 y 133 (proyecto de artículo 9);

A/CN.9/WG.IV/WP.73, párrs. 16-27, 37 y 38, 50-57, y 58-60;

A/CN.9/437, párrs. 29-50 y 90-113 (proyecto de artículos A, B y C); y

A/CN.9/WG.IV/WP.71, párrs. 52-60.

Observaciones

Definiciones de "firma electrónica" y de "firma electrónica [segura] [refrendada]"

16. De conformidad con la decisión adoptada por el Grupo de Trabajo en su 32º período de sesiones (A/CN.9/446, párr. 30), la definición de "firma electrónica" remite al artículo 7 de la Ley Modelo. Según la decisión que se adopte respecto de la relación entre el Régimen Uniforme y la Ley Modelo, es posible que sea preciso indicar íntegramente las disposiciones del inciso a) del párrafo 1 del artículo 7 de la Ley Modelo.

17. La distinción entre una noción amplia de "firma electrónica" y una categoría menos amplia (denominada provisionalmente firma electrónica "segura" o "refrendada") se ha mantenido a fin de poner de relieve las diferencias de naturaleza jurídica de los dos tipos de procedimientos. Por una parte, una amplia gama de técnicas de autenticación no especificadas (denominadas "firmas electrónicas") podrían obtener reconocimiento jurídico como firma de significancia jurídica, siempre que cumplan las condiciones de fiabilidad que se indican en el inciso b) del párrafo 1) del artículo 7 de la Ley Modelo, que habría que establecer después de que se haya utilizado la firma electrónica y que, típicamente, requeriría la intervención de un juez, árbitro, u otro verificador de hechos. Por otra parte, algunas técnicas de autenticación designadas mediante procedimientos administrativos para que las defina cada Estado promulgante o como resultado de acuerdo expreso entre las partes, gozaría de reconocimiento por anticipado como equivalente funcional de las firmas manuscritas.

Definición de "firma numérica"

18. La categoría de "firmas numéricas" no se define como subdivisión de las firmas electrónicas "refrendadas". Esto es así para reflejar el hecho de que, aunque en la mayor parte de las situaciones las técnicas "numéricas" (recurriendo o sin recurrir a las autoridades certificadoras) se utilizarán para obtener los efectos jurídicos previstos para la categoría más "segura" de las firmas electrónicas, dichas técnicas también se pueden utilizar en un contexto menos específico. O sea que la definición de "firma numérica" tiene por finalidad poner de relieve el carácter neutral del Régimen Uniforme.

Definición de "autoridad certificadora"

19. El Régimen Uniforme no enuncia ningún requisito que hayan de cumplir las autoridades certificadoras antes de que se les permita operar. Esta cuestión se examinó en el Grupo de Trabajo en períodos de sesiones anteriores y también se trata de ella en el proyecto de artículo 19. Si se considerase necesario proporcionar orientación a los Estados promulgantes, sea en el texto del Régimen Uniforme, sea en una guía de aplicación, habrá que tener en cuenta el siguiente ejemplo de posible disposición:

Las autoridades certificadoras deberán:

- a) ser suficientemente fiables para ofrecer servicios de certificación;

- b) emplear personal que posea los conocimientos, la experiencia y las cualificaciones necesarios para los servicios ofrecidos;
- c) utilizar sistemas fiables y equipo y programas de informática generalmente reconocidos que sean adecuados para el tipo de servicio y el grado de seguridad que se ofrecen;
- d) poseer suficientes recursos financieros para operar de conformidad con [el presente Régimen];
- e) conservar toda la información pertinente relativa a un certificado [seguro] [refrendado] durante un período apropiado de tiempo, en particular para estar en condiciones de brindar pruebas de la certificación en el contexto de una acción judicial. Esa conservación debe hacerse por medios electrónicos;
- f) publicar todas las informaciones pertinentes relativas a la utilización adecuada y segura de servicios de certificación y establecer procedimientos para la solución de controversias y reclamaciones; y
- g) publicar, con relación a los servicios disponibles para el público, toda la información pertinente relativa a los procedimientos seguidos y las prácticas aplicadas, los términos y las condiciones de los contratos, en particular las obligaciones que se asumen en materia de responsabilidad, así como los procedimientos de solución de controversias y reclamaciones que aplican; la publicación será accesible fácilmente y de forma apropiada.

Definiciones de "certificado [de identificación]" y de "certificado [seguro] [refrendado]"

20. Las definiciones de los incisos e) y f) se basan en la sugerencia hecha en el 32º período de sesiones del Grupo de Trabajo de que se diferencien los casos en los que se utilizaron firmas numéricas a efectos de transacciones de comercio internacional con intención de firmar (es decir, de identificar al firmante y de vincular al firmante con la información que se firma), y otros usos de las firmas numéricas, por ejemplo para determinar el nivel de autoridad de una persona ("certificados de autoridad") (véase A/CN.9/446, párr. 72). Aunque las disposiciones contenidas en el capítulo III del Régimen Uniforme tratan principalmente de las técnicas de firma numérica como medio de establecer una equivalencia predeterminada con las firmas manuscritas, el Grupo de Trabajo quizá desee examinar hasta qué punto se debe tratar de las técnicas de firma numérica en otros contextos. Si el Régimen Uniforme estima que las firmas numéricas son equivalentes a las firmas manuscritas, entonces quizá sea necesario distinguir entre "certificados", "certificados de identificación" y "certificados [seguros] [refrendados]". Cabe recordar que cualquier otro uso de firmas digitales que requieran un grado inferior de seguridad puede quedar abarcado también por las disposiciones generales del proyecto de artículo 2.

Artículo 2. Efectos de la firma electrónica

- 1) Por lo que se refiere a un mensaje de datos autenticado mediante una firma electrónica [que no sea una firma electrónica segura], la firma electrónica satisfará todos los requisitos jurídicos para una firma si la firma electrónica es tan fiable como procedente para la finalidad para la cual se consignó, a la luz de todas las circunstancias, incluido cualquier acuerdo que pueda existir sobre el particular.
- 2) El párrafo 1) se aplicará si los requisitos jurídicos mencionados en él revisten la forma de una obligación o si la ley prevé sencillamente las consecuencias en caso de falta de una firma.
- 3) A no ser que se disponga expresamente otra cosa en [el presente Régimen], las firmas electrónicas que no sean firmas electrónicas [seguras] [refrendadas] no quedarán sujetas a los reglamentos, normas o

procedimientos de concesión de licencias establecidos por ... [las autoridades o los órganos especificados por el Estado que se mencionan en el artículo] o a las presunciones establecidas por los artículos 4, 5 y 6.

4) Lo dispuesto en el presente artículo no será aplicable a: [...].

Referencias

A/CN.9/446, párrs. 27-46 (proyecto de artículo 1).

Observaciones

21. La finalidad del proyecto de artículo 2 es tratar del efecto jurídico de las firmas electrónicas que no satisfacen los requisitos establecidos para el reconocimiento de su carácter "seguro" o "refrendado". En consonancia con el mandato recibido de la Comisión y con opiniones expresadas en el 32º período de sesiones del Grupo de Trabajo (véase A/CN.9/446, párrs. 4 y 45), la finalidad del proyecto de artículo era conseguir que el Reglamento Uniforme se atuviera al criterio de neutralidad respecto de los medios disponibles, dejar bien sentado que no estaba prohibida la utilización de técnicas de autenticación de bajo nivel de seguridad, y prever el debido reconocimiento de la autonomía de la voluntad de las partes, sin permitirles que hagan derogaciones respecto de las normas legislativas obligatorias relativas a las firmas. Los párrafos 1), 2) y 4) no hacen más que reiterar disposiciones ya contenidas en el artículo 7 de la Ley Modelo. El párrafo 3) trata de la distinción que ha de establecerse entre los efectos jurídicos de las firmas electrónicas en general, y los resultantes de las técnicas de autenticación "seguras" o "refrendadas".

Sección II. Firmas electrónicas [seguras] [refrendadas]

Artículo 3. Presunción de firma

1) Se presume que un mensaje de datos ha sido firmado [si] [a partir del momento en que] una firma electrónica [segura] [refrendada] ha sido consignada en el mensaje de datos.

2) Lo dispuesto en el presente artículo no será aplicable a: [...].

Referencias

A/CN.9/446, párrs. 47 y 48 (proyecto de artículo 2) y 49-61 (proyecto de artículo 3);

A/CN.9/WG.IV/WP.73, párrs. 28-36; y

A/CN.9/437, párrs. 43, 48 y 92.

Observaciones

22. El proyecto de artículo que crea la presunción de que un mensaje de datos ha de considerarse como "firmado" si está autenticado por una firma electrónica segura, se ha vuelto a redactar de conformidad con una opinión expresada en el 32º período de sesiones, según la cual la relación entre la definición entre una firma electrónica segura y las presunciones dimanadas de la utilización de dicha firma electrónica segura tenían que esclarecerse (véase A/CN.9/446, párr. 34).

23. El Régimen Uniforme no contiene ninguna definición de "firma" y ninguna indicación de algún efecto jurídico específico correspondiente a dicha "firma". Con arreglo al proyecto de artículo 3, el efecto jurídico de una firma ha de determinarse por referencia a la legislación nacional aparte del Régimen Uniforme.

Artículo 4. Presunción de atribución

1) Una firma electrónica [segura] [refrendada] se presumirá que es la de la persona que pretende haberla consignado, o en cuyo nombre se pretenda haberla consignado,

Variante A a menos que el presunto firmante establezca que la firma electrónica [segura] [refrendada] se consignó sin su autorización.

Variante B a menos que la parte que se fía de la firma establezca que el procedimiento de seguridad o la combinación de procedimientos de seguridad que se hayan utilizado para verificar la firma

- a) eran comercialmente razonables en las circunstancias del caso;
- b) los aplicó la parte que se fía de la firma en forma digna de confianza, y
- c) merecen la confianza de la parte que se fía de la firma razonablemente y de buena fe.

2) Lo dispuesto en el presente artículo no será aplicable a: [...]

Referencias

A/CN.9/446, párrs. 49-61 (proyecto de artículo 3);
A/CN.9/WG.IV/WP.73, párrs. 33-36;
A/CN.9/437, párrs. 118-124 (proyecto de artículo E); y
A/CN.9/WG.IV/WP.71, párrs. 64 y 65.

Observaciones

24. La variante A trata de la atribución de una firma electrónica mediante la asignación de la carga de la prueba según lo sugerido en el 32º período de sesiones del Grupo de Trabajo (véase A/CN.9/446, párr. 60). La variante B asigna la carga de la prueba a la parte que se fía de la firma.

Artículo 5. Presunción de integridad

1) Si el presunto firmante ha utilizado un procedimiento de seguridad que puede brindar la prueba [fiable] de que un mensaje de datos o una firma [electrónica] [electrónica [segura] [refrendada]] consignada en él no ha sido modificado desde el momento en que el procedimiento de seguridad se aplicó al mensaje de datos o a la firma, entonces se presumirá [en ausencia de toda prueba de lo contrario,] que el mensaje de datos o la firma no han sido modificados.

2) Lo dispuesto en el presente artículo no será aplicable a: [...].

Referencias

A/CN.9/446, párrs. 47 y 48 (proyecto de artículo 2);
A/CN.9/WG.IV/WP.73, párrs. 28-32; y
A/CN.9/437, párrs. 43, 48 y 92.

Observaciones

25. El anterior proyecto de Régimen Uniforme se refería a la verificación de la integridad del mensaje de datos como elemento de la definición de "firma electrónica segura". Se ha indicado a la atención de la Secretaría que la verificación de la integridad del mensaje de datos podía llevarse a cabo mediante procedimientos separados. Además, cabe pensar que algunas técnicas de autenticación conseguirían el alto nivel de seguridad requerido en la definición de firmas electrónicas "refrendadas" sin necesidad de verificar la integridad del mensaje de datos.

26. Si el Grupo de Trabajo lo considera más apropiado, las disposiciones de los proyectos de artículos 3, 4 y 5 se pueden redactar de nuevo para establecer efectos jurídicos en vez de presunciones.

Artículo 6. Predeterminación de la firma electrónica [segura] [refrendada]

- 1) Un procedimiento de seguridad o una combinación de procedimientos de seguridad satisfará los requisitos que se exigen de una firma electrónica [segura] [refrendada] si así lo declara ... [el órgano o la autoridad que haya designado el Estado promulgador como competente para formular esa declaración ...].
- 2) Entre la persona que firme un mensaje de datos y cualquier otra persona que se fíe del mensaje firmado, se considerará que un procedimiento de seguridad o una combinación de procedimientos de seguridad cumplen los requisitos de una firma electrónica [segura] [refrendada] si así lo acuerdan expresamente las partes.
- 3) Lo dispuesto en el párrafo 2) no será aplicable a: [...].

Referencias

A/CN.9/446, párrs. 37-45 (proyecto de artículo 1); y
A/CN.9/WG.IV/WP.73, párr. 27.

Observaciones

27. Al contrario que las "firmas electrónicas" no cualificadas de que se trata en el proyecto de artículo 2, las firmas electrónicas [seguras] [refrendadas] previstas en el proyecto de artículo 6 ofrecen la ventaja de que, sea mediante el cumplimiento de las normas aplicables, sea mediante contrato, las partes comerciales pueden estar ciertas de los efectos jurídicos de una técnica determinada de firma antes de utilizar dicha técnica. El Grupo de Trabajo quizá desee examinar si las limitaciones de la autonomía de la voluntad de las partes a ese respecto se debe tratar en el Régimen Uniforme o si se debe dejar sencillamente que la legislación nacional se ocupe de la cuestión con arreglo al párrafo 3) (véase el párr. 14 supra).

Artículo 7. Responsabilidad respecto de la firma electrónica [segura] [refrendada]

Variante A

Cuando la firma electrónica [segura] [refrendada] no haya sido autorizada y el supuesto firmante no haya ejercido una diligencia razonable para evitar la utilización no autorizada de su firma y para impedir que el destinatario confíe en ella, el supuesto firmante será responsable [de pagar daños y perjuicios para compensar a la parte que se fió de la firma] de los daños causados, a menos que la parte confiante supiera o hubiera debido saber que la firma no era la del supuesto firmante.

Variante B

Cuando la firma electrónica [segura] [refrendada] no haya sido autorizada y el supuesto firmante no haya ejercido una diligencia razonable para impedir la utilización no autorizada de su firma y para evitar que el destinatario confíe en ella, se considerará que la firma es la del supuesto firmante a menos que la parte confiante supiera o hubiera debido saber que la firma no era la del supuesto firmante.

Referencias

- A/CN.9/446, párrs. 49-61 (proyecto de artículo 3);
A/CN.9/WG.IV/WP.73, párrs. 33-36;
A/CN.9/437, párrs. 118-124 (proyecto de artículo E); y
A/CN.9/WG.IV/WP.71, párrs. 64 y 65.

Observaciones

28. En su 32º período de sesiones, el Grupo de Trabajo deliberó sobre si el Régimen Uniforme debía tratar únicamente de la atribución de firmas electrónicas seguras (o de firmas numéricas) o si debía ocuparse también de la cuestión de la responsabilidad del supuesto firmante respecto de las partes que se fían de la firma. Se recalcó que, al establecer el vínculo entre la firma electrónica y el supuesto firmante, el Régimen Uniforme debía crear también un incentivo para la utilización de firmas numéricas atribuyendo apropiadamente la responsabilidad por las pérdidas originadas a la parte confiante debido a que el supuesto firmante no ejerció una diligencia razonable ni evitó la utilización no autorizada de su firma (véase A/CN.9/446, párr. 51).

29. El Grupo de Trabajo quizá desee examinar el vínculo entre el Régimen Uniforme y el artículo 13 de la Ley Modelo. Mientras que el artículo 13 de la Ley Modelo trata de la atribución del mensaje de datos, la cuestión de la atribución de una firma electrónica se trata en la definición de "firma electrónica [segura] [refrendada]" y en el proyecto de artículo 4.

30. La variante A limita la responsabilidad del supuesto firmante a los daños probados por la parte que se fía de la firma, que se pueden estimar sobre una base contractual o según los daños sufridos, según las circunstancias. La variante B estipula que el supuesto firmante es responsable del contenido del mensaje de datos.

Sección III. Firmas numéricas respaldadas por certificados

Artículo 8. Contenido del certificado [seguro] [refrendado]

Para los fines del presente Régimen Uniforme, un certificado [seguro] [refrendado], por lo menos:

- a) identificará la autoridad certificadora que lo emita;
- b) nombrará o identificará al [firmante] [titular del certificado] o un dispositivo o agente electrónico bajo control [del firmante] [del titular del certificado] [de esa persona];
- c) contendrá una clave pública que corresponda a una clave privada del [firmante] [titular del certificado];
- d) especificará el período de vigencia del certificado;

- e) estará firmado numéricamente o, en otro caso, estará asegurado por la autoridad certificadora que lo emita;
- [f] especificará las restricciones, si las hubiere, respecto del ámbito de utilización de la clave pública;]
[y]
- [g] identificará el algoritmo que haya de aplicarse].

Referencias

- A/CN.9/446, párrs. 113-131 (proyecto de artículo 8);
A/CN.9/WG.IV/WP.73, párrs. 50-57;
- A/CN.9/437, párrs. 98-113 (proyecto de artículo C); y
A/CN.9/WG.IV/WP.71, párrs. 18-45 y 59 y 60.

Observaciones

31. En su 32º período de sesiones el Grupo de Trabajo no decidió si, como cuestión de redacción, el Régimen Uniforme debía referirse al "titular del certificado" o indicar específicamente que el titular debería ser una "persona". Con miras a facilitar la comprensión del texto del Régimen Uniforme, se ha utilizado sistemáticamente el término "firmante", mientras que la palabra "titular" se ha mantenido también a efectos de comparación. Aunque el Régimen Uniforme puede acomodar una referencia a la noción de "persona", se necesitaría una nueva y extensa labor de redacción para evitar toda ambigüedad en cuanto a la persona que se quiere incluir. La definición de "firmante" en el proyecto de inciso h) del artículo 1 indica que el firmante ha de ser una "persona".

Artículo 9. Efectos de las firmas numéricas respaldadas por certificados

- 1) Por lo que se refiere a la totalidad o a parte de un mensaje de datos, cuando el iniciador esté identificado por una firma numérica, se considera que la firma numérica [es una firma electrónica [segura] [refrendada]] [satisface las condiciones del artículo 7 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico] si:
 - a) la firma numérica fue creada con seguridad durante el período de vigencia de un certificado válido y ha sido verificada con seguridad por referencia a la clave pública enunciada en el certificado; y
 - b) el certificado vincula una clave pública con la identidad [de una persona] [del firmante] debido a que:
 - i) el certificado fue emitido por una autoridad certificadora licenciada por ... [el Estado promulgante especifica el órgano o la autoridad competente para licenciar a las autoridades certificadoras y promulgar reglamentos para el funcionamiento de las autoridades certificadoras licenciados]; o
 - ii) el certificado fue emitido por una autoridad certificadora acreditada por un órgano responsable de la acreditación que aplique normas comercialmente apropiadas e internacionalmente reconocidas relativas a la fiabilidad de la tecnología, las prácticas y otras características pertinentes de la autoridad certificadora. Una lista no exclusiva de órganos o normas que cumplen con lo dispuesto en el presente párrafo podrá ser publicada por ... [el Estado promulgante especifica el

órgano o la autoridad competente para establecer normas reconocidas sobre el funcionamiento de las autoridades certificadoras licenciadas]; o

iii) el certificado fue de alguna otra manera emitido de conformidad con normas comercialmente apropiadas e internacionalmente reconocidas [...] [; o]

[iv) hay pruebas suficientes que indiquen que el certificado vincula [con exactitud] la clave pública con la identidad [del titular] [del firmante.]]

[2) Si un mensaje de datos está firmado con una firma numérica [creada durante el período de vigencia de un certificado] que no satisface los requisitos contenidos en el párrafo 1), la firma numérica se considerará como firma electrónica [segura] [refrendada] si hay pruebas suficientes que indiquen que [el certificado] vincula con exactitud la clave pública con la identidad del [firmante] [titular del certificado].]

3) Lo dispuesto en el presente artículo no será aplicable a: [...].

Referencias

A/CN.9/446, párrs. 71-84 (proyecto de artículo 5);
A/CN.9/WG.IV/WP.73, párrs. 39-44; y
A/CN.9/437, párrs. 43, 48 y 92.

Observaciones

32. Las palabras iniciales del párrafo 1) reflejan la decisión adoptada por el Grupo de Trabajo en su 32º período de sesiones (véase A/CN.9/446, párr. 76).

33. Si se consignan debidamente, las firmas numéricas deben constituir firmas electrónicas seguras. Ahora bien, una cosa es determinar si una firma numérica se ha consignado de forma que pueda establecer su condición de firma segura. No todas las firmas numéricas verificables por referencia a un certificado son firmas seguras, especialmente cuando hay incertidumbre acerca de si la identificación o autenticación del firmante o la clave pública son exactas. Los factores primarios que determinan si una firma numérica es segura son los siguientes: 1) si la autoridad certificadora ha identificado correctamente al firmante; 2) si la autoridad certificadora ha autenticado correctamente la clave pública del firmante; 3) si la clave privada del firmante se ha visto expuesta; y 4) si el proceso es fidedigno (por ejemplo, si el algoritmo de la clave pública y la longitud de la clave utilizada son apropiados).

34. El párrafo 1) enuncia dos criterios básicos para determinar si una firma numérica se justifica como firma electrónica segura. El primero requiere que la firma se cree durante el período de vigencia de un certificado válido y haya sido verificada con referencia a la clave pública enunciada en el certificado. El período de vigencia del certificado comienza normalmente en el momento de su emisión y termina en cuanto se produce su expiración, su revocación o su suspensión.

35. El segundo paso entraña que se tenga la seguridad de que el propio certificado identifica correctamente a una persona como firmante en relación con una clave privada correspondiente a la clave pública especificada en el certificado. La fiabilidad del certificado puede evaluarse con referencia a las normas, los procedimientos y demás requisitos establecidos por las autoridades reconocidas del Estado promulgante. Esas normas pueden probarse mediante la acreditación de las autoridades certificadoras por terceros o la licencia voluntaria de las autoridades certificadoras o requerir de algún otro modo el cumplimiento de las reglas adoptadas por el Estado promulgante.

36. Otra posibilidad es que, conforme al párrafo 2), cuando un tribunal u otra autoridad encargada de averiguar los hechos determina, como hecho probado, que la información contenida en el certificado es en efecto verdadera, la fiabilidad del certificado resulte obvia. Ahora bien, en esta etapa esa autoridad tendrá que determinar caso por caso si el certificado fue emitido por una autoridad certificadora que identificó al titular y autenticó su clave pública correctamente.

37. Consecuente con el "criterio dual" adoptado por el Grupo de Trabajo, el proyecto de artículo 9 tiene por finalidad ofrecer la máxima latitud posible para hacer la determinación de la fiabilidad de un certificado emitido por una autoridad certificadora. Esta flexibilidad es de particular importancia en vista de que la utilización de firmas numéricas es una novedad y de que los modelos para su uso, así como su reglamentación, no han sido aún plenamente desarrollados. Importa, por consiguiente, facilitar una utilización cada vez mayor de las firmas numéricas en el comercio electrónico, estableciendo al mismo tiempo las normas necesarias para efectuar una determinación presunta de la fiabilidad de un mensaje firmado numéricamente.

38. Es importante también observar que, mientras una de las opciones expuestas en el proyecto de artículo 9 entraña una determinación judicial de la exactitud del certificado, la otra opción da por supuesta esa exactitud cuando el certificado fue emitido por una autoridad certificadora acreditada por el Estado promulgante o cuando de algún otro modo satisface ciertas normas establecidas por dicho Estado. En ese caso, no se precisa una conclusión judicial de exactitud para merecer la condición de firma electrónica segura. La segunda opción puede ser útil a las personas que se dedican al comercio electrónico que deseen saber, antes de actuar confiando en una comunicación, si la acción consiguiente goza de ejecutoriedad. Sin embargo, la presunción de exactitud puede ser destruida demostrando que un certificado emitido por esa autoridad certificadora no es, en realidad, ni exacto ni fidedigno (véase A/CN.9/WG.IV/WP.73, párrs. 39-44).

CAPÍTULO III. AUTORIDADES CERTIFICADORAS Y CUESTIONES CONEXAS

Artículo 10. Declaración al emitir un certificado

- 1) Al emitir un certificado, la autoridad certificadora declara [a toda persona que razonablemente se fie de él] que:
 - a) la autoridad certificadora ha cumplido todos los requisitos aplicables [del presente Régimen];
 - b) toda la información que figura en el certificado es exacta en la fecha en que se emitió, [a menos que la autoridad certificadora haya declarado en el certificado que la exactitud de la información especificada no ha sido confirmada];
 - c) por lo que le consta a la autoridad certificadora, no hay hechos materiales conocidos que se hayan omitido del certificado y que podrían perjudicar la fiabilidad de la información que figura en el certificado; y
 - [d) si la autoridad certificadora ha publicado una declaración sobre prácticas de certificación, el certificado ha sido emitido por la autoridad certificadora de conformidad con dicha declaración sobre prácticas de certificación.]
- 2) Al emitir un certificado [seguro] [refrendado], la autoridad certificadora formula las siguientes declaraciones adicionales respecto del [firmante] [titular] identificado en el certificado [a toda persona que razonablemente se fie del certificado]:

- a) que la clave pública y la clave privada del [firmante] [titular] identificado en el certificado funcionan a modo de juego conjunto; y
- b) que en el momento de emitir el certificado, la clave privada es:
 - i) la del [firmante] [titular] identificado en el certificado; y
 - ii) corresponde a la clave pública indicada en el certificado.

Referencias

A/CN.9/446, párrs. 134-145 (proyecto de artículo 10);
A/CN.9/WG.IV/WP.73, párrs. 61-63;
A/CN.9/437, párrs. 51-73 (proyecto de artículo H); y
A/CN.9/WG.IV/WP.71, párrs. 70-72.

Observaciones

39. El proyecto de artículo 10 se basa en una distinción entre certificados [seguros] [refrendados] y una categoría más amplia de certificados. Según la decisión que adopte el Grupo de Trabajo acerca de la medida en que el Régimen Uniforme debe tratar de las firmas numéricas que se utilicen para fines diferentes del establecimiento de una equivalencia predeterminada respecto de firmas manuscritas, quizá no sea necesaria esa distinción (véase el párrafo 20 supra).

Artículo 11. Responsabilidad contractual

Variante A

1) Entre una autoridad certificadora que emite un certificado y el titular de ese certificado [o toda otra parte que se fie de la firma y esté ligada con la autoridad certificadora por una relación contractual], los derechos y las obligaciones de las partes [y sus eventuales limitaciones] quedarán determinados por el acuerdo celebrado entre las partes [sujeto a la ley aplicable].

[2) Sin perjuicio de lo dispuesto en el artículo 10, la autoridad certificadora podrá, mediante acuerdo, eximirse de la responsabilidad por cualquier pérdida [producida por la confianza en el certificado] [causada por defectos en la información indicada en el certificado, averías técnicas o circunstancias análogas. No obstante, la cláusula que limite o excluya la responsabilidad de la autoridad certificadora no podrá ser invocada cuando la exclusión o la limitación de la responsabilidad contractual falte gravemente a la equidad, habida cuenta de la finalidad del contrato].]

[3) La autoridad certificadora no estará facultada para limitar su responsabilidad cuando se pruebe que la pérdida fue consecuencia de un acto o una omisión de esa autoridad certificadora con la intención de causar un daño o de forma temeraria y con conocimiento de que probablemente se ocasionaría un daño.]

Variante B

De conformidad con la ley aplicable, los derechos y las obligaciones de una autoridad certificadora, de un [firmante] [titular] identificado en el certificado, y de cualquier otra parte se regirán por el acuerdo o los acuerdos celebrados entre esas partes en la medida en que el acuerdo o los acuerdos traten de esos derechos y obligaciones y de sus eventuales limitaciones.

Variante C

Cuando haya celebrado acuerdos la autoridad certificadora, un [firmante] [titular] identificado en un certificado, o cualquier otra parte, los derechos y las obligaciones de esas partes y sus eventuales limitaciones de que se trate en los acuerdos, se registrarán por los acuerdos de conformidad con la ley aplicable y en la medida en que dicha ley lo permita.

Referencias

A/CN.9/446, párrs. 146-154 (proyecto de artículo 11);

A/CN.9/WG.IV/WP.73, párrs. 64 y 65;

A/CN.9/437, párrs. 51-73 (proyecto de artículo H); y

A/CN.9/WG.IV/WP.71, párrs. 70-72.

Observaciones

40. Antes de examinar las variantes propuestas para el texto del proyecto de artículo 11, el Grupo de Trabajo quizá desee examinar la cuestión de si debía mantenerse en el Régimen Uniforme el proyecto de artículo 11. En el 32º período de sesiones del Grupo de Trabajo se declaró que el proyecto de artículo trataba de cuestiones que sería más adecuado que estuvieran reguladas por el contrato y la ley aplicable. En particular, se observó que quizá no fuera necesario reiterar el principio de la autonomía de la voluntad de las partes, del que ya se había tratado en el artículo 4 de la Ley Modelo; y que otras cuestiones de que se trataba en el proyecto de artículo interferían con la ley nacional en asuntos tal vez no susceptibles de unificación. Si bien se estimó que era una opción aceptable dejar que la responsabilidad contractual se rigiera por el contrato y por la ley aplicable fuera del ámbito del Régimen Uniforme, prevaleció el criterio de que merecía la pena intentar lograr cierto grado de unificación en esta importante cuestión (véase A/CN.9/446, párr. 148).

Artículo 12. Responsabilidad de la entidad certificadora frente a las partes que se fían de los certificados

1) A reserva de lo dispuesto en el párrafo 2), cuando una autoridad certificadora emita un certificado se la tendrá por responsable ante toda persona que razonablemente se fíe del certificado por:

a) los errores en el certificado, salvo que una autoridad certificadora demuestre que ella o sus representantes adoptaron [todas] las medidas [razonables] [comercialmente razonables] [que eran procedentes para la finalidad para la que se emitió el certificado, a la luz de todas las circunstancias] para evitar errores en el certificado;

b) no haber registrado la revocación del certificado, salvo que la autoridad certificadora demuestre que ella o sus representantes adoptaron [todas] las medidas [razonables] [comercialmente razonables] [que eran procedentes para la finalidad para la que se emitió el certificado, a la luz de todas las circunstancias] para registrar prontamente la revocación al serles notificada la revocación [; y

c) las consecuencias de no aplicar:

i) un procedimiento enunciado en la declaración sobre prácticas de certificación publicada por la autoridad certificadora; o

ii) un procedimiento enunciado en la ley aplicable].

2) La confianza en un certificado no será razonable en la medida en que sea contraria a la información contenida [o incorporada por remisión] en el certificado [o en una lista de revocación] [o en la información sobre la revocación]. [La confianza no será razonable, en particular, cuando:

- a) sea contraria a la finalidad para la que se emitió el certificado;
- b) exceda del valor para el que es válido el certificado; o
- c) [...].]

Referencias

A/CN.9/446, párrs. 155-173 (proyecto de artículo 12);
A/CN.9/WG.IV/WP.73, párrs. 66 y 67;
A/CN.9/437, párrs. 51-73 (proyecto de artículo H); y
A/CN.9/WG.IV/WP.71, párrs. 70-72.

Observaciones

41. El proyecto de artículo 12 refleja la decisión adoptada por el Grupo de Trabajo en su 32º período de sesiones (A/CN.9/446, párr. 173). En ese período de sesiones se expresó la opinión de que el proyecto de artículo 12 sólo debía aplicarse a las autoridades certificadoras que emitiesen certificados de identificación.

Observación general relativa a los proyectos de artículos 13 a 16

42. En su anterior período de sesiones, por falta de tiempo el Grupo de Trabajo decidió aplazar su examen de los proyectos de artículos 13 a 16 hasta un futuro período de sesiones (véase A/CN.9/446, párr. 174). Salvo cambios editoriales, encaminados principalmente a lograr la compatibilidad de las diversas disposiciones incluidas en el texto revisado del Régimen Uniforme, el texto de los proyectos de artículos 13 a 16 del presente documento es sustancialmente idéntico al texto de esos artículos que figura en el documento A/CN.9/WG.IV/WP.73.

Artículo 13. Revocación de certificados

- 1) Durante el período de vigencia de un certificado, la autoridad certificadora que emitió el certificado deberá revocarlo de conformidad con las políticas y los procedimientos que rijan la revocación especificados en la declaración sobre prácticas de certificación aplicable o, a falta de tales políticas y procedimientos, prontamente al:
 - a) recibir una solicitud de revocación del [firmante] [titular] identificado en el certificado y confirmación de que la persona que solicita la revocación es el [legítimo] [firmante] [titular], o es un mandatario del [firmante] [titular] facultado para solicitar la revocación;
 - b) recibir pruebas fidedignas del fallecimiento del [firmante] [titular] si el [firmante] [titular] es una persona física; o
 - c) recibir pruebas fidedignas de que el [firmante] [titular] ha sido disuelto o ha dejado de existir, si el [firmante] [titular] es una persona jurídica.

2) El [firmante] [titular] de un juego de claves certificado estará obligado a hacer revocar, o a pedir que se revoque, el certificado correspondiente si llega a conocimiento del [firmante] [titular] que la clave privada se ha perdido, o corre peligro o está expuesta a ser de algún modo indebidamente utilizada. El [firmante] [titular] que, llegada esa situación, no haga revocar, o no pida que se revoque, el certificado será responsable respecto de cualquier persona que se haya fiado del contenido de un mensaje por no haber cumplido el [firmante] [titular] con su obligación de revocar el certificado.

3) Independientemente de que el [firmante] [titular] identificado en el certificado consienta en la revocación, la autoridad certificadora que emitió un certificado deberá revocar el certificado prontamente al tener conocimiento de que:

- a) un hecho material indicado en el certificado es falso;
- b) la clave privada de la autoridad certificadora o su sistema de información estuvo expuesto de manera que afectaba a la fiabilidad del certificado; o
- c) la clave privada o el sistema de información del [firmante] [titular] estuvo expuesto.

3) Al efectuar la revocación de un certificado conforme a lo dispuesto en el párrafo 3), la autoridad certificadora deberá notificar al [firmante] [titular] y a las partes que se fian del certificado de conformidad con las políticas y los procedimientos que rijan la notificación de revocación especificada en la declaración sobre prácticas de certificación aplicable o, a falta de tales políticas y procedimientos, deberá notificar prontamente al [firmante] [titular] y publicar prontamente un aviso de la revocación si el certificado se publicó, y, en general, revelar el hecho de la revocación a la parte que se fió del certificado que consulte al respecto.

4) [Entre el [firmante] [titular] y la autoridad certificadora,] la revocación será efectiva desde el momento en que sea [recibida] [registrada] por la autoridad certificadora.

[5) Entre la autoridad certificadora y toda otra parte que se fie del certificado, la revocación será efectiva desde el momento en que sea [registrada] [publicada] por la autoridad certificadora.]

Referencias

- A/CN.9/446, párr. 174 (proyecto de artículo 13);
A/CN.9/WG.IV/WP.73, párr. 68;
A/CN.9/437, párrs. 125-139 (proyecto de artículo F); y
A/CN.9/WG.IV/WP.71, párrs. 66 y 67.

Observaciones

43. El proyecto de artículo 13 tiene por objeto reflejar las diversas opiniones expresadas en el 31º período de sesiones del Grupo de Trabajo, estipulando una norma supletoria que rija la revocación de certificados. No obstante, en cualquier momento una autoridad certificadora puede evitar la norma supletoria estableciendo procedimientos aplicables a la revocación en su declaración sobre prácticas de certificación y ateniéndose a esos procedimientos. En cuanto al momento en que la revocación sea efectiva, el Grupo de Trabajo tal vez desee decidir si hay que establecer una distinción entre la situación del firmante y la de las demás partes que se fian del certificado (véase A/CN.9/437, párr. 130).

Artículo 14. Suspensión de certificados

Durante el período de vigencia de un certificado, la autoridad certificadora que lo emitió deberá suspenderlo de conformidad con las políticas y los procedimientos que rijan la suspensión especificados en la declaración sobre prácticas de certificación aplicable o, a falta de tales políticas y procedimientos, prontamente al recibir una solicitud en ese sentido de una persona que la autoridad certificadora crea razonablemente que es el [firmante] [titular] indicado en el certificado o una persona autorizada para actuar en nombre de ese [firmante] [titular].

Referencias

A/CN.9/446, párr. 174 (proyecto de artículo 14);
A/CN.9/WG.IV/WP.73, párr. 69; y
A/CN.9/437, párrs. 133-135 (proyecto de artículo F)

Observaciones

44. En su 31º período de sesiones, el Grupo de Trabajo decidió que el Régimen Uniforme contuviera una disposición sobre suspensión de certificados (véase A/CN.9/437, párrs. 133 y 134). En cuanto al momento de la efectividad de la suspensión, el Grupo de Trabajo quizá quiera decidir si hay que añadir disposiciones análogas a los párrafos 4) y 5) del proyecto de artículo 13.

Artículo 15. Registro de certificados

1) Toda autoridad certificadora deberá llevar un registro electrónico de certificados emitidos, al que tenga acceso el público, que indique la fecha de expiración de cada certificado o la fecha en que fue suspendido o revocado.

2) La autoridad certificadora deberá conservar esa inscripción en su registro

Variante A por lo menos durante [30] [10] [5] años.

Variante B durante ... [el Estado promulgante especifica el plazo durante el cual debe mantenerse en el registro la información pertinente]

siguientes a la fecha de revocación o de expiración del período de vigencia de todo certificado emitido por esa autoridad certificadora.

Variante C de conformidad con las políticas y los procedimientos especificados por la autoridad certificadora en la declaración sobre prácticas de certificación aplicable.

Referencias

A/CN.9/446, párr. 174 (proyecto de artículo 15);
A/CN.9/WG.IV/WP.73, párrs. 70 y 71;
A/CN.9/437, párrs. 140-148 (proyecto de artículo G); y
A/CN.9/WG.IV/WP.71, párrs. 68 y 69.

Observaciones

45. En el 31º período de sesiones del Grupo de Trabajo no se planteó ninguna objeción de principio contra la inclusión en el Régimen Uniforme de una disposición sobre el registro de certificados (véase A/CN.9/437, párr. 142). Cabe considerar el correcto mantenimiento de un registro ampliamente accesible (denominado a veces "depósito") que comprenda, en particular, una lista de revocaciones de certificados (LRC), como importante elemento para comprobar la fiabilidad de las firmas numéricas. Al estudiar de qué manera las autoridades certificadoras deberían llevar esos registros y LRC, el Grupo de Trabajo tal vez desee examinar si las partes que se fían del certificado han de estar obligadas a verificar la situación del certificado consultando el registro o la LRC pertinentes antes de poderse fiar de la validez del certificado.

46. En términos más generales, el Grupo de Trabajo posiblemente quiera examinar si el Régimen Uniforme, al establecer normas mínimas para el funcionamiento de las autoridades certificadoras, tendría que ocuparse además de los derechos y las obligaciones de las partes que se fían de los certificados.

Artículo 16. Relaciones entre las partes que se fían de los certificados
y las autoridades certificadoras

- [1] La autoridad certificadora sólo podrá pedir los datos que necesite para identificar al [firmante] [titular del certificado].
- 2) Cuando se pida, la autoridad 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 autoridad 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) los requisitos técnicos de la autoridad certificadora con relación al equipo de comunicaciones que han de utilizar las partes que se fían de los certificados;
 - f) las condiciones en que la autoridad certificadora envía advertencias a las partes que se fían de los certificados en caso de irregularidades o defectos de funcionamiento del equipo de comunicaciones;
 - g) toda limitación de la responsabilidad de la autoridad certificadora;
 - h) toda restricción impuesta por la autoridad certificadora respecto de la utilización del certificado;
y
 - i) las condiciones en las que el [firmante] [titular] tiene derecho a imponer restricciones respecto de la utilización del certificado.
- 3) La información indicada en el párrafo 1) se entregará al [posible] [firmante] [titular] antes de la concertación de un acuerdo final de certificación. Esta información podrá ser entregada por la autoridad certificadora en forma de declaración sobre prácticas de certificación.

- 4) Con un preaviso [de un mes], el [firmante] [titular] podrá dar por terminado el acuerdo de vinculación con la autoridad certificadora. Este 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. Este preaviso surtirá efecto desde el momento de su recepción.]

Referencias

A/CN.9/446, párr. 174 (proyecto de artículo 16);
A/CN.9/WG.IV/WP.73, párr. 72;
A/CN.9/437, párrs. 149 y 150 (proyecto de artículo J); y
A/CN.9/WG.IV/WP.71, párr. 76.

Observaciones

47. En su 31º período de sesiones, el Grupo de Trabajo observó que los diversos elementos enumerados en el proyecto de artículo 15 debían ponerse entre corchetes, para que el Grupo de Trabajo los examinara en una etapa posterior (véase A/CN.9/437, párr. 150).

CAPÍTULO IV. FIRMAS ELECTRÓNICAS EXTRANJERAS

Artículo 17. Prestación de servicios por autoridades certificadoras extranjeras

- 1) Variante A Las [personas] [entidades] extranjeras podrán establecerse como autoridades certificadoras locales o prestar servicios de certificación desde otro país sin un establecimiento local si satisfacen las mismas normas objetivas [y aplican los mismos procedimientos] que las entidades y personas nacionales que puedan convertirse en autoridades certificadoras.

Variante B A reserva de lo dispuesto en las leyes del Estado promulgante, las [personas] [entidades] extranjeras podrán:

- a) establecerse como autoridades certificadoras locales; o
- b) prestar servicios de certificación sin un establecimiento local si satisfacen las mismas normas objetivas y aplican los mismos procedimientos que las entidades y personas nacionales que puedan convertirse en autoridades certificadoras.

Variante C No se negará a las [personas] [entidades] extranjeras el derecho a establecerse localmente o a prestar servicios de certificación únicamente por el sólo hecho de que sean extranjeras si satisfacen las mismas normas objetivas [y aplican los mismos procedimientos] que las entidades o personas nacionales que puedan convertirse en autoridades certificadoras

- [2) Variante X La norma formulada en el párrafo 1) no será aplicable a: [...].

Variante Y Podrán hacerse excepciones a la norma formulada en el párrafo 1) en la medida en que lo requiera la seguridad nacional.]

Referencias

A/CN.9/446, párr. 175-188 (proyecto de artículo 17);
A/CN.9/WG.IV/WP.73, párr. 73;
A/CN.9/437, párrs. 74-89 (proyecto de artículo I); y
A/CN.9/WG.IV/WP.71, párrs. 73-75.

Observaciones

48. Al permitir que entidades extranjeras puedan establecerse como autoridades certificadoras, el proyecto de artículo 17 afirma el principio de que no se debe discriminar contra las entidades extranjeras si satisfacen las mismas normas que las autoridades certificadoras nacionales. Aunque este principio pueda ser generalmente aceptado, tal vez sea particularmente pertinente expresarlo con respecto a las autoridades certificadoras, ya que cabe esperar que éstas funcionen sin tener necesariamente un establecimiento u otra presencia física en el país en el que operen.

Artículo 18. Homologación de certificados extranjeros por autoridades certificadoras nacionales

Variante A Los certificados emitidos por autoridades certificadoras extranjeras podrán ser utilizados para los fines de una firma numérica en las mismas condiciones que los certificados sujetos al presente Régimen, de ser reconocidos por una autoridad certificadora que funcione conforme a ... [la ley del Estado promulgante], y de garantizar esta autoridad, en la misma medida que respecto de sus propios certificados, la regularidad de los detalles del certificado, así como su validez y vigencia.

Variante B Los certificados emitidos por autoridades certificadoras extranjeras podrán ser utilizados para los fines de una firma numérica en las mismas condiciones que los certificados sujetos al presente Régimen siempre que exista la correspondiente garantía emitida por una autoridad certificadora que funcione conforme a ... [la ley del Estado promulgante].

Referencias

A/CN.9/446, párrs. 189-195 (proyecto de artículo 18);
A/CN.9/WG.IV/WP.73, párr. 74;
A/CN.9/437, párrs. 74-89 (proyecto de artículo I); y
A/CN.9/WG.IV/WP.71, párrs. 73-75.

Observaciones

49. El proyecto de artículo 18 habilita a las autoridades certificadoras nacionales para garantizar, en la misma medida que respecto de sus propios certificados, la regularidad de los detalles del certificado extranjero, y para garantizar que el certificado extranjero tiene validez y vigencia. Se refiere a los asuntos denominados "certificación recíproca" en el 31º período de sesiones del Grupo de Trabajo. El proyecto de artículo 18 contiene en sustancia una disposición sobre la asignación de la responsabilidad a la autoridad certificadora nacional en caso de que el certificado extranjero resulte defectuoso (véase A/CN.9/437, párrs. 77 y 78).

Artículo 19. Reconocimiento de certificados extranjeros

Variante A

- 1) Variante X No podrá privarse a los certificados emitidos por autoridades certificadoras extranjeras del mismo reconocimiento que los certificados emitidos por autoridades certificadoras nacionales en razón de haber sido emitidos por autoridades certificadoras extranjeras.

Variante Y Los certificados emitidos por una autoridad certificadora extranjera se reconocerán como jurídicamente equivalentes a los emitidos por las autoridades certificadoras que funcionen conforme a ... [la ley del Estado promulgante] cuando las prácticas de la autoridad certificadora extranjera ofrezcan un grado de fiabilidad por lo menos equivalente al requerido por las autoridades certificadoras de conformidad con el presente Régimen. [Este reconocimiento podrá hacerse mediante una determinación publicada del Estado o mediante un acuerdo bilateral o multilateral entre los Estados interesados.]

2) Las firmas y las constancias que cumplan con las leyes de otro Estado relativas a las firmas numéricas u otras firmas electrónicas se reconocerán como jurídicamente equivalentes a las firmas y constancias que cumplen con el presente Régimen cuando las leyes del otro Estado requieran un grado de fiabilidad por lo menos equivalente al requerido para esas constancias y firmas conforme a ... [la ley del Estado promulgante]. [Este reconocimiento podrá hacerse mediante una determinación publicada del Estado o mediante un acuerdo bilateral o multilateral con otros Estados.]

2)[3] Las firmas numéricas verificadas con referencia a un certificado emitido por una autoridad certificadora extranjera [tendrán] [no serán privadas de tener] eficacia [por parte de los tribunales y otras autoridades encargadas de averiguar los hechos] cuando el certificado sea tan fiable como corresponda a la finalidad para la cual se emitió, a la luz de todas las circunstancias.

3)[4] Sin perjuicio de lo dispuesto en el párrafo anterior, los órganos públicos y las partes en transacciones comerciales y de otro tipo podrán hacer constar que se debe utilizar una determinada autoridad certificadora, clase de autoridades certificadoras o clase de certificados en relación con los mensajes o las firmas presentados a esos órganos.

Variante B

1) Los certificados emitidos por una autoridad certificadora extranjera se reconocerán como jurídicamente equivalentes a los certificados emitidos por las autoridades certificadoras que funcionen conforme a ... [la ley del Estado promulgante] cuando las prácticas de la autoridad certificadora extranjera ofrezcan un grado de fiabilidad por lo menos equivalente al requerido de las autoridades certificadoras de conformidad con el presente Régimen.

[2) La determinación de la equivalencia descrita en el párrafo 1) podrá hacerse mediante una determinación publicada del Estado o mediante un acuerdo bilateral o multilateral con otros Estados.]

3) Al determinar la equivalencia, deberán tenerse en cuenta los siguientes factores:

- a) recursos humanos y financieros, incluida la existencia de activo bajo jurisdicción;

- b) fiabilidad de los sistemas de equipo y programas informáticos;
- c) procedimientos para la tramitación de certificados y solicitudes de certificados y conservación de registros;
- d) disponibilidad de información para los [firmantes] [titulares] identificados en certificados y para posibles partes que se fien de los certificados;
- e) regularidad y detalle de la auditoría hecha por un órgano independiente;
- f) existencia de una declaración del Estado, un órgano acreditador o la autoridad certificadora acerca del cumplimiento o la existencia de lo antedicho;
- g) estatuto respecto de la jurisdicción de los tribunales del Estado promulgante; y
- h) grado de discrepancia entre la ley aplicable a la responsabilidad de la autoridad certificadora y la ley del Estado promulgante.

Variante C

Se considera que una autoridad certificadora extranjera es fiable [en el Estado promulgante] para los fines de un certificado que emita a fin de respaldar firmas en relación con mensajes de datos si, al emitir dicho certificado, la autoridad certificadora cumple con cualquier régimen nacional de concesión de licencias aplicable a un certificado de ese tipo, y está sujeta por lo menos a las mismas obligaciones que se imponen en el presente Régimen y en ese régimen nacional de concesión de licencias.

Variante D

- 1) Se considera que una autoridad certificadora extranjera es fiable [en el Estado promulgante] para los fines de un certificado que emita a fin de respaldar firmas en relación con mensajes de datos si, al emitir dicho certificado, la autoridad certificadora proporciona un grado de fiabilidad [por lo menos] equivalente al [requerido] de las autoridades certificadoras nacionales que emitan dichos certificados.
- 2) Al evaluar el grado de fiabilidad de una autoridad certificadora, deberán tenerse en cuenta los siguientes factores:
 - a) recursos humanos y financieros, incluida la existencia de activo bajo jurisdicción;
 - b) fiabilidad de los sistemas de equipo y programas informáticos;
 - c) procedimientos para la tramitación de certificados y solicitudes de certificados y conservación de registros;
 - d) disponibilidad de información para los [firmantes] [titulares] identificados en certificados y para posibles partes que se fien de los certificados;
 - e) regularidad y detalle de la auditoría hecha por un órgano independiente;
 - f) existencia de una declaración del Estado, un órgano acreditador o la autoridad certificadora acerca del cumplimiento o la existencia de lo antedicho;

g) estatuto respecto de la jurisdicción de los tribunales del Estado promulgante; y

h) grado de discrepancia entre la ley aplicable a la responsabilidad de la autoridad certificadora y la ley del Estado promulgante.

Referencias

A/CN.9/446, párrs. 196-207 (proyecto de artículo 19);

A/CN.9/WG.IV/WP.73, párr. 75;

A/CN.9/437, párrs. 74-89 (proyecto de artículo I); y

A/CN.9/WG.IV/WP.71, párrs. 73-75.

Observaciones

50. El proyecto de artículo 19 se refiere a los asuntos denominados "reconocimiento transfronterizo" en el 31º período de sesiones del Grupo de Trabajo (véase A/CN.9/437, párrs. 77 y 78). La variante A se basa en la sugerencia de combinar los párrafos 1) y 2) que se hizo en el 32º período de sesiones del Grupo de Trabajo (véase A/CN.9/446, párrs. 197-204). La variante B ofrece una lista ilustrativa de los criterios que han de tenerse en cuenta al evaluar la fiabilidad de los certificados extranjeros. Las variantes C y D se centran en el reconocimiento de las autoridades certificadoras extranjeras. Cabe observar que, si el Grupo de Trabajo decidiera incluir en el Régimen Uniforme criterios que han de satisfacer las autoridades certificadoras nacionales (véase párr. 19 supra), es posible que no sea necesario enunciar esos criterios en el proyecto de artículo 19.

Notas

¹ Documentos Oficiales de la Asamblea General, quincuagésimo primer período de sesiones, Suplemento No. 17 (A/51/17), párrs. 223 y 224.

² Ibid., quincuagésimo segundo período de sesiones, Suplemento No. 17 (A/52/17), párrs. 249-251.