



Asamblea General

Distr.
LIMITADA

A/CN.9/WG.IV/WP.73
12 de diciembre de 1997

ESPAÑOL
Original: INGLÉS

COMISIÓN DE LAS NACIONES UNIDAS PARA EL
DERECHO MERCANTIL INTERNACIONAL
Grupo de Trabajo sobre Comercio Electrónico
32º período de sesiones
Viena, 19 a 30 de enero 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	12-75	5
CAPÍTULO I. ESFERA DE APLICACIÓN Y DISPOSICIONES GENERALES	12-15	5
CAPÍTULO II. FIRMAS ELECTRÓNICAS	16-46	6
Sección I. Firmas electrónicas seguras	16-36	6
Artículo 1. Definiciones	16-27	6
Artículo 2. Presunciones	28-32	10
Artículo 3. Atribución	33-36	12

	<u>Párrafos</u>	<u>Página</u>
Sección II. Firmas numéricas	37-45	13
Artículo 4. Definición	37-38	13
Artículo 5. Efectos	39-44	15
[Artículo 6. Firma de personas jurídicas]	45	16
Sección III. Otras firmas electrónicas	46	17
CAPÍTULO III. AUTORIDADES CERTIFICADORAS Y CUESTIONES CONEXAS	47-72	17
Artículo 7. Autoridad certificadora	47-49	17
Artículo 8. Certificado	50-57	18
Artículo 9. Declaración sobre prácticas de certificación	58-60	20
Artículo 10. Declaraciones al emitir un certificado	61-63	21
Artículo 11. Responsabilidad contractual	64-65	23
Artículo 12. Responsabilidad de la autoridad certificadora frente a las partes que se fian de los certificados	66-67	24
Artículo 13. Revocación de certificados	68	26
Artículo 14. Suspensión de certificados	69	27
Artículo 15. Registro de certificados	70-71	27
Artículo 16. Relaciones entre las partes que se fian de los certificados y las autoridades certificadoras	72	28
CAPÍTULO IV. RECONOCIMIENTO DE FIRMAS ELECTRÓNICAS EXTRANJERAS	73-75	29
Artículo 17. Autoridades certificadoras extranjeras que ofrecen servicios conforme al presente Régimen	73	29
Artículo 18. Homologación de certificados extranjeros por autoridades certificadoras nacionales	74	30
Artículo 19. Reconocimiento de certificados extranjeros	75	30

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 entidades 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 entidades certificadoras y posiblemente sobre asuntos conexos. El Grupo de Trabajo recordó que, al margen de las cuestiones de las firmas numéricas y las entidades 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 entidades certificadoras (denominado en adelante "el Régimen Uniforme").

4. Con respecto a la forma y al alcance exacto 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 en lo relativo a los diversos medios técnicos disponibles. 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 entidades 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 entidades certificadoras habrían de respetar estrictamente, particularmente en casos en los que se solicitara una certificación de validez transfronteriza.

5. Como tema adicional que había de considerarse en el marco de la futura labor en materia de comercio electrónico, se sugirió que el Grupo de Trabajo tal vez necesitara examinar, en una etapa ulterior, las cuestiones de competencia jurisdiccional, ley aplicable y solución de controversias en el marco de la Internet. Se informó a la Comisión de que se había de celebrar, en junio de 1997, un coloquio sobre cuestiones de competencia jurisdiccional y ley aplicable en lo relativo a la Internet bajo el patrocinio de la Conferencia de La Haya de Derecho Internacional Privado. Se informó a la Comisión de que una conferencia internacional convocada por la Organización de Cooperación y Desarrollo Económicos, que se celebraría en noviembre de 1997, trataría de establecer un enfoque coordinado de las cuestiones del comercio electrónico entre los países interesados, las organizaciones intergubernamentales y no gubernamentales y ciertos grupos del sector privado. La Comisión expresó la esperanza de que la Secretaría asistiera a esas dos reuniones e informara al respecto².

6. La presente nota contiene proyectos de disposición revisados que pueden incluirse en el Régimen Uniforme. Estas disposiciones tratan de las firmas numéricas, otras firmas electrónicas, entidades certificadoras y cuestiones jurídicas conexas. Se prepararon de conformidad con las deliberaciones y las decisiones del Grupo de Trabajo en su 31º período de sesiones, tal como quedan reflejadas en el informe de ese período (A/CN.9/437), así como con las deliberaciones y decisiones de la comisión en su 30º período de sesiones, antes reproducidas. 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 anterior 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 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. En un plano más general, a la espera de una decisión definitiva acerca de la relación entre la Ley Modelo, el Régimen Uniforme y posibles normas de incorporación por remisión (véase A/CN.9/437, párrs. 151 a 155), los proyectos de disposición intentan ser coherentes con los principios expresados y con la terminología empleada en la Ley Modelo (A/CN.9/437, párr. 26).

7. La presente nota no se ocupa de las cuestiones de competencia, ley aplicable y solución de controversias en la Internet, la formación y el cumplimiento de los contratos en un entorno electrónico ni de ninguna otra cuestión que el Grupo de Trabajo pueda tener que abordar en un futuro período de sesiones. Se presentará un informe verbal al Grupo de Trabajo acerca del coloquio sobre cuestiones de competencia jurisdiccional y ley aplicable en lo relativo a la Internet, que se celebró en junio de 1997 con los auspicios de la Conferencia de La Haya de Derecho Internacional Privado, y la conferencia internacional convocada por la OCDE en noviembre de 1997 (véase *supra*, párr.5).

8. 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.

I. OBSERVACIONES GENERALES

9. La finalidad del Régimen Uniforme, reflejado 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 internacional privado de las operaciones comerciales, el Proyecto 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" (esto es, 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, ENTIDADES 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 habría que incorporarlas en una versión ampliada de la Ley Modelo, por ejemplo, como una nueva Parte III de la Ley Modelo.

13. Si el Régimen Uniforme se prepara como instrumento aparte o como adición a la Ley Modelo, se supone que tendrá que contener disposiciones acordes con el artículo 1 (Ámbito de aplicación), los apartados a), b) y e) del artículo 2 (Definiciones de "mensaje de datos", "iniciador" y "destinatario"), y los artículos 3 (Interpretación), 7 (Firma) y 13 (Atribución de los 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 (véase el documento A/CN.9/WG.IV/WP.71, párrs. 49 y 50).

14. En cuanto a la cuestión de la autonomía de la voluntad de las partes, no bastaría la mera referencia al artículo 4 (Modificación mediante acuerdo) para obtener una solución satisfactoria, en vista 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 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 (véase el documento A/CN.9/WG.IV/WP.71, párr. 51).

CAPÍTULO II. FIRMAS ELECTRÓNICAS

Sección I. Firmas electrónicas seguras

Artículo 1. Definiciones

Para los fines del presente Régimen:

- a) por "firma" se entenderá cualquier símbolo utilizado, o cualquier procedimiento de seguridad adoptado, por una persona [o en su nombre] con la intención de identificar a esa persona e indicar que esa persona aprueba la información a la que esa firma está adherida;
- b) por "firma electrónica" se entenderá [la firma] [los datos] en forma electrónica contenida (contenidos) en un mensaje de datos o adjunta (adjuntos) a él o lógicamente vinculada (vinculados) con él [y utilizada (utilizados) por una persona o [en su nombre] con la intención de identificar a esa persona e indicar su aprobación del contenido de ese mensaje de datos] [y utilizada (utilizados) para satisfacer las condiciones del [artículo 7 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico]];
- c) por "firma electrónica segura" se entenderá una firma electrónica que
 - i) sea una firma electrónica conforme al artículo 4 y satisfaga los requisitos contenidos en el artículo 5; o

ii) al tiempo en que se consignó, pueda verificarse como la firma de una persona determinada mediante la aplicación de un procedimiento de seguridad que esté exclusivamente vinculado con la persona que la utiliza; sea capaz de identificar pronta, objetiva y automáticamente a esa persona; haya sido creada de manera o con unos medios bajo control exclusivo de la persona que la utilice; y esté vinculada con el mensaje de datos a que se refiera de modo que, si el mensaje es alterado, quede invalidada la firma electrónica; o

iii) sea comercialmente razonable, en las circunstancias previamente acordadas, y debidamente aplicadas, por las partes [entre las partes que participen en la generación, el envío, la recepción, el archivo u otra elaboración de mensajes de datos en el curso ordinario de sus actividades].

Referencias

A/CN.9/437, párrs. 29 a 50 y 90 a 113 (proyectos de artículo A, B y C); A/CN.9/WG.IV/WP.71, párrs. 52 a 60.

Observaciones

16. El proyecto de artículo 1 tiene por fin reflejar la decisión alcanzada por el Grupo de Trabajo en su 30º período de sesiones de que, consecuentemente con la neutralidad de la Ley Modelo en lo relativo a los diversos medios técnicos disponibles, el Régimen Uniforme no debía desalentar la utilización de ninguna técnica que ofreciera un "método tan fiable como fuese apropiado" para servir de solución alternativa a las firmas manuscritas y otras firmas en un medio de documentación escrita, de conformidad con el artículo 7 de la Ley Modelo. Si bien el Régimen Uniforme podría centrarse en las cuestiones referentes a las firmas numéricas, había que adoptar también un criterio más general y cabía igualmente examinar cuestiones pertinentes a otras técnicas de firma electrónica (A/CN.9/437, párr.22).

17. Mediante una definición de "firma" y de "firma electrónica" en los apartados a) y b), queda delineado en términos generales el alcance del Régimen Uniforme de modo que abarque todas las técnicas que se pueden aplicar para obtener el equivalente funcional de una firma manuscrita, tal como se entiende en el artículo 7 de la Ley Modelo. Es preciso observar que la definición de "firma", que se limita a reiterar en forma de definición lo dispuesto en el apartado a) del párrafo 1 del artículo 7 de la Ley Modelo, no se propone sustituir ni afectar de alguna otra manera ninguna definición de "firma" o de "firma manuscrita" que pudiese existir fuera del Régimen Uniforme (por ejemplo, en la legislación o en la jurisprudencia nacionales). Esa definición tiene por fin sobre todo servir de base para las posteriores definiciones de "firma electrónica" y "firma electrónica segura". Puede así mismo ser una útil referencia en los países donde no hay actualmente definición de "firma".

18. Los tres niveles de definición del proyecto de artículo 1 (es decir, "firma", "firma electrónica" y "firma electrónica segura") obedecen al propósito de ofrecer al Grupo de Trabajo un instrumento analítico y reflejar una distinción que se ha hecho familiar en los proyectos legislativos de una serie de países. Pero, según sea el contenido del Régimen Uniforme, puede que no sean necesarias las tres definiciones. Si el Grupo de Trabajo decide concentrarse en la eficacia jurídica de las firmas electrónicas (esto es, su reconocimiento como equivalentes funcionales de las manuscritas), sólo habría que tener en cuenta una categoría de "firmas electrónicas". Las nociones actualmente definidas como "firma electrónica" y "firma electrónica segura" podrían por tanto refundirse en una sola categoría jurídica, prescindiendo del número y la variedad de las técnicas que se considerasen dentro de esa categoría.

19. La principal definición a la que hay que recurrir con el fin de delinear el ámbito de aplicación del Régimen Uniforme es la actualmente contenida en el apartado c) bajo el encabezamiento "firma electrónica segura". Desde el punto de vista de la redacción, cabe observar que la palabra "segura" no pretende indicar que alguna técnica determinada pueda, de hecho o de derecho, brindar una seguridad absoluta. Quiere sólo predicar un nivel superior de fiabilidad de una firma electrónica con referencia a un conjunto de criterios que, una vez satisfechos, acarrearían ciertas consecuencias jurídicas.

20. Junto con la intención de proporcionar una base para los efectos jurídicos que se derivarían de la utilización de firmas electrónicas, el apartado c) tiene también por fin reflejar el "criterio dual" adoptado por el Grupo de Trabajo en su anterior período de sesiones. El "criterio dual" provenía de las dos soluciones posibles debatidas, a saber, el establecimiento de criterios para la concesión de una autorización oficial a las autoridades certificadoras y el reconocimiento de criterios de actuación de las autoridades certificadoras que operasen fuera de una infraestructura de claves públicas a cargo de la administración. El Grupo de Trabajo llegó a la conclusión de que esas dos soluciones tal vez no fueran mutuamente excluyentes. La diferencia entre ambas situaciones podía estribar en los efectos jurídicos atribuidos a las firmas numéricas en uno y otro caso. En el caso de las autoridades certificadoras autorizadas ("licenciadas") 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 esa entidad; a su vez, ese requisito sería una condición para el reconocimiento de la eficacia jurídica de los certificados emitidos 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 emitidos 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 debería determinar si fue emitido por una autoridad certificadora que se ajustaba a esos criterios (véase el documento A/CN.9/437, párr.48).

21. Además de permitir la actuación de autoridades certificadoras tanto licenciadas como no licenciadas, el apartado c) abre aún más la esfera de aplicación del Régimen Uniforme hasta abarcar dispositivos de autenticación que funcionarían sin tener que depender de ningún tipo de entidad certificadora ni otro "tercero de confianza". La referencia a la condición de "segura" admite, pues, la introducción tanto de planes de licencias mediante los cuales los Estados promulgantes podrían comprobar la calidad y la fiabilidad de las firmas numéricas como las prácticas fijadas por el mercado que pudieran recurrir a otras formas de firma electrónica.

22. Conforme al inciso i) del apartado c), en virtud del Régimen Uniforme, se presumiría la condición de segura de la firma numérica que se consignase de conformidad con una infraestructura de claves públicas a cargo del Estado promulgante. A falta de esa infraestructura, o además de ella, se podría otorgar la condición de segura a las firmas electrónicas de cualquier tipo (es decir, firmas numéricas y otras firmas electrónicas consignadas con o sin la intervención de autoridades certificadoras u otros terceros de confianza), siempre que se satisficieran los requisitos mínimos. Con miras a proporcionar una norma básica con referencia a la cual pudiera evaluarse la calidad de esas firmas electrónicas, el inciso ii) del apartado c) enumera cuatro criterios: exclusividad, identificación, fiabilidad y vinculación con la información que se firme.

23. El requisito de que una firma electrónica segura esté "exclusivamente vinculada" con la persona que la utilice tiene por fin garantizar que no hay probabilidad razonable de que más de una persona produzca la misma firma, supuesta la ausencia de fraude u otra conducta impropia. El requisito de la exclusividad podría presumiblemente satisfacerse también con una firma de base biométrica que contuviera ciertos atributos exclusivos del firmante, como una impresión digital o una imagen de escáner retinal. Ese requisito se satisfaría igualmente con respecto a una firma numérica en que el par de claves utilizado por el firmante fuera generado aleatoriamente y suficientemente largo, de modo que la probabilidad de que alguna otra persona generara el mismo par de claves fuese extremadamente remota.

24. Una firma segura debiera ser tal que se pudiese utilizar para identificar al firmante. Esto no quiere decir que la firma misma deba consistir en el nombre del firmante o contenerlo. Bastaría la identificación mediante la referencia a otras fuentes de información. Por ejemplo, una firma numérica puede identificar al firmante mediante remitiéndose a un certificado emitido por una autoridad certificadora. El principal requisito es que el proceso de identificación sea relativamente rápido, objetivo y automático. Así pues, mientras que una firma manuscrita es presumiblemente capaz de identificar al firmante, esa identificación no puede normalmente hacerse con presteza ni automáticamente y con frecuencia no es una determinación objetiva. En muchos casos, la firma misma es ilegible. Incluso si es legible, la firma podrá en definitiva identificar al firmante, pero el momento y la certidumbre del proceso de identificación posiblemente no satisfará las necesidades del comercio electrónico. Una firma electrónica no siempre se podrá identificar fidedignamente como la firma de un individuo determinado (a falta de la admisión del hecho o de un testigo de la firma) sin el testimonio de un perito en análisis grafológico que haya comparado firmas reconocidas del supuesto firmante con la firma de que se trate. En ese caso, el resultado no será seguramente rápido ni automático y la conclusión a que llegue el perito es en muchos aspectos más subjetiva que objetiva. Por el contrario, la utilización de un número de identificación personal (NIP) en un cajero automático cuando se retiran fondos proporciona al banco una identificación automática, objetiva y rápida de una persona determinada vinculada con una dirección y un número de cuenta determinados. Esa persona no está en condiciones de negar que la solicitud de fondos contiene su firma (aunque puede negar que ha firmado la solicitud; ese es el tema del requisito de fiabilidad).

25. Además de identificar a una persona como el firmante de un mensaje, el procedimiento utilizado para firmar el mensaje ha de ofrecer un garantía razonablemente fiable de que la persona identificada como firmante es efectivamente la persona que firmó el mensaje. Un procedimiento de seguridad que requiera el empleo de una manera o de un medio que se halla únicamente bajo el control de la persona que crea la firma puede satisfacer ese requisito de fiabilidad. La utilización de un tercero de confianza puede aportar así mismo el grado de fiabilidad requerido. Pueden existir también otros medios con los que satisfacer este requisito. El Grupo de Trabajo tal vez desee examinar otros enfoques mediante los cuales conseguir un aceptable grado de fiabilidad.

26. Una firma segura debe estar vinculada con el mensaje de datos que se firme, de manera que cuando se cambie el mensaje la firma quede invalidada. Esa vinculación puede considerarse como un requisito decisivo para una firma segura, ya que, de no existir esa vinculación, la firma podría simplemente extraerse de un mensaje datos y pegarse a otro mensaje distinto.

27. Los incisos i) y ii) del apartado c) serían aplicables a falta de un acuerdo contractual preexistente relativo a las firmas electrónicas entre el iniciador y el destinatario del mensaje de datos que se firme. Sin embargo, consecuentemente con el criterio adoptado en la Ley Modelo, el Régimen Uniforme puede verse en la necesidad de reafirmar la validez de los sistemas contractuales con respecto a la autenticación de los mensajes de datos. El inciso iii) del apartado c) valida por tanto los acuerdos que establecen sistemas cerrados. Puede que el Grupo de Trabajo quiera estudiar si es necesario el texto entre corchetes ("entre las partes que participen en la generación, el envío, la recepción, el archivo u otra elaboración mensajes de datos en el curso ordinario de sus actividades,"), que retoma la redacción utilizada en la Ley Modelo, para limitar los efectos de la autonomía de la voluntad de las partes a la utilización comercial de las firmas electrónicas, con exclusión de las operaciones con consumidores (véase el documento A/CN.9/437, párr. 24).

Artículo 2. Presunciones

- 1) Con respecto a los mensajes de datos autenticados mediante una firma electrónica segura, se presumirá, salvo prueba en contrario, que:
 - a) el mensaje de datos no ha sido modificado desde el momento en que se consignó en él la firma electrónica segura;
 - b) la firma electrónica segura es la firma de la persona a quien se refiere; y
 - c) la firma electrónica segura fue consignada por esa persona con la intención de firmar el mensaje.
- 2) Con respecto a los mensajes de datos autenticados mediante una firma electrónica que no sea una firma electrónica segura, nada de lo dispuesto en el presente Régimen afectará las reglas substantivas o probatorias acerca de la carga de la prueba de la autenticidad y la integridad de un mensaje de datos o una firma electrónica.
- 3) Lo dispuesto en el presente artículo no será aplicable a: [...].
4. Las presunciones del párrafo 1) podrán ser destruidas mediante:
 - a) pruebas que indiquen que un procedimiento de seguridad empleado para verificar una firma electrónica no es generalmente reconocido como fiable, debido a los adelantos en la tecnología, la manera como el procedimiento se hizo funcionar o por otras razones;
 - b) pruebas que indiquen que el procedimiento de seguridad convenido entre las partes conforme al inciso iii) del apartado c) del artículo 1 no se hizo funcionar de manera fidedigna; o
 - c) pruebas relativas a hechos de que la parte que aceptó la firma era consciente que sugerirían que la confianza en el procedimiento de seguridad no era razonable. La razonabilidad comercial de un procedimiento de seguridad convenido por las partes conforme al inciso iii) del apartado c) del artículo 1 se determinará a la luz de las finalidades del procedimiento y las circunstancias comerciales en el momento en que las partes convinieron en adoptar el procedimiento, inclusive la naturaleza de la operación, el grado de avance tecnológico de las partes, el volumen de operaciones análogas en que ha intervenido una de las partes o ambas, la existencia de otras posibles soluciones ofrecidas a la parte pero rechazadas por ella, el costo de otros procedimientos posibles y los procedimientos de uso general para tipos de transacción análogos.]

Referencias

A/CN.9/437, párrs. 43, 48 y 92.

Observaciones

28. El proyecto de artículo 2 se centra en los efectos jurídicos que se derivan del reconocimiento de la condición de "firma electrónica segura". En su anterior período de sesiones, el Grupo de Trabajo examinó la posibilidad de que ciertas cuestiones relacionadas con las firmas electrónicas (por ejemplo, la responsabilidad de las autoridades certificadoras y la atribución de los mensajes firmados numéricamente) se trataran por medio de presunciones (véase el documento A/CN.9/437, párrs. 58, 70 y 120 y 121).

29. El concepto de firma electrónica segura y las presunciones simples que se infieren de su condición de tal pueden considerarse críticos para habilitar un sistema de comercio electrónico viable. En las operaciones en un medio de documentación escrita, la parte que acepta la firma puede utilizar varios indicadores para determinar si el documento es auténtico y la firma genuina. Figuran entre ellos el uso de papel (a veces con marcas de agua, fondos de color u otros indicadores de fiabilidad) sobre el que se ha escrito el mensaje, el uso de membrete, las firmas manuscritas o la entrega en sobres sellados por un tercero de confianza (como los servicios postales). Pero en las comunicaciones electrónicas no está presente ninguno de estos factores de fiabilidad. Todo cuanto se puede comunicar es un conjunto de impulsos electrónicos, idénticos en todos los aspectos y fáciles de copiar o de modificar. Por consiguiente, importa en muchos casos al destinatario o a cualquier otra parte pueda tener que basarse en una comunicación electrónica saber, en el momento en que se recibe o se recurre a ella, si el mensaje es auténtico, si se ha mantenido la integridad de su contenido y si podrá probar ambos hechos en caso de una posterior controversia (es decir, probar ante un tribunal el repudio negativo de un mensaje de datos). Con este fin, la existencia de presunciones simples respecto de las firmas seguras puede proporcionar esas garantías a las partes interesadas, permitiéndoles así dedicarse a actividades comerciales en la confianza de que sus operaciones serán más fácilmente llevadas a cumplimiento en caso necesario.

30. El efecto de las presunciones del proyecto de artículo 2 debe distinguirse del efecto de atribución previsto en el proyecto de artículo 3. Las presunciones del primero tiene por objeto aliviar la carga de la prueba de la fuente de un mensaje electrónico cuando el receptor ha verificado la fuente aparente del mensaje utilizando una firma electrónica segura. Se pide, pues, a la persona a la que se refiere la firma que pruebe que, pese a la verificación por el destinatario de la firma electrónica segura y el empleo del procedimiento de seguridad, la firma no era la de esa persona. Como justificación para establecer esa presunción, cabe observar que las pruebas necesarias para demostrar quién envió realmente el mensaje se hallan normalmente en poder de la persona a la que se refiere la firma. Por ejemplo, en el caso de una firma numérica, esta persona es la que se halla en mejor situación que cualquier otra parte interesada para probar que la clave privada fue hurtada, copiada, expuesta o utilizada sin permiso por un tercero. En una situación típica, el receptor del mensaje no dispondrá de más prueba que el procedimiento de seguridad para demostrar que la persona a la que se refiere la firma envió realmente el mensaje. No obstante, en virtud del proyecto de artículo 3, incluso si la parte a la que se refiere la firma puede probar que no envió el mensaje de que se trate, puede sin embargo tener que responder por las pérdidas experimentadas por el receptor que razonablemente se fió del mensaje cuando se satisfacen los requisitos del proyecto de artículo 3.

31. Consecuentemente con el enfoque adoptado en el artículo 7 de la Ley Modelo, el párrafo 1) no crea una presunción de que el mensaje de datos que ostenta una firma electrónica segura constituye una obligación jurídicamente vinculante. El párrafo 1) se limita a presumir que la firma electrónica segura fue consignada por el supuesto firmante con intención de firmar el mensaje. Si hay pruebas de que la persona cuya firma se consignó fue víctima de error, engaño, violencia u otra causa de nulidad, se podrá negar eficacia jurídica al mensaje, pero la carga de plantear estas cuestiones corresponde a la persona que niega eficacia al mensaje de datos.

32. El párrafo 2) pone en claro que, a falta de una firma electrónica segura, nada de lo dispuesto en el Régimen Uniforme cambia las reglas ordinarias de la prueba sobre la carga de demostrar cuál es la fuente del mensaje. El párrafo 3) está imitado de disposiciones análogas de la Ley Modelo. Obedece al propósito de facilitar la exclusión de ciertas situaciones del beneficio otorgado por el proyecto de artículo 2 en los casos en que un interés legítimo requiera esa exclusión por parte del Estado promulgante. Por ejemplo, los Estados promulgantes pueden decidir que las presunciones establecidas en el proyecto de artículo 2 no se apliquen en la esfera del derecho penal. El párrafo 4) enumera varias maneras de destruir la presunción establecida en el párrafo 1). El Grupo de Trabajo tal vez desee examinar si se necesita esa disposición ilustrativa en el texto del Régimen Uniforme o si habría que considerarla en el contexto de una guía o comentario.

Artículo 3. Atribución

- 1) Variante A Sin perjuicio de lo dispuesto en [el artículo 13 de la ley Modelo de la CNUDMI sobre Comercio Electrónico], el iniciador de un mensaje de datos en el que se ha consignado su firma electrónica segura [estará obligado por el contenido][se considerará firmante] del mensaje de la misma manera que si el mensaje hubiera existido en forma [manualmente] firmada con arreglo a la ley aplicable al contenido del mensaje.

Variante B Entre el titular de una clave privada y todo tercero que se fíe de una firma numérica susceptible de ser [verificada][autenticada] utilizando la correspondiente clave pública certificada, la firma numérica [se presumirá que pertenece al titular][satisface las condiciones expuestas en [el párrafo 1 del artículo 7 de la ley Modelo de la CNUDMI sobre Comercio Electrónico]].

- 2) El párrafo 1) no se aplicará cuando

a) el [iniciador][titular] pueda demostrar que la [firma electrónica segura][clave privada] se utilizó sin permiso y que el [iniciador][titular] no pudo evitar dicha utilización ejerciendo una diligencia razonable;

b) la parte que se fió de la firma sabía o debió haber sabido, si hubiese pedido información [al iniciador][a la autoridad certificadora] o hubiese de otra manera ejercido una diligencia razonable, que la firma [electrónica segura][numérica] no pertenecía al [iniciador][titular de la clave privada].

Referencias

A/CN.9/437, párrs. 118 a 124 (proyecto de artículo E);

A/CN.9/WG.IV/WP.71, párrs. 64 y 65.

Observaciones

33. En su anterior período de sesiones, el Grupo de Trabajo estimó en general que no había que intentar confirmar en el contexto del Régimen Uniforme los principios expuestos en el artículo 13 de la ley Modelo de la CNUDMI sobre Comercio Electrónico (véase el documento A/CN.9/437, párrs. 119 y 120). No obstante, se estimó también que debía aclararse la relación entre el Régimen Uniforme y los artículos 7 y 13 de la Ley Modelo. En ese sentido, la Variante A del párrafo 1), que refleja un principio que el Grupo de Trabajo, en su anterior período de sesiones, juzgó en general aceptable (véase el documento A/CN.9/437, párr. 120), está redactada en términos amplios a efectos de abarcar las firmas numéricas y otras técnicas que se pueden utilizar para producir una firma numérica segura.

34. La Variante B crea una presunción de que una firma numérica satisface los requisitos de un "método fiable" conforme al artículo 7 de la Ley Modelo. El Grupo de Trabajo podría quizá considerar si esa presunción debe ampliarse para que abarque no sólo las firmas numéricas sino también otros casos en los que se utiliza una firma electrónica segura. Si el Grupo de Trabajo deseara limitar el alcance de la disposición a las firmas numéricas, habría que reubicar en consecuencia el proyecto de artículo 3.

35. El Grupo de Trabajo tal vez desee examinar si cabe utilizar el proyecto de artículo 3 para tratar más precisamente la cuestión de cuándo se puede considerar a una persona responsable del contenido de un mensaje de datos cuando el mensaje no fue enviado en realidad por esa persona y el mensaje se comunica en un entorno abierto (es decir, sin un acuerdo previo celebrado directamente entre el iniciador y el receptor del mensaje (o en el contexto de unas "reglas del sistema") acerca del procedimiento que se ha de aplicar para determinar la atribución del mensaje de datos). Si bien el apartado a) del párrafo 3 del artículo 13 de la Ley Modelo se ocupa de la cuestión cuando se utiliza "un procedimiento aceptado previamente por el iniciador", la Ley Modelo no se refiere expresamente al entorno abierto. Dado el alto grado de seguridad inherente a las firmas electrónicas seguras, tal vez el Grupo de Trabajo quiera examinar si se podría establecer una regla general en el sentido de que el receptor de un mensaje que razonablemente se fie en una firma electrónica segura tiene derecho a considerar que el mensaje es del iniciador.

36. Como ejemplo de una disposición en ese sentido, el Grupo de Trabajo podría examinar la siguiente redacción:

Salvo lo dispuesto por otra ley aplicable, una firma electrónica segura es atribuible a la persona a la que al parecer se refiere, con su autorización o sin ella, cuando:

a) la firma electrónica es el resultado de actos de una persona que obtuvo el acceso a cifras, códigos, programas informáticos u otra información necesaria para crear la firma de una fuente bajo el control del supuesto firmante, haciéndola aparecer como procedente de esa persona;

b) el acceso se produjo en circunstancias de una omisión en el ejercicio de una diligencia razonable por parte del supuesto firmante; y

c) el receptor se fió de buena fe en perjuicio suyo de la fuente aparente del mensaje de datos.

El efecto de esa redacción es asignar el riesgo de la pérdida entre las dos partes interesadas, es decir, el supuesto iniciador que no firmó realmente el mensaje de que se trata y el receptor que confió de buena fe en el mensaje, de conformidad con un procedimiento de seguridad comercialmente razonable. El riesgo de la pérdida se carga al supuesto iniciador solamente en la situación en que el mensaje ostente su firma como resultado de su supuesta culpa. Esa situación puede producirse cuando la firma fue creada por una persona que obtuvo la información necesaria de una fuente bajo el control del supuesto iniciador y si el acceso tuvo lugar en circunstancias resultantes de una omisión en el ejercicio de una diligencia razonable por parte del supuesto iniciador. En tal caso, si el receptor confía razonablemente en el mensaje, el supuesto iniciador quedará vinculado. En todos los demás casos, el riesgo de la pérdida recaerá sobre el receptor a pesar de su razonable confianza. La mención de "otra ley aplicable" en las palabras iniciales puede ser necesaria a fin de excluir del alcance de la norma que se sugiere las operaciones con los consumidores.

Sección II. Firmas numéricas

Artículo 4. Definición

Para los fines del presente Régimen,

Variante A por "firma numérica" se entenderá un tipo de firma electrónica consistente en una transformación de un mensaje de datos gracias al empleo de una función de compendio de mensajes y un criptosistema asimétrico que permitan que una persona que disponga

del mensaje de datos sin transformar y de la clave pública del firmante pueda determinar con exactitud:

- a) si la transformación se efectuó utilizando la clave privada del firmante que corresponde a su clave pública; y
- b) si el mensaje de datos inicial fue modificado después de efectuada la transformación.

Variante B

a) por "firma numérica" se entenderá un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido vinculado a la clave criptográfica privada del iniciador, permite determinar que ese valor numérico se ha obtenido exclusivamente con la clave criptográfica privada del iniciador.

b) Los procedimientos matemáticos utilizados para generar firmas numéricas autorizadas a tenor del presente Régimen se basan en la criptografía de clave pública. Aplicados a un mensaje de datos, esos procedimientos matemáticos transforman del mensaje de modo que permite que una persona que tenga el mensaje inicial y la clave pública del iniciador pueda determinar con exactitud:

i) si la transformación se efectuó utilizando la clave privada del firmante que corresponde a la clave pública del iniciador; y

ii) si el mensaje de datos inicial fue modificado después de efectuada la transformación.

Referencias

A/CN.437, párrs. 30 a 38 (proyecto de artículo A);

A/CN.9/WG.IV/WP.71, párrs. 18 a 45 y 55 y 56.

Observaciones

37. Las diferencias entre las Variantes A y B son mayormente de redacción. Mientras que la Variante B refleja las conclusiones alcanzadas por el Grupo de Trabajo en su anterior período de sesiones (véase el documento A/CN.437, párr. 32), la Variante A ofrece un texto más simple, desarrollando la definición de "firma electrónica". En ambas Variantes, "firma numérica" se define sin hacer referencia a "autoridades certificadoras" ni a "certificados".

38. No se ha intentado presentar definiciones de "clave privada", "clave pública", "par de claves" ni de otros conceptos relativos a la criptografía de clave pública. Aunque en el anterior período de sesiones del Grupo de Trabajo se hicieron sugerencias de otras definiciones, se aconsejó cautela en la introducción de un gran número de definiciones en unas normas uniformes de carácter legal, lo que podría ser contrario a la tradición legislativa de muchos países. El Grupo de Trabajo tal vez desee examinar en qué medida se necesitarían más definiciones (véase el documento A/CN.437, párr. 29).

Artículo 5. Efectos

- 1) Si un mensaje de datos está firmado en todo o en parte con una firma numérica, ésta se considerará como firma electrónica segura con respecto a la parte pertinente del mensaje cuando:
 - a) la firma numérica fue creada durante el período de vigencia de un certificado [válido] y ha sido verificada con referencia a la clave pública enunciada en el certificado; y
 - b) se estime que el certificado vincula con exactitud una clave pública con la identidad de una persona porque:
 - i) el certificado fue emitido por una autoridad certificadora licenciada [acreditada] por ... *[el Estado promulgante especifica el órgano o la autoridad competente para licenciar a las autoridades certificadoras y promulgar reglamentos para su funcionamiento]*; o
 - ii) el certificado fue de alguna otra manera emitido por una autoridad certificadora de conformidad con las normas dictadas por ... *[el Estado promulgante especifica el órgano o la autoridad competente para establecer normas reconocidas sobre el funcionamiento de autoridades certificadoras licenciadas]*.
- 2) Si un mensaje de datos está firmado en todo o en parte con una firma numérica que no satisface los requisitos contenidos en el párrafo 1), la firma numérica se considerará como firma electrónica segura con respecto a esa parte del mensaje si hay pruebas suficientes que indiquen que el certificado vincula con exactitud una clave pública con la identidad del titular.
3. Lo dispuesto en el presente artículo no será aplicable a: [...].

Referencias

A/CN.9/437, párrs. 43, 48 y 92.

Observaciones

39. Las firmas numéricas, debidamente utilizadas, deben constituir firmas electrónicas seguras. Sin embargo, se plantea la cuestión de determinar cuándo la instrumentación de una firma numérica se ha hecho de manera que justifique su condición de segura. No todas las firmas numéricas verificables con referencia a un certificado son seguras, en especial si existe incertidumbre acerca de si la identificación o la autenticación del titular es exacta. Los factores primarios que determinan si una firma numérica es segura son: 1) si la autoridad certificadora ha identificado correctamente al titular; 2) si la autoridad certificadora ha autenticado correctamente la clave pública del titular; 3) si la clave privada del titular 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 son apropiados).

40. El párrafo 1) enumera dos criterios básicos para determinar cuándo 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 desde que se produce su expiración, su revocación o su suspensión.

41. El segundo paso entraña el cerciorarse de que el certificado mismo identifica correctamente a una persona como titular de la 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 en el Estado promulgante. Esas normas pueden probarse mediante la acreditación de las autoridades certificadoras por terceros o la licencia voluntaria de estas autoridades o requerir de algún otro modo el cumplimiento de las reglas adoptadas por el Estado promulgante.

42. 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 resulta obvia. Pero, 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.

43. Consecuente con el "criterio dual" adoptado por el Grupo de Trabajo, el artículo 5 tiene por fin 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.

44. Es también importante observar que, mientras una de las opciones expuestas en el artículo 5 entraña una determinación judicial de la exactitud del certificado, la otra 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 éste. En ese caso, no se precisa una conclusión judicial 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 valiéndose de 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 acreditada no es, en realidad, ni exacto ni fidedigno.

[Artículo 6. Firma de personas jurídicas

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 la persona física autorizada para actuar en nombre de dicha persona jurídica.]

Referencias

A/CN.437, párrs. 114 a 117 (proyecto de artículo D);
A/CN.9/WG.IV/WP.71, párrs. 61 a 63.

Observaciones

45. En el anterior período de sesiones, predominaba la opinión de que había que suprimir el artículo 6. Pero, tras un debate, el Grupo de Trabajo decidió que se colocara entre corchetes, para volverlo a examinar en un período de sesiones posterior (A/CN.437, párrs. 115 a 117). Aunque una disposición análoga al proyecto de

artículo 6 pueda parecer que se injiere indebidamente en otras zonas del derecho (por ejemplo, el mandato y las disposiciones sobre sociedades que tratan de su representación por personas físicas), puede también ser útil, en la presente etapa del desarrollo del Régimen Uniforme, como recordatorio de que el Grupo de Trabajo quizá se vea en el caso de tener que examinar más a fondo la medida en que el Régimen Uniforme tiene que validar el funcionamiento de los "mandatarios electrónicos" a los efectos de autenticar automáticamente los mensajes de datos.

Sección III. Otras firmas electrónicas

46. Dado que no se comunicó a la Secretaría información sobre cómo ocuparse en el Régimen Uniforme de otras técnicas distintas de las firmas numéricas, no se ha preparado ninguna disposición especial para incluirla en esta sección. El Grupo de Trabajo posiblemente querrá examinar si esas técnicas de autenticación deben ser tratadas con más detalle en el Régimen Uniforme. Si el Grupo de Trabajo llega a la conclusión de que esas técnicas no deben ser abordadas más concretamente, el Régimen Uniforme seguiría con todo favoreciendo la utilización cada vez mayor de métodos alternativos a las firmas numéricas, merced al principio de no discriminación incorporado a las definiciones de "firma" y "firmas electrónicas seguras", y mediante la condición jurídica reconocida a toda técnica de autenticación que satisfaga los requisitos de una "firma electrónica segura".

CAPÍTULO III. AUTORIDADES CERTIFICADORAS Y CUESTIONES CONEXAS

Artículo 7. Autoridad certificadora

- 1) Para los fines del presente Régimen, por "autoridad certificadora" se entenderá:
 - a) toda persona o entidad licenciada [acreditada] por ...*[el Estado promulgante especifica el órgano o la autoridad competente para conceder licencias a las autoridades certificadoras y promulgar reglamentos para su funcionamiento]* para actuar de conformidad con el presente Régimen; o
 - b) toda persona o entidad que, como parte ordinaria de sus actividades, se dedique a emitir certificados en relación con claves criptográficas utilizadas para firmas numéricas.
- [2] Toda autoridad certificadora autorizada podrá prestar o facilitar servicios de inscripción registral y de certificación cronológica de la transmisión y recepción de mensajes de datos, así como desempeñar otras funciones respecto de una comunicación protegida por medio de una firma numérica.]

Referencias

A/CN.437, párrs. 39 a 50 y 90 a 97 (proyecto de artículo B);
A/CN.9/WG.IV/WP.71, párrs. 18 a 45 y 57 y 58.

Observaciones

47. Como se indicó con referencia al proyecto de artículo 1, el Régimen Uniforme debe otorgar reconocimiento jurídico tanto a la situación en que un Estado promulgante desee reglamentar el funcionamiento de las autoridades certificadoras mediante una infraestructura de claves públicas u otro sistema de licencias

como a aquella en que puedan funcionar libremente, conforme a las normas de la práctica fijadas por el mercado, autoridades certificadoras sin licencia (véase *supra*, párrs. 17 y 18).

48. Al ocuparse de las autoridades de certificación licenciadas, el párrafo 1) no trata de definir los criterios que han de utilizar los Estados promulgantes al organizar una infraestructura de claves públicas u otro sistema de licencias para las autoridades certificadoras. Una razón para no abordar esos criterios puede ser el fuerte componente de orden público de esas infraestructuras, que tal vez no se presten demasiado a una armonización internacional por medio de un modelo de disposiciones legislativas. De emprender el Grupo de Trabajo un examen más detallado de los criterios que se han de emplear en el contexto de un sistema de licencias, quizá desee analizar los siguientes factores a tener en cuenta al determinar si una autoridad certificadora es digna de confianza: 1) independencia (es decir, ausencia de un interés financiero o de otro tipo en las operaciones subyacentes); 2) recursos y capacidad financieros para asumir la responsabilidad por el riesgo de pérdida; 3) competencia del personal de gestión, experiencia en tecnologías de clave pública y familiaridad con procedimientos de seguridad apropiados; 4) longevidad (las autoridades certificadoras pueden tener que presentar pruebas de certificaciones o claves de descodificación muchos años después de que se haya completado la operación subyacente, por ejemplo en el contexto de un juicio o un reclamación de propiedad); 5) aprobación del equipo y los programas; 6) mantenimiento de un registro de auditoría y realización de auditorías por una entidad independiente; 7) existencia de un plan para casos de emergencia (por ejemplo, "programas de recuperación en casos de desastres" o depósito de claves bloqueado); 8) selección y administración del personal; 9) disposiciones para proteger su propia clave privada; 10) seguridad interna; 11) disposiciones para cesar las operaciones, incluida la notificación a los usuarios; 12) garantías y declaraciones (otorgadas o excluidas); 13) limitación de la responsabilidad; 14) seguros; 15) interoperabilidad con otras autoridades certificadoras; 16) procedimientos de revocación (en caso de que se hayan perdido o estén expuestas las claves criptográficas); 17) separación de la función certificadora de cualquier otra actividad que la autoridad pudiera desarrollar (véanse los documentos A/CN.9/WG.IV/WP.71, párr. 44, y A/CN.9/437, párr. 45).

49. El apartado b) del párrafo 1) define "autoridad certificadora" sin hacer mención de la autorización pública, con referencia a su función como emisora de certificados. Esa disposición, en combinación con el párrafo 2), intenta también reflejar que, si bien las autoridades certificadoras pueden desempeñar otras funciones y ofrecer otros servicios además de la emisión de certificados, esas funciones y esos servicios quedan fuera del ámbito de aplicación del Régimen Uniforme y no se han de tener en cuenta al referirse a los efectos jurídicos de las firmas electrónicas. Tal vez el Grupo de Trabajo quiera examinar si tiene que formar parte del Régimen Uniforme una disposición análoga al párrafo 2), de naturaleza principalmente descriptiva, o si habría que enunciarla más bien en una guía o un comentario.

Artículo 8. Certificado

Para los fines del presente Régimen Uniforme, por "certificado" se entenderá un mensaje de datos [u otra constancia] que, por lo menos:

- a) identifique a la autoridad certificadora que lo emita;
- b) nombre o identifique a su titular o un dispositivo o agente electrónico bajo el control del titular;
- c) contenga una clave pública que corresponda a una clave privada bajo el control del titular;
- d) especifique su período de vigencia [y las restricciones que haya, si las hay, respecto del ámbito de utilización de la clave pública]; y

- e) esté firmado [numéricamente] por la autoridad certificadora que lo emita.

Referencias

A/CN.437, párrs. 98 a 113 (proyecto de artículo C);
A/CN.9/WG.IV/WP.71, párrs. 18 a 45 y 59 a 60.

Observaciones

50. Por más que un certificado pueda utilizarse para desempeñar una serie de funciones y transmitir otra información, ajena al ámbito del Régimen Uniforme, la única función de un certificado de que éste trata es la de vincular una clave pública con determinado titular. Esa vinculación puede hacerse directamente, nombrando en el certificado al titular de la clave pública. Puede hacerse también indirectamente, describiendo ciertos atributos del titular (por ejemplo, un encargado de las compras con mandato para efectuarlas hasta una determinada cuantía) o describiendo una máquina, un dispositivo o agente de programas bajo el control del titular. Así, por ejemplo, se puede emitir un certificado al empleado de una empresa en el que se especifiquen sólo los límites de ese mandato para efectuar compras. Podrá luego utilizarse en operaciones de compra con interlocutores comerciales si la identidad del empleado concreto no es importante, sino que las cuestiones principales son saber si el empleado tiene facultades para actuar en nombre de una persona identificada (es decir, el empleador) y el límite de ese mandato. Pero en todos los casos existe una persona, conocida como el "titular" que controla la clave privada que corresponde a la clave pública identificada en el certificado, que es la persona a la se han de atribuir los mensajes firmados numéricamente verificados con referencia al certificado. Si no se identifica a esa persona, el certificado no puede utilizarse para verificar que una firma numérica pertenece a determinada persona.

51. El proyecto de artículo 8 tiene por fin reflejar los elementos que el Grupo de Trabajo considera como los componentes fundamentales de un certificado, a saber, que un certificado debe: ser un mensaje de datos; identificar a la autoridad certificadora; contener la clave pública del titular; identificar al titular; y estar firmado numéricamente por la autoridad certificadora (véase el documento A/CN.9/437, párr.101). En cuanto a si el certificado tiene que adoptar necesariamente la forma de un mensaje de datos, el Grupo de Trabajo posiblemente desee examinar si el Régimen Uniforme ha de ocuparse también de los certificados extendidos sobre papel.

52. En el anterior período de sesiones, el Grupo de Trabajo decidió que podría tener que examinar si el establecimiento de una norma imperativa sobre la información mínima que debía suministrarse en un certificado podía ser contrario a la ley aplicable sobre protección de datos. Se supone que, en vista de la naturaleza de los elementos enumerados en el proyecto de artículo 8, se evita esa posibilidad.

53. La definición de "certificado" no distingue entre los diferentes grados de seguridad que pueden proporcionarse comercialmente bajo el epígrafe de un "certificado". No obstante al preparar el Régimen Uniforme, el Grupo de Trabajo puede tener presente que las autoridades certificadoras suelen ofrecer diversas clases de certificados. En el anterior período de sesiones del Grupo de Trabajo, se hicieron distintas sugerencias para el Régimen Uniforme reflejase los diversos grados de seguridad que pueden darse como consecuencia de la utilización de esos certificados (véase el documento A/CN.9/437, párrs. 20, 56, 138 y 145). Como ejemplo de esa diversidad, se informa de que existen en el mercado las tres clases de "certificados" que se enumeran a continuación.

54. Los certificados de la Clase I confirman que el nombre y la dirección de correo electrónico de un usuario forman el nombre inequívoco de un objeto dentro del registro, o "depósito" que conserva la autoridad

certificadora. Se suelen utilizar para consulta en la Internet y para el correo electrónico personal, con la finalidad de aumentar modestamente la seguridad de esos entornos. Los certificados de la Clase I no se proponen autenticar la identidad del titular. Representan, más bien, una simple comprobación de la inequívocidad del nombre de que se trate dentro del depósito y una verificación limitada de la dirección de correo electrónico. El nombre de un titular que figure en un certificado de la Clase I se considera como una información no verificada. Estos certificados proporcionan un grado muy bajo de seguridad. No están destinados al uso comercial cuando se precisa una prueba de la identidad y no deben hacerse valer en esos casos.

55. Los certificados de la Clase II confirman que la información suministrada por el titular cuando solicita un certificado no se contradice con la información accesible en bases de datos para consumidores ampliamente reconocidas. Los certificados de la Clase II suelen utilizarse para: 1) correo electrónico entre organizaciones; 2) operaciones de escaso valor y de bajo riesgo; 3) correo electrónico personal; 4) validación de programas informáticos; y 5) servicios en línea por suscripción. Los certificados de la Clase II brindan cierto nivel de certeza en cuanto a la identidad del titular, sobre la base de un proceso automatizado y en línea.

56. Los certificados de la Clase III proporcionan seguridades importantes en cuanto a la identidad del titular al requerir, por ejemplo, la comparecencia personal (física) del titular ante un representante de la autoridad certificadora o la verificación de su identidad mediante los documentos de identificación adecuados. La clave privada correspondiente a la clave pública que figura en un certificado de la Clase III debe ser generada y almacenada de manera fidedigna de acuerdo con los requisitos expresados por la autoridad certificadora. Estos certificados se utilizan en la práctica para ciertas aplicaciones del comercio electrónico como la banca electrónica, el intercambio electrónico de datos (EDI) y los servicios en línea basados en la afiliación. Los procesos para emitir certificados de la Clase III utilizan diversos procedimientos para obtener elementos probatorios de la identidad de sus suscriptores. Estos procedimientos de validación proporcionan seguridades mayores sobre la identidad de un solicitante que los de la Clase II.

57. En los anteriores ejemplos, está claro que únicamente los certificados de la Clase III caerían dentro del alcance actual del Régimen Uniforme. El Grupo de Trabajo tal vez quiera examinar si hay que ampliar el alcance del Régimen Uniforme para que abarque igualmente clases inferiores de certificados, en cuyo caso habría que adoptar una decisión acerca de los diversos efectos jurídicos que se asignarían a las distintas clases de certificados, en particular en relación con el grado de responsabilidad que se impondría a las autoridades certificadoras con respecto a la emisión de certificados de clase inferior. Otra posibilidad sería modificar la definición de "certificado" en el Régimen Uniforme para poner en claro que no quedarían comprendidos en él los certificados con un grado de seguridad inferior.

Artículo 9. Declaración sobre prácticas de certificación

Para los fines del presente Régimen Uniforme, 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 manipulación de certificados.

Referencias

A/CN.437, párrs. 60 a 62, 70, 110 y 111, y 149 (proyecto de artículo J);
A/CN.9/WG.IV/WP.71, párr. 89.

Observaciones

58. La medida en que una parte que se basa en un certificado pueda confiar en el vínculo entre una persona y una clave pública, tal como figura en un certificado, depende de varios factores. Entre esos factores se cuentan las prácticas y los procedimientos aplicados por la autoridad certificadora para autenticar al titular del juego de claves y las normas de funcionamiento, los procedimientos y los controles de seguridad de esa autoridad. Las autoridades certificadoras presentan a menudo las declaraciones sobre prácticas de certificación como uno de los principales elementos mediante los cuales fomentan la confianza en la exactitud de los certificados que expiden y, más generalmente, como la norma de calidad y responsabilidad que debe regir la relación entre las autoridades certificadoras y sus clientes.

59. Una declaración sobre prácticas de certificación es aquella por la que la autoridad certificadora expone las directrices que sigue o los pormenores de las prácticas, los procedimientos y los sistemas que emplea en su funcionamiento y en apoyo de la emisión, gestión y revocación de los certificados. Entre los puntos que pueden constar en una declaración sobre prácticas de certificación figuran: 1) los procedimientos utilizados para autenticar la identidad de quien solicita un certificado (antes de emitirlo); 2) los controles físicos, de procedimiento y del personal utilizados por la autoridad certificadora para llevar a cabo con seguridad las funciones de generación de claves, expedición de certificados, revocación de certificados, auditoría y archivo; 3) las medidas de seguridad adoptadas por la autoridad certificadora para proteger sus claves criptográficas; y 4) cualquier otra información conexas. Estas cuestiones tienen importancia tanto para el tenedor, que obtiene el certificado como para las partes que se fíen de él y que utilizarán el certificado emitido por la autoridad como base para realizar operaciones con el titular.

60. La declaración sobre prácticas de certificación puede adoptar diversas formas, como un contrato entre todas las partes interesadas o un aviso público a todas ellas. Pero el elemento principal es la notificación a las partes que se hayan de basar en él. La declaración sobre prácticas de certificación debe constituir una notificación de la autoridad certificadora a todas las partes interesadas (inclusive los titulares) en las prácticas empleadas por la autoridad en la emisión, la gestión y la revocación de certificados.

Artículo 10. Declaraciones al emitir un certificado

Variante A

1) Al emitir un certificado, la autoridad certificadora declara a toda persona que razonablemente se fie del certificado o de una firma numérica verificable por la clave pública indicada en él, que:

a) la autoridad certificadora ha cumplido con todos los requisitos aplicables, a tenor del presente Régimen, para la emisión del certificado y, caso de publicar el certificado o de ponerlo por cualquier otro medio a disposición de alguna persona que razonablemente se fie de su contenido, declara así mismo que el titular indicado en el certificado [y que sea titular legítimo de la clave privada correspondiente] ha aceptado que así se hiciera;

b) el titular designado en el certificado tiene [legítimamente] en su poder la clave privada correspondiente a la clave pública indicada en el certificado;

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

d) toda la información que figura en el certificado es exacta a la fecha en que se emitió, salvo que la autoridad certificadora haya declarado en el certificado [o en otro lugar al que éste remita] que no confirma la exactitud del algún dato determinado; y

e) la autoridad certificadora no tiene constancia de que en el certificado se hayan omitido datos sustanciales que, de conocerse, restarían fiabilidad a las declaraciones que anteceden.

2) Sin perjuicio de lo dispuesto en el párrafo 1), la autoridad certificadora que emite un certificado declara a cualquier persona que razonablemente se fie de él o de una firma numérica verificable por la clave pública indicada en el certificado que la autoridad certificadora lo ha emitido con arreglo a cualquier declaración sobre prácticas de certificación aplicable [incorporada al certificado por vía de remisión o] de la cual esa persona tenga noticia.

Variante B

1) Al emitir un certificado, la autoridad certificadora declara al titular y a toda persona que razonablemente se fie de la información contenida en el certificado [,de buena fe y] durante su período de vigencia, que:

a) la autoridad certificadora ha [procesado][aprobado][emitido] y gestionará y si es necesario revocará, el certificado de acuerdo con:

i) el presente Régimen;

ii) toda otra ley aplicable que rija la emisión del certificado; y

iii) toda declaración sobre prácticas de certificación formulada en el certificado o incorporada a él por vía de remisión, o de la cual esa persona tenga noticia, si la hubiere;

b) la autoridad certificadora ha verificado la identidad del titular en la medida indicada en el certificado o en cualquier declaración sobre prácticas de certificación aplicable o, a falta de esa declaración, la ha verificado de manera [fiable][fidedigna];

c) la autoridad certificadora ha verificado que la persona que solicita el certificado tiene en su poder la clave privada correspondiente a la clave pública indicada en el certificado;

d) salvo lo expresado en el certificado o en cualquier declaración sobre prácticas de certificación aplicable, por lo que le consta a la autoridad certificadora, toda otra información que figure en el certificado es exacta a la fecha en que se emitió;

e) si la autoridad certificadora ha publicado el certificado, el titular indicado en el certificado ha aceptado que así se hiciera.

[2) Si una autoridad certificadora emitió el certificado con sujeción a las leyes de otra jurisdicción, esa autoridad da también las garantías y hace las declaraciones por otra parte aplicables, en su caso, conforme a la ley que rigió su emisión.]

Referencias

A/CN.437, párrs. 51 a 73 (proyecto de artículo H);
A/CN.9/WG.IV/WP.71, párrs. 70 a 72.

Observaciones

61. El proyecto de artículo 10 obedece al propósito de reflejar la decisión adoptada por el Grupo de Trabajo de que, en principio, el proyecto de Régimen Uniforme contenga disposiciones relativas a la responsabilidad de las autoridades certificadoras en el contexto de su participación en los sistemas de firmas numéricas (A/CN.437, párr. 55). La norma mínima de responsabilidad formulada en el proyecto de artículo 10 está pensada sólo para la emisión de certificados referentes a las firmas numéricas como se definen en el proyecto de artículo 4. El proyecto de Régimen Uniforme no se propone ocuparse de otras actividades o servicios que puedan desarrollar o prestar las autoridades certificadoras. Esas actividades y esos servicios pueden ser objeto de un arreglo contractual entre las autoridades certificadoras y sus cliente y a cualquier otra ley aplicable (*ibid.*, párr. 71).

62. En su 31º período de sesiones, el Grupo de Trabajo convino en general en que una redacción análoga a la del párrafo 1) de la Variante A era, en su mayor parte, substancialmente aceptable como base de futuros debates. Si bien no establece expresamente una norma de responsabilidad, el párrafo 1) fija una norma mínima que no debe permitirse que las partes modifiquen mediante un acuerdo privado. En particular, no debe considerarse comprendida dentro del ámbito de protección o beneficio algunos previstos por el proyecto de Régimen Uniforme ninguna cláusula que limite la responsabilidad de una autoridad certificadora si está en conflicto con los mencionados requisitos. Cuando se invoca la responsabilidad de una autoridad certificadora, se presume que ésta responde de las consecuencias de la emisión del certificado, a menos que pueda probar que satisface los requisitos enumerados en el párrafo 1). Sin embargo, si una autoridad certificadoras quisiese asumir obligaciones más estrictas que las declaraciones indicadas en el párrafo 1), debe permitírsele que así lo haga, mediante cláusulas incluidas en una declaración sobre prácticas de certificación o por otra vía (A/CN.437, párr. 70). El párrafo 2) tiene por fin hacer frente a situaciones en que las declaraciones sobre prácticas de certificación contuviesen esas normas más estrictas.

63. La Variante B, aunque inspirada en la Variante A, hace mayor hincapié en la autorreglamentación de las autoridades certificadoras. En particular, en el apartado b), la autoridad certificadora no garantiza que el titular tiene lícitamente la clave privada en su poder. En vez de ello, garantiza que, a los efectos de demostrar el vínculo entre el titular de la clave privada, siguió por lo menos los procedimientos expuestos en su declaración sobre prácticas de certificación o utilizó métodos "fiabes" o "fidedignos" para identificar al titular. El párrafo 2) de la Variante B aclara que el inciso ii) del apartado a) del párrafo 1 es también aplicable si el certificado se emite conforme a las leyes de otra jurisdicción. El Grupo de Trabajo tal vez desee decidir si esa aclaración ha de expresarse en el Régimen Uniforme o en una guía o comentario.

Artículo 11. Responsabilidad contractual

1) Entre una autoridad certificadora que emite un certificado y el titular de ese certificado [o toda otra parte ligada con la autoridad certificadora por una relación contractual], el acuerdo celebrado entre ellas determinará los derechos y obligaciones de las partes.

2) Sin perjuicio de lo dispuesto en el artículo 10, la autoridad certificadora podrá, mediante acuerdo, eximirse de la responsabilidad por cualquier pérdida 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 con la intención de causar un daño o temerariamente y con conocimiento de que probablemente se ocasionaría un daño.

Referencias

A/CN.437, párrs. 51 a 73 (proyecto de artículo H);
A/CN.9/WG.IV/WP.71, párrs. 70 a 72.

Observaciones

64. El párrafo 1) reafirma el principio de la autonomía de la voluntad de las partes en relación con el régimen de la responsabilidad aplicable a la autoridad certificadora. El párrafo 2) trata de la cuestión de las cláusulas de exención, que en general aceptables, con dos excepciones. La primera procede de una referencia al proyecto de artículo 10, que se propone fijar una norma mínima de la que no se puede permitir que las autoridades certificadoras se aparten (véase *supra*, párrafo 58). La segunda excepción se inspira en los Principios de UNIDROIT relativos a los contratos mercantiles internacionales (artículo 7.1.6), como un intento de brindar una norma uniforme para evaluar la aceptabilidad de las cláusulas de exención. Cabe observar que la referencia a que la limitación o la exención pueda "faltar gravemente a la equidad" sugiere un enfoque flexible para las cláusulas de exención. Ese enfoque puede llevar a un reconocimiento más amplio de las cláusulas de limitación o exención del que se daría si el Régimen Uniforme se remitiera meramente a la ley aplicable fuera del Régimen Uniforme.

65. El párrafo 3) se ocupa de la situación en que se produjese una pérdida u otro perjuicio como resultado de un comportamiento incorrecto de la autoridad certificadora o de sus representantes. La regla que se sugiere está inspirada en el texto análogo utilizado en muchas convenciones internacionales sobre transporte y recientemente en el artículo 18 de la Ley Modelo sobre transferencias internacionales de crédito.

Artículo 12. Responsabilidad de la autoridad certificadora frente a las partes que se fian de los certificados

- 1) A falta de acuerdo en contrario, la autoridad certificadora que emita un certificado responderá ante toda persona que razonablemente se fie de él por:
 - a) [incumplimiento de una garantía otorgada conforme al artículo 10][negligencia al presentar como correcta información incorrecta ofrecida en el certificado];
 - b) el pronto registro de la revocación de un certificado al recibo del aviso de su revocación; y
 - c) [las consecuencias de no][negligencia en] aplicar:
 - i) un procedimiento expresado en la declaración sobre prácticas de certificación publicada por la autoridad certificadora; o
 - ii) un procedimiento expresado en la ley aplicable.
- 2) No obstante lo dispuesto en el párrafo 1), la autoridad certificadora no será responsable si puede demostrar que ella o sus representantes adoptaron todas las medidas necesarias para evitar errores en el certificado o que les fue imposible adoptarlas;

- 3) No obstante lo dispuesto en el párrafo 1, la autoridad certificadora podrá, en el certificado [o de otra manera], limitar la finalidad para la que se pueda utilizar el certificado. No se tendrá por responsable a la autoridad certificadora de los daños y perjuicios derivados de la utilización del certificado con otra finalidad.
- 4) No obstante lo dispuesto en el párrafo 1), la autoridad certificadora podrá, en el certificado [o de otra manera], limitar el valor de las operaciones para las que es válido el certificado. No se tendrá por responsable a la autoridad certificadora de los daños y perjuicios que excedan de ese límite.

Referencias

A/CN.437, párrs. 51 a 73 (proyecto de artículo H);
A/CN.9/WG.IV/WP.71, párrs. 70 a 72.

Observaciones

66. El proyecto de artículo 12 se propone reflejar la opinión expresada en el anterior período de sesiones de que el Régimen Uniforme debería contener una norma por la que se creara una presunción simple de responsabilidad. Conforme a esa norma, por ejemplo, en caso de identificación errónea de una persona o de atribución errónea de una clave pública a una persona, la autoridad certificadora respondería por la pérdida experimentada por una parte perjudicada, a menos que pudiese demostrar que había hecho todo lo posible por evitar el error. Ese sistema de responsabilidad tiene como finalidad dar mayor protección a cualquier persona que utilice los servicios de una autoridad certificadora, sin por ello imponer a ésta una responsabilidad objetiva (véase el documento A/CN.437, párr. 58).

67. En el marco del debate sobre los proyectos de artículos 10 a 12, el Grupo de Trabajo quizá quiera examinar la cuestión de si hay que someter a límites la responsabilidad de las autoridades certificadoras y cómo se podrían establecer esos límites (véase el documento A/CN.437, párrs. 63 a 67). En su anterior período de sesiones, el Grupo de Trabajo examinó diversas sugerencias con respecto a los posibles métodos para limitar la cuantía de la responsabilidad en que pueden incurrir las autoridades certificadoras. Un enfoque posible sería determinar una cantidad fija. Otros criterios que se sugirieron se basarían en una limitación de la responsabilidad con referencia a un multiplicador de las cuotas pagadas por el suscriptor, un porcentaje del valor de la operación o un porcentaje de la pérdida real experimentada por la parte perjudicada. Se señaló, sin embargo, que los daños y perjuicios que pudiesen resultar de los actos de una autoridad certificadora no eran fácilmente cuantificables como criterio objetivo para llegar a una cuantía fija de responsabilidad. Además, el servicio prestado por una autoridad certificadora, así como los derechos que cobraba, a menudo no guardaban relación con el valor de las operaciones a las que se referían ni con los daños y perjuicios que pudiesen sufrir las partes (*ibid.*, párr. 66). En cuanto a la comparación que se sugirió entre la situación de una autoridad certificadora y la de un porteador conforme a los convenios internacionales aplicables al transporte de mercancías y al de pasajeros (*ibid.*, párr. 67), un examen preliminar de esos textos hace pensar que los límites de la responsabilidad se establecen generalmente con referencia a una cantidad fija (por ejemplo, en el caso del transporte de pasajeros), posiblemente en combinación con una referencia al valor de las mercancías que se transportan. Puede que el Grupo de Trabajo tenga que examinar esta cuestión en un futuro período de sesiones sobre la base de un ulterior estudio de la Secretaría.

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 titular identificado en el certificado y confirmación de que la persona que solicita la revocación es el titular [legítimo], o es un mandatario del titular facultado para solicitar la revocación;
- b) recibir pruebas fidedignas del fallecimiento del titular, cuando el titular es una persona física; o
- c) recibir pruebas fidedignas de que el titular ha sido disuelto o ha dejado de existir, cuando el titular es una persona jurídica.

2) El titular de un juego de claves certificado estará obligado a hacer revocar el certificado correspondiente si llegase a su conocimiento que la clave privada se ha perdido, o corre peligro o está expuesta a ser de algún modo indebidamente utilizada. El titular que, llegada esa situación, no haga revocar 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 revocar el certificado.

3) Independientemente de que el titular indicado en un 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 relevante indicado en el certificado es falso;
- b) la clave privada de la autoridad certificadora o su sistema de información estuvo expuesto de manera que afecte la fiabilidad del certificado; o
- c) la clave privada o el sistema de información del titular estuvo expuesto.

3) Al efectuar la revocación de un certificado conforme al párrafo 3), la autoridad certificadora deberá notificar al titular y a las partes que se fían del certificado 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, notificar prontamente al titular y publicar prontamente un aviso de la revocación cuando 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 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.437, párrs. 125 a 139 (proyecto de artículo F);

A/CN.9/WG.IV/WP.71, párrs. 66 a 67.

Observaciones

68. El proyecto de artículo 13 tiene por objeto reflejar las diversas opiniones expresadas en el anterior 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 ellas. Por lo que hace al momento de eficacia de la revocación, el Grupo de Trabajo tal vez desee decidir si hay que establecer una distinción entre la situación del titular y la de las demás partes dependientes (véase el documento A/CN.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 titular indicado en el certificado o una persona autorizada para actuar en nombre de ese titular.

Referencias

A/CN.437, párrs. 133 a 135 (proyecto de artículo F).

Observaciones

69. Como en su anterior período de sesiones, el Grupo de Trabajo decidió que el Régimen Uniforme contuviera una disposición sobre suspensión de certificados (véase el documento A/CN.437, párrs. 133 a 134). Por lo que se refiere a momento de eficacia 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, indicando la fecha en que se emitió cada certificado, su fecha de expiración y 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 los [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 que rijan la suspensión especificados por la autoridad certificadora en la declaración sobre prácticas de certificación aplicable.

Referencias

A/CN.437, párrs. 140 a 148 (proyecto de artículo G);
A/CN.9/WG.IV/WP.71, párrs. 68 y 69.

Observaciones

70. En el anterior período de sesiones, no se planteó ninguna objeción de principio contra la inclusión en el Régimen Uniforme de una disposición sobre el registro de certificados (véase el documento A/CN.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 un importante elemento para comprobar la fiabilidad de las firmas numéricas. Al estudiar la manera como las autoridades certificadoras deberían llevar esos registros y LRC, el Grupo de Trabajo tal vez desee examinar si las partes dependientes han de estar obligadas a verificar la situación del certificado consultando el registro o la LRC pertinente antes de poderse fiar de la validez del certificado.

71. 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 obligaciones de las partes que se fian de los certificados.

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

- [1] La autoridad certificadora sólo podrá pedir los datos que necesite para identificar al usuario.
- 2) A petición de personas jurídicas o físicas, 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) las especificaciones técnicas de la autoridad certificadora relativas al equipo de comunicaciones del usuario;
 - f) las condiciones en que la autoridad certificadora envía advertencias a los usuarios en caso de irregularidades o de algún defecto de funcionamiento del equipo de comunicaciones;
 - g) toda limitación de la responsabilidad de la autoridad certificadora;
 - h) cualquier restricción impuesta por la autoridad certificadora respecto del empleo del certificado;
 - i) las condiciones en las que el usuario tendrá derecho a imponer 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 podrá ser entregada por la autoridad 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 autoridad certificadora. Este preaviso surtirá efecto al ser recibido por la autoridad certificadora.
- 5) Con un preaviso [de tres meses], la entidad certificadora podrá dar por terminado ese mismo acuerdo. Ese preaviso surtirá efecto desde el momento de su recepción.]

Referencias

A/CN.437, párrs. 149 a 150 (proyecto de artículo J);
A/CN.9/WG.IV/WP.71, párr. 76.

Observaciones

72. En su anterior 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 el documento A/CN.437, párr. 150).

CAPÍTULO IV. RECONOCIMIENTO DE FIRMAS ELECTRÓNICAS EXTRANJERAS

Artículo 17. Autoridades certificadoras extranjeras que ofrecen servicios conforme al presente Régimen

Variante A 1) Las [personas][autoridades] 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.

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.

Variante B El (La) ... [el Estado promulgante designa el órgano o la autoridad competente para reglamentar la aprobación de certificados extranjeros] queda autorizado para aprobar certificados extranjeros y dictar normas concretas por las que se rija dicha aprobación.

Referencias

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

Observaciones

73. Al permitir que entidades extranjeras puedan establecerse como autoridades certificadoras locales, el proyecto de artículo 17 afirma simplemente el principio de que no se debe discriminar contra las entidades extranjeras. Aunque ese principio puede ser generalmente aceptado, tal vez sea particularmente pertinente expresarlo con respecto a las autoridades certificadoras, ya que cabe esperar 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

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 nacional 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.

Referencias

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

Observaciones

74. 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 garantizar así mismo su validez y vigencia. Se refiere a los asuntos denominados "certificación recíproca" en el anterior 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 el caso de que el certificado extranjero resulte defectuoso (véase el documento A/CN.437, párrs. 77 a 78).

Artículo 19. Reconocimiento de certificados extranjeros por autoridades certificadoras nacionales

1) 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 extranjera ofrezcan un grado de fiabilidad por lo menos equivalente al requerido de las autoridades certificadoras de conformidad con el presente Régimen. [Ese 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*]. [Ese reconocimiento podrá hacerse mediante una determinación publicada del Estado o mediante un acuerdo bilateral o multilateral entre los Estados interesados.]

3) Se admitirá [por parte de los tribunales y otras autoridades encargadas de averiguar los hechos] la eficacia de las firmas numéricas verificadas con referencia a un certificado emitido por una autoridad certificadora extranjera cuando el certificado sea tan fiable como corresponda a la finalidad para la cual se emitió el certificado, a la luz de todas las circunstancias.

4) Sin perjuicio de lo dispuesto en el párrafo anterior, los órganos públicos podrán hacer constar [mediante publicación] que se debe utilizar un autoridad certificadora, clase de autoridades certificadoras o clase de certificados en relación con los mensajes o las firmas presentados a esos órganos.

Referencias

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

Observaciones

75. El proyecto de artículo 19 se refiere a los asuntos denominados "reconocimiento transfronterizo" en el anterior período de sesiones del Grupo de Trabajo (véase el documento A/CN.437, párrs. 77 y 78). Los párrafos 1) y 2) tratan de las maneras de determinar la fiabilidad de los certificados y firmas extranjeros antes de efectuar una operación (y de que se suscite una controversia sobre el grado de fiabilidad de una firma). El párrafo 3) fija la norma en relación con la cual se pueden evaluar las firmas y los certificados extranjeros a falta de una previa determinación su fiabilidad. El párrafo 4) deja a salvo el derecho de los órganos públicos de determinar qué procedimientos se han de utilizar para comunicarse electrónicamente con ellos.

* * *

Notas

¹ *Documentos Oficiales de la Asamblea General, quincuagésimo primer período de sesiones, Suplemento N° 17 (A/51/71), párrs. 223 y 224.*

² *Ibid., quincuagésimo segundo período de sesiones, Suplemento N° 17 (A/52/17), párrs. 249 a 251.*