NACIONES UNIDAS **A**

Asamblea General

Distr. LIMITADA
A/CN.9/WG.IV/WP.82
29 de junio de 1999

ESPAÑOL
Original: INGLÉS

COMISIÓN DE LAS NACIONES UNIDAS PARA EL DERECHO MERCANTIL INTERNACIONAL
Grupo de Trabajo sobre Comercio Electrónico
35º período de sesiones
Viena, 6 a 17 de septiembre de 1999

PROYECTO DE RÉGIMEN UNIFORME PARA LAS FIRMAS ELECTRÓNICAS

Nota de la Secretaría

ÍNDICE

V.99-85659

INTRODUCCIÓN

1. La Comisión, en su 29º período de sesiones (1996), decidió incluir en su programa las cuestiones de las firmas numéricas y las entidades certificadoras. Se pidió al Grupo de Trabajo que examinara la conveniencia y la viabilidad de preparar un régimen uniforme sobre estos temas. Se acordó que el régimen uniforme que se preparase debía ocuparse de cuestiones como: el fundamento jurídico en que se apoyaban los procesos de certificación, inclusive la tecnología emergente de autenticación y certificación digitales; la aplicabilidad del proceso de certificación; la asignación del riesgo y las responsabilidades de los usuarios, proveedores y terceros en el contexto de la utilización de técnicas de certificación; las cuestiones específicas de la certificación mediante el uso de registros; y la incorporación por remisión[1].

2. En su 30º período de sesiones (1997), la Comisión tuvo ante sí el informe del Grupo de Trabajo sobre la labor de su 31º período de sesiones (A/CN.9/437). El Grupo de Trabajo indicaba a la Comisión que había llegado a un consenso sobre la importancia y la necesidad de trabajar hacia la armonización del derecho en ese ámbito. Aunque no hubo ninguna decisión firme sobre la forma y el contenido de esa labor, el Grupo de Trabajo había llegado a la conclusión preliminar de que era posible emprender la preparación de un proyecto de régimen uniforme, por lo menos sobre las cuestiones de las firmas numéricas y las entidades certificadoras, y posiblemente sobre asuntos conexos. El Grupo de Trabajo recordó que, junto con las firmas numéricas y las entidades certificadoras, la futura labor en el ámbito del comercio electrónico podría tener también que referirse a: cuestiones relativas a las técnicas alternativas a la criptografía de clave pública; cuestiones generales de funciones desempeñadas por proveedores de servicios como terceros; y contratación electrónica (A/CN.9/437, párrs. 156 y 157).

3. La Comisión hizo suyas las conclusiones acordadas por el Grupo de Trabajo y encargó a éste la preparación de un régimen uniforme para las firmas numéricas y para las entidades certificadoras (en adelante denominado "el Régimen Uniforme"). Con respecto al alcance exacto y la forma del Régimen Uniforme, la Comisión convino en general en que no se podía adoptar ninguna decisión en esta etapa inicial del proceso. Se juzgó que, mientras que el Grupo de Trabajo podía concentrar adecuadamente su atención sobre las cuestiones de las firmas numéricas en vista del papel aparentemente predominante desempeñado por la criptografía de clave pública en la práctica emergente del comercio electrónico, el Régimen Uniforme debía ser coherente con la neutralidad respecto de los medios técnicos utilizados por la CNUDMI en materia de comercio electrónico (en adelante denominada Ley Modelo). Así pues, el Régimen Uniforme no debería desalentar la utilización de otras técnicas de autenticación. Además, al ocuparse de la criptografía de clave pública, el Régimen Uniforme podría tener que admitir diversos niveles de seguridad y reconocer los diferentes efectos jurídicos y niveles de fiabilidad correspondientes a los diversos tipos de servicios prestados en el contexto de las firmas numéricas. Con respecto a las entidades certificadoras, si bien la Comisión reconocía el valor de las normas orientadas por el mercado, se estimó en general adecuado que el Grupo de Trabajo previera la creación de un conjunto de reglas mínimas que deberían cumplir las entidades certificadoras, en particular cuando se procurara obtener una certificación transfronteriza[2].

4. El Grupo de Trabajo inició la preparación del Régimen Uniforme en su 32º período de sesiones sobre la base de una nota preparada por la Secretaría (A/CN.9/WG.IV/WP.73).

5. En su 31º período de sesiones (1998), la Comisión tuvo ante sí el informe del Grupo de Trabajo acerca de la labor de su 32º período de sesiones (A/CN.9/446). Se observó que el Grupo de Trabajo, a lo largo de sus períodos de sesiones 31º y 32º, había tropezado con dificultades manifiestas en alcanzar un entendimiento común de las nuevas cuestiones jurídicas que planteaba el uso cada vez mayor de las firmas numéricas y otras firmas electrónicas. También se observó que no se había llegado aún a un consenso sobre cómo ocuparse de estas cuestiones en un marco jurídico internacionalmente aceptable. La Comisión estimó, no obstante, que los progresos realizados hasta el momento indicaban que el Régimen Uniforme para las Firmas Electrónicas iba tomando forma y convirtiéndose en una estructura eficaz. La Comisión reafirmó la decisión adoptada en su 30º período de sesiones acerca de la viabilidad de preparar ese Régimen Uniforme y expresó su confianza en que el Grupo de Trabajo podía hacer más progresos en su 33º período de sesiones sobre la base del proyecto revisado preparado por la Secretaría

(A/CN.9/WG.IV/WP.76). En el contexto de ese debate, la Comisión observó con satisfacción que el Grupo de Trabajo había llegado a ser generalmente reconocido como un foro internacional particularmente importante para el intercambio de pareceres acerca de las cuestiones jurídicas del comercio electrónico y para la preparación de soluciones a esas cuestiones[3].

6. En su 32º período de sesiones (1999), la Comisión tuvo ante sí el informe del Grupo de Trabajo acerca de la labor de sus períodos de sesiones 33º (julio de 1998) y 34º (febrero de 1999) (A/CN.9/454 y 457). La Comisión expresó su agradecimiento por los esfuerzos desplegados por el Grupo de Trabajo con miras a preparar el proyecto de régimen uniforme para las firmas electrónicas. Si bien en general se convino en que durante esos períodos de sesiones se habían logrado progresos considerables en la comprensión de las cuestiones jurídicas relativas a las firmas electrónicas, también se estimó que el Grupo de Trabajo había afrontado dificultades para formar un consenso con respecto a la política legislativa en que debía basarse el régimen uniforme.

7. Se expresó la opinión de que el enfoque que actualmente adoptaba el Grupo de Trabajo no reflejaba en forma suficiente la necesidad comercial de flexibilidad en la utilización de las firmas electrónicas y otras técnicas de autenticación. El régimen uniforme, tal como ahora lo concebía el Grupo de Trabajo hacía demasiado hincapié en las técnicas de la firma numérica y, en el ámbito de la firma numérica, en una aplicación específica de ésta que requería la certificación de terceros. Por tanto, se sugirió que la labor del Grupo de Trabajo respecto de las firmas electrónicas se limitase a las cuestiones jurídicas de la certificación de validez transfronteriza o se aplazara completamente hasta que las prácticas del mercado se hubiesen establecido con mayor claridad. Se expresó una opinión conexa en el sentido de que, para los fines del comercio internacional, casi todas las cuestiones jurídicas emanadas de la utilización de las firmas electrónicas ya estaban resueltas en la Ley Modelo de la CNUDMI sobre Comercio Electrónico. Si bien se requería cierto grado de reglamentación con respecto a algunos usos de las firmas electrónicas que rebasaban el ámbito del derecho comercial, el Grupo de Trabajo no debía desempeñar ninguna función de reglamentación.

8. Según la opinión ampliamente predominante, el Grupo de Trabajo debía continuar su tarea sobre la base de su mandato original (véase el párr. 3 *supra*). Con respecto a la necesidad de contar con un régimen uniforme para las firmas electrónicas, se explicó que en muchos países las autoridades gubernamentales y legislativas que estaban preparando legislación sobre cuestiones relativas a las firmas electrónicas, incluido el establecimiento de infraestructuras de clave pública (ICP) u otros proyectos sobre cuestiones estrechamente relacionadas con éstas (véase A/CN.9/457, párr. 16), esperaban que la CNUDMI les brindara orientación. En cuanto a la decisión adoptada por el Grupo de Trabajo de concentrarse en las cuestiones y la terminología relativas a las ICP, se recordó que si bien la interacción de relaciones entre los tres tipos de partes distintas (a saber, los titulares de las claves, las entidades certificadores y las partes confiantes) correspondía a un posible modelo de ICP, otros modelos eran concebibles, por ejemplo, cuando no participara una entidad certificadora independiente. Una de las principales ventajas que podrían obtenerse si se centrara la atención en las cuestiones relativas a las ICP era facilitar la estructuración del régimen uniforme mediante la referencia a tres funciones (o papeles) con respecto a los pares de claves, a saber, la función del emisor (o suscriptor) de la clave, la función de certificación y la función de confianza. Se convino en general en que esas tres funciones eran comunes a todos los modelos de ICP. Se convino también en que las tres funciones debían abordarse sin perjuicio de que las desempeñasen tres entidades distintas o de que dos de esas funciones las desempeñase la misma persona (por ejemplo, cuando la entidad certificadora fuese asimismo parte confiante). Además, se estimó en general que al centrar la atención en las funciones típicas de las ICP y no en un determinado modelo podría facilitarse la elaboración de una norma plenamente neutral respecto de los medios en una etapa ulterior (ibíd., párr. 68).

9. Tras un debate, la comisión reafirmó sus decisiones anteriores en cuanto a la viabilidad de preparar un régimen uniforme (véase *supra*, párrs. 3 y 5) y se declaró segura de que el Grupo de Trabajo realizaría progresos aun mayores en sus próximos períodos de sesiones.

10. La presente nota contiene los proyectos de artículo revisados a la luz de las deliberaciones y decisiones del propio Grupo de Trabajo, así como de la Comisión en su 32º período de sesiones, anteriormente reseñadas. La finalidad del texto revisado es la de reflejar las decisiones del Grupo de Trabajo en su 34º período de sesiones. Las disposiciones nuevamente revisadas figuran subrayadas.

11. De conformidad con las instrucciones relativas a la limitación y al estricto control de la documentación de Naciones Unidas, se ha procurado reducir en lo posible las observaciones explicativas de los proyectos de artículo. Durante la reunión se darán verbalmente otras explicaciones adicionales.

Referencias a legislación nacional y a otros textos

12. A efectos de información y comparación se incluyen en este párrafo referencias en pequeña tipografía a legislación nacional y a otros textos en relación con varios artículos. Se mencionan a continuación las leyes de las que tiene conocimiento la Secretaría y de cuyos textos ha podido disponer. Otros textos se citan por haber sido concertados por organizaciones internacionales o por tener una amplia difusión y estar disponibles para el público. Las abreviaturas remiten a los siguientes instrumentos legislativos y textos:

-	Alemania	Ley de firmas numéricas de 1997 (artículo 3, Ley de servicios de información y comunicación, aprobada el 13 de junio de 1997 y vigente desde el 1º de agosto de 1997);
-	Illinois	Estados Unidos de América, *Electronic Commerce Security Act 1998, (1997 Illinois House Bill 3180; 5 Ill. Comp. Stat. 175*, promulgada en agosto de 1998);
-	Minnesota	Estados Unidos de América, *Electronic Authentication Act (Minnesota Statutes §325*, promulgada en mayo de 1997);
-	Missouri	Estados Unidos de América, *Digital Signature Act, 1998 (1998 SB 680*, promulgada en julio de 1998);
-	Singapur	*Electronic Transactions Act 1998*, Ley Nº 25 de 1998.
-	Directrices de la Asociación de Abogados de los Estados Unidos (ABA)	*American Bar Association, Science and Technology Section, "Digital Signature, Guidelines" 1996*;
-	Proyecto de directiva de la CE	Proyecto de directiva del Parlamento Europeo y del Consejo acerca de un marco común para las firmas electrónicas, 1999 (7015/99);
-	GUIDEC	Cámara de Comercio Internacional, "Uso general en el comercio internacional asegurado digitalmente", 1997.

I. OBSERVACIONES GENERALES

13. La finalidad del Régimen Uniforme reflejada en los proyectos de artículo presentados en la parte II de la presente nota, es facilitar el creciente empleo que se hace de las firmas electrónicas en las operaciones comerciales internacionales. Inspirándose en los muchos instrumentos legales ya en vigor o que se están preparando en cierto número de países, el presente régimen quisiera prevenir toda eventual falta de armonía en el régimen aplicable al

comercio electrónico sentando una serie de pautas sobre el fundamento para que se reconozca la validez jurídica de las firmas numéricas y demás firmas electrónicas, con la asistencia eventual de entidades certificadoras, para las cuales se ha preparado también cierto número de reglas básicas.

14. Al haber centrado su atención en los aspectos de derecho privado de las obligaciones comerciales, el Régimen Uniforme no trata de resolver todas las cuestiones que puedan ir surgiendo en el contexto de un empleo más difundido de la firma electrónica. En particular, el Régimen Uniforme no trata de todos los aspectos de orden público, de derecho administrativo, de legislación protectora del consumidor o de derecho penal que el legislador deberá probablemente tener en cuenta al preparar un marco jurídico interno general para la firma electrónica.

15. Al haber adoptado como base la Ley Modelo, el Régimen Uniforme trata de reflejar en particular: el principio de la neutralidad respecto de los medios técnicos utilizados; el criterio de la no discriminación de todo equivalente funcional de los conceptos y prácticas que tradicionalmente funcionan sobre soporte de papel; y una amplia confianza en la autonomía contractual de las partes. El proyecto de Régimen ha sido concebido para ser utilizado como marco normativo mínimo en un entorno "abierto" (es decir, un entorno en el que las partes negocien por vía electrónica sin acuerdo previo) y como reglas de derecho supletorio en un entorno "cerrado" (es decir, un entorno en el que las partes estén obligadas por reglas contractuales y procedimientos previamente estipulados que habrán de ser respetados al negociar por vía electrónica).

16. Al considerar los proyectos de artículo propuestos para ser incluidos en el Régimen Uniforme, el Grupo de Trabajo tal vez desee considerar desde una perspectiva más general la relación entre el Régimen Uniforme y la Ley Modelo. Este proyecto de Régimen Uniforme se ha preparado con el criterio de que constituya un instrumento aparte. Se han incorporado al proyecto dos artículos recientemente agregados que reflejan disposiciones de la Ley Modelo: los artículos 1 (Ámbito de aplicación) y 4 (Interpretación). Las transacciones con consumidores no se han excluido explícitamente del ámbito de aplicación del Régimen Uniforme, pero en el proyecto de artículo 1 se ha incluido la nota de pie de página que figura en la Ley Modelo para dejar claro que el Régimen Uniforme no debe prevalecer sobre ninguna disposición de derecho nacional a cuestiones de protección del consumidor.

17. El Grupo de Trabajo tal vez desee considerar si un preámbulo aclararía la finalidad por la que se desea introducir el Régimen Uniforme, a saber, la de promover una utilización eficiente de las vías electrónicas de negociación al establecer un marco de seguridad y al atribuir al mensaje escrito y al mensaje electrónico idéntica consideración en lo que respecta a su validez jurídica.

18. En su 33º período de sesiones, el Grupo de Trabajo expresó dudas sobre la idoneidad de los términos "refrendada" o "segura", con los que se describían ciertas técnicas de firma que permitirían dar una fiabilidad mayor que la de una "firma electrónica" en general (A/CN.9/454, párr. 29). El Grupo de Trabajo concluyó que, en ausencia de un término más apropiado, se retuviera el término "refrendada". En el 34º período de sesiones (A/CN.9/457, párr.39) se sugirió que tal vez hubiera que reexaminar la definición "firma electrónica refrendada", junto con la arquitectura general del Régimen Uniforme, una vez aclarado el propósito de ocuparse de dos categorías de firmas electrónicas, en particular por lo que se refiere a los efectos jurídicos de ambos tipos de firmas. Se sostuvo que la regulación de las firmas electrónicas que ofrecían un elevado grado de fiabilidad sólo se justificaba si el Régimen Uniforme hubiese de proporcionar un equivalente funcional a usos específicos de firmas manuscritas. Si ello hubiese de resultar particularmente difícil a nivel internacional, ofreciendo al mismo tiempo escaso interés para las operaciones comerciales internacionales, convendría tal vez aclarar el beneficio adicional que cabría esperar de utilizar una "firma electrónica refrendada" por oposición a una simple "firma electrónica".

19. Ante el debate sobre la necesidad de una categoría de "firmas electrónicas refrendadas", el presente proyecto revisado de Régimen Uniforme ofrece otro posible enfoque para el debate en el Grupo de Trabajo. La definición de la "firma electrónica refrendada" en el proyecto de artículo 2 b) se ha puesto entre corchetes. Las observaciones relativas a una posible enmienda de la definición se han incluido en el marco del artículo 2. En los artículos 6, 7 y

8 del proyecto figuran las partes pertinentes de esa definición como posibles disposiciones de fondo. La finalidad de esta otra opción es ayudar al Grupo de Trabajo a decidir si es conveniente eliminar las referencias a las firmas electrónicas y a las firmas electrónicas refrendadas de modo que el Régimen Uniforme regule sólo una única categoría de firmas electrónicas. Las observaciones sobre propuestas concretas se comentan en los párrafos correspondientes a los respectivos artículos.

20. El presente proyecto revisado prevé que la aplicación del Régimen Uniforme vaya más allá de la situación en que haya requisitos jurídicos de forma o en que la ley prevea consecuencias en ausencia de ciertas condiciones, como la firma o el original. De este modo, el alcance del Régimen Uniforme es potencialmente más amplio que el de la Ley Modelo, si bien el proyecto de artículo 6 no incluye el requisito de forma que recoge el artículo 7 de la Ley Modelo. El Grupo de Trabajo tal vez desee estudiar la posibilidad de dar al Régimen Uniforme esta aplicación más amplia.

II. PROYECTOS DE ARTÍCULO SOBRE LAS FIRMAS ELECTRÓNICAS

Artículo 1. Ámbito de aplicación

El presente Régimen se aplicará a las firmas electrónicas utilizadas en el contexto de las relaciones comerciales* y no derogará las leyes destinadas a la protección del consumidor.

* El término "comercial" deberá ser interpretado ampliamente de forma que abarque las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual. Las relaciones de índole comercial comprenden, sin limitarse a ellas, las operaciones siguientes: toda operación comercial de suministro o intercambio de bienes o servicios; todo acuerdo de distribución; toda operación de representación o mandato comercial; de facturaje ("factoring"); de arrendamiento de bienes de equipo con opción de compra ("leasing"); de construcción de obras; de consultoría; de ingeniería; de concesión de licencias; de inversión; de financiación; de banca; de seguros; todo acuerdo de concesión o explotación de un servicio público; de empresa conjunta y otras formas de cooperación industrial o comercial; de transporte de mercancías o de pasajeros por vía aérea, marítima y férrea, o por carretera.

Referencias a documentos de la CNUDMI

A/CN.9/457, párrs. 53 a 64

Observaciones

21. Inicialmente, el proyecto de artículo 1 fue propuesto en el 34º período de sesiones del Grupo de Trabajo como párrafo 1) de un artículo relativo a la autonomía de las partes (proyecto de artículo E, A/CN.9/457, párrs. 55 y 60). Dado que esa disposición regulaba más bien cuestiones de ámbito de aplicación del Régimen Uniforme, ha sido incluida en este proyecto como artículo aparte bajo el título “ámbito de aplicación”. Conforme a lo convenido por el Grupo de Trabajo (A/CN.9/457, párr. 64), el proyecto de artículo 1 incluye una nota de pie de página en la que se repite la definición del término “comercial” que figura en el artículo 1 de la Ley Modelo sobre Comercio Electrónico, adoptando los términos de la nota de pie de página** de la Ley Modelo relativa a la cuestión de los consumidores. Se han agregado al artículo las palabras “firmas electrónicas utilizadas en el contexto de”, a fin de definir con mayor precisión la temática básica del Régimen Uniforme.

Artículo 2. Definiciones

Para los fines del presente Régimen:

a) Por "firma electrónica" se entenderá [los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, y] [todo método relacionado con un mensaje de datos] que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos e indicar que el titular de la firma aprueba la información contenida en el mensaje de datos;

[b) Por "firma electrónica refrendada" se entenderá una firma electrónica respecto de la cual se pueda demostrar, mediante la aplicación de un [procedimiento de seguridad] [método], que esa firma electrónica:

i) es exclusiva del titular de la firma [para los fines para los] [en el contexto en el] que se utilice;

ii) ha sido creada y consignada en el mensaje de datos por el titular de la firma o utilizando un medio bajo el control exclusivo del titular de la firma [y por ninguna otra persona];

[iii) ha sido creada y está vinculada al mensaje de datos al que se refiere de forma que garantice con fiabilidad la integridad de dichos mensaje";]]

c) Por "certificado" se entenderá todo mensaje de datos que sea emitido por el certificador de información con la intención de comprobar la identidad de una persona o entidad en cuyo poder obre un determinado [juego de claves] [dispositivo de firma];

d) Por "mensaje de datos" se entenderá la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax;

e) Por "titular de la firma" [titular del dispositivo] [suscriptor] [titular del dispositivo] [firmante] [signatario] se entenderá la persona que pueda crear y adjuntar a un mensaje de datos, o en cuyo nombre se puede crear o adjuntar a un mensaje de datos, una firma electrónica refrendada.

f) Por "certificador de información" se entenderá a toda persona o entidad que, en el curso habitual de su negocio, proporcione [servicios de identificación] [información de certificación] que se [utilicen] [utilice] para apoyar la utilización de firmas electrónicas [refrendadas].

Referencias a documentos de la CNUDMI

A/CN.9/457, párrs. 22 a 47, 66 y 67; 89; 109;
A/CN.9/WG.IV/WP.80, párrs. 7 a 10;
A/CN.9/WG.IV/WP.79, párr. 21;
A/CN.9/454, párr. 20;
A/CN.9/WG.IV/WP.76, párrs. 16 a 20;
A/CN.9/446, párrs. 27 a 46 (proyecto de artículo 1), 62 a 70 (proyecto de artículo 4), 113 a 131 (proyecto de artículo 8), 132 y 133 (proyecto de artículo 9);
A/CN.9/WG.IV/WP.73, párrs. 16 a 27, 37 y 38, 50 a 57 y 58 a 60;
A/CN.9/437, párrs. 29 a 50 y 90 a 113 (proyectos de artículo A, B y C); y
A/CN.9/WG.IV/WP.71, párrs. 52 a 60.

Observaciones

Definición de “firma electrónica”

22. La definición de firma electrónica ha sido revisada de conformidad con la decisión adoptada por el Grupo de Trabajo en su 34º período de sesiones (A/CN.9/457, párrs. 23 a 32). Las palabras que figuran entre corchetes (“[todo método relacionado con un mensaje de datos]”) han sido incluidas en el texto para ajustar los términos de la definición en el Régimen Uniforme con la del artículo 7 de la Ley Modelo.

Definición de “firma electrónica refrendada”

23. De conformidad con la decisión adoptada por el Grupo de Trabajo en su 34º período de sesiones (A/CN.9/457, párr. 39), se ha revisado la definición de “firma electrónica refrendada”, incluyendo en el apartado iii) del párrafo b) el texto entre corchetes como vínculo necesario entre la firma refrendada que figura en el mensaje de datos y la información recogida en dicho mensaje, en forma de función de integridad. El Grupo de Trabajo tal vez desee examinar si el concepto de integridad debe incorporarse a la definición de firma electrónica refrendada o si guarda una mayor relación con la idea de un original, como en el artículo 8 de la Ley Modelo y en el proyecto de artículo 7 del presente Régimen Uniforme. En esta revisión se ha omitido el texto que figuraba anteriormente en el apartado ii) (“se pueda utilizar para identificar objetivamente al titular de la firma en relación con el mensaje de datos”), dado que forma parte de la definición de “firma electrónica” del párrafo a).

24. En las palabras iniciales del párrafo b) se ha agregado la palabra “método” como alternativa a “procedimiento de seguridad” para armonizar más la terminología con la de la Ley Modelo.

25. En el apartado ii) del párrafo b) se han puesto entre corchetes las palabras “y por ninguna otra persona” debido a que su inclusión en el texto plantea una serie de problemas. En primer lugar, al incluirse esas palabras en la definición de firma electrónica refrendada se puede dar a entender que toda firma no creada y adjuntada por el titular de la firma (y por lo tanto potencialmente no autorizada) no es una firma electrónica refrendada. Con esta interpretación, estas firmas pueden quedar excluidas del ámbito de aplicación de algunos artículos del proyecto de Régimen Uniforme, por ejemplo, de los artículos 8, 9 y 10. En particular, podría resultar incierta la aplicación de las partes del proyecto de artículo 9 que regulan la responsabilidad en caso de que los dispositivos de firmas estén en entredicho.

26. En segundo lugar, la inclusión de esas palabras en el texto requeriría que, a fin de que un procedimiento de seguridad o un método constituyera una firma electrónica refrendada, pudiera demostrarse que la firma era realmente creada y adjuntada por el titular de la firma. Dado que para algunas tecnologías puede ocurrir que no sea posible, la inclusión de ese requisito en el texto puede dar a entender que es necesario utilizar un identificador personal, como un método de biométrica o alguna otra técnica similar, junto con el dispositivo para firmas.

27. Otra cuestión que el Grupo de Trabajo tal vez desee examinar en el contexto del apartado ii) del párrafo b) es la relación entre el requisito de “control exclusivo” y la disposición del párrafo 2) del proyecto de artículo 9 que prevé un control conjunto. Esta cuestión también se plantea en relación con la definición de “titular de la firma”, que figura más adelante.

28. En el apartado iii) del párrafo b) se han sustituido las palabras “garantice razonablemente” por las palabras “garantice con fiabilidad”, a fin de mantener la coherencia con la terminología del artículo 8 de la Ley Modelo.

Definición de “certificado”

29. La definición de “certificado” se ha incluido en el Régimen Uniforme con el fin de completar sus disposiciones. Esta definición se basa en la definición de “certificado de identificación” que figura en el documento A/CN.9/WG.IV/WP.79, aunque en el presente Régimen Uniforme ya no se describa como “certificado de identificación”. El Grupo de Trabajo tal vez desee examinar si las palabras “o alguna otra característica importante”, que figuran entre corchetes, pueden suprimirse por la razón que se expone a continuación. El concepto de identidad puede ser más que una referencia al nombre del titular de la firma y puede aludir a otras características importantes, como su posición o autoridad, ya sea en combinación con un nombre o sin hacer referencia a él. De este modo, no sería necesario distinguir entre la identidad y otras características importantes ni limitar el Régimen Uniforme a las situaciones en que sólo se utilizaran certificados de identificación que mencionaran al titular de la firma. Sobre el significado de “identificación” puede leerse otro criterio en el documento de trabajo del curso práctico conjunto OCDE-sector privado sobre autenticación electrónica celebrado en California del 2 al 4 de junio de 1999 (véase “Background Paper on Electronic Authentication Technologies and Issues” págs. 6 a 9).

30. El Grupo de Trabajo tal vez desee examinar si las palabras “confirmar la identidad” son apropiadas, teniendo en cuenta que de hecho con el certificado no se confirma la identidad del titular de la firma sino que más bien se identifica a éste siguiendo ciertos procedimientos y se certifica que esa identidad guarda relación con el dispositivo de firma o con la clave pública que se mencionan en el certificado. A fin de asegurar que el Régimen Uniforme sea neutral con respecto a la tecnología, el Grupo de Trabajo tal vez desee plantearse la sustitución de las palabras “juego de claves” por una expresión más neutral con respecto a la tecnología como “dispositivo de firma”, ya que “juego de claves” se refiere específicamente a las firmas numéricas. La utilización de las palabras “juego de claves” en relación con la definición de “certificado” puede ser apropiada en situaciones en que los certificados se utilicen únicamente en el contexto de una firma numérica.

Definición de “mensaje de datos”

31. La definición de “mensaje de datos” se ha incluido en el proyecto de Régimen Uniforme con el fin de completar sus disposiciones. El Grupo de Trabajo tal vez desee plantearse la necesidad de incluir esta definición en el contexto de la relación del Régimen Uniforme con la Ley Modelo.

Definición de “titular de la firma”

32. El Grupo de Trabajo no concluyó su debate sobre la definición de “titular de la firma” en su 34º período de sesiones (A/CN.9/457, para. 47). En la actual definición revisada figuran entre corchetes diversos términos que, a juicio del Grupo de Trabajo, podrían ser más apropiados que “titular de la firma”. Es posible que deba revisarse esa definición en el contexto del apartado ii) del párrafo b) de la definición de “firma electrónica refrendada “ y del proyecto de artículo 9 2), como se señala en el párrafo 27.

Definición de “certificador de información”

33. Esta definición no fue examinada por el Grupo de Trabajo en su anterior período de sesiones y sigue sin cambios. No obstante, habida cuenta de anteriores debates (A/CN.9/457, para. 109), el Grupo de Trabajo tal vez desee examinar si las palabras “en el curso habitual de su negocio”, que figuran en la definición de “certificador de información”, deben interpretarse en el sentido de que las actividades relacionadas con la certificación deben ser la actividad exclusiva del certificador de información o si, a fin de abarcar las situaciones en que las empresas de tarjetas de crédito emiten certificados, debe quedar comprendida también la cuestión de los certificados como parte secundaria de la actividad de una entidad.

Referencias a legislación nacional y a otros textos

Directrices de la Asociación de Abogados de los Estados Unidos (ABA)

Primera parte: Definiciones
1.5 Certificado
Mensaje que al menos
1) identifica a la autoridad certificadora que lo emite;
2) nombra o identifica a su suscriptor;
3) contiene la clave pública del suscriptor;
4) especifica el período de validez; y
5) está firmado numéricamente por la autoridad certificadora que lo emite.

1.6 Autoridad certificadora
Persona que expide un certificado.

1.27 Parte que confía
Persona que ha recibido un certificado y una firma numérica verificable con una referencia a una clave pública consignada en el certificado y que está en condiciones de confiar en el certificado y en la firma.

1.30 Firmante
Persona que crea una firma numérica para un mensaje.

1.31 Suscriptor
Persona que
1) es la persona nombrada o identificada en un certificado expedido para ella, y que
2) dispone de una clave privada que corresponde a una clave pública consignada en ese certificado.

Proyecto de Directiva de la Comunidad Europea

Artículo 2
Definiciones
Para los fines de la presente Directiva:
1. Por "firma electrónica" se entenderá los datos en forma electrónica adjuntados o lógicamente asociados a otros datos electrónicos que sirven como método de autenticación.
1a) Por "firma electrónica avanzada" se entenderá la firma electrónica que cumple los siguientes criterios:
a) tiene una relación singular con el signatario;
b) puede identificar al signatario;
c) es creada con medios que el signatario puede mantener bajo su control exclusivo; y
d) está vinculada a los datos con los que guarda relación de tal modo que puede detectarse cualquier cambio ulterior de los datos.
2. Por "signatario" se entenderá la persona que posee un dispositivo para la creación de firmas y que actúa en su nombre o en nombre de la persona o entidad que representa.
3. Por "datos de creación de firmas" se entenderá los datos singulares, como códigos o claves criptográficas privadas, que utiliza el signatario para crear una firma electrónica.
3a) Por "dispositivo para la creación de firmas" se entenderá un dispositivo configurado con dotación lógica o física para ejecutar los datos de creación de firmas.
3 b) Por "dispositivo para la creación segura de firmas" se entenderá un dispositivo para la creación de firmas que cumple los requisitos del anexo III.
4. Por "datos de verificación de firmas" se entenderán datos como códigos o claves criptográficas públicas que se utilizan para verificar la firma electrónica.
4 a) Por "dispositivo de verificación de firmas" se entenderá un dispositivo configurado con dotación lógica o física para ejecutar los datos de verificación de firmas.
4 b) Por "certificado" se entenderá una prueba electrónica que vincula unos datos de verificación de firmas a una persona y confirma la identidad de esa persona.
5. [...]

6. Por "proveedor de servicios de certificación" se entenderá una persona o entidad que emite certificados o presta otros servicios relacionados con firmas electrónicas.

Alemania

§2 Definiciones
1) A efectos de la presente ley, se entenderá por firma numérica el sello sobre datos numéricos creados con una clave privada que, utilizado conjuntamente con una clave pública conexa a la que se adjunta un certificado de clave criptográfica de un certificador o de la autoridad prevista en el párrafo 3, permite identificar al titular de la clave y verificar la autenticidad de los datos.
2) A efectos de la presente ley, se entenderá por certificador toda persona física o jurídica que certifique la atribución de claves criptográficas públicas a personas físicas y disponga para tal fin de la licencia prevista en el párrafo 4.
3) A efectos de la presente ley, se entenderá por certificado toda prueba numérica relativa a la atribución de una clave criptográfica pública a una persona física a la que se adjunta una firma numérica (certificado de clave criptográfica), o una prueba numérica especial que remita inequívocamente a un certificado de clave criptográfica y contenga demás información (certificado de atribución).

GUIDEC

VI. Glosario de términos
2. Certificado
Mensaje asegurado por una persona que certifica la exactitud de los hechos de interés para los efectos jurídicos del acto de otra persona.

4. Certificador
Persona que emite un certificado con el que da fe de la exactitud de un hecho de interés para los efectos jurídicos del acto de otra persona.

12. Certificado de clave pública
Certificado que identifica una clave pública con su suscriptor, que corresponde a una clave privada en poder de dicho suscriptor.

14. Suscriptor
Persona que es objeto de un certificado.

Illinois

Artículo 5. Registros y firmas electrónicas en general
Sección 5-105. Definiciones
Por "certificado" se entenderá todo registro que por lo menos: a) identifique la autoridad certificadora que lo emite; b) nombre o especifique de otro modo a su suscriptor, o el dispositivo o agente electrónico bajo control del suscriptor; c) contenga una clave pública que corresponda a la clave privada bajo control del suscriptor; d) especifique su período de validez; y e) esté firmado numéricamente por la autoridad certificadora que lo emite.

Por "autoridad certificadora" se entenderá la persona que autoriza o tramita la expedición de un certificado.

Por "firma electrónica" se entenderá la firma en forma electrónica adjuntada o lógicamente asociada a un registro electrónico.

Por "dispositivo de firma" se entenderá toda información singular, como códigos, algoritmos, letras, cifras, claves privadas, o números de identificación personal (PINS), o todo dispositivo físico de configuración singular, que sea requisito único o que se requiera junto con otra información u otros dispositivos para crear una firma electrónica atribuible a una determinada persona.

Singapur

Primera parte. Sección 2. Interpretación
Por "certificado" se entenderá un registro emitido con miras a apoyar firmas numéricas destinadas a confirmar la identidad u otras características importantes de la persona en cuyo poder obre un juego de claves;

Por "autoridad certificadora" se entenderá la persona u organización que expide un certificado;

Por "firma electrónica" se entenderá las letras, caracteres, cifras u otros símbolos en forma digital adjuntados o lógicamente asociados a un registro electrónico, y ejecutados o adoptados con la intención de autenticar o aprobar el registro electrónico;

Por "juego de claves" se entenderá, en un criptosistema asimétrico, una clave privada y su clave pública con la que esté matemáticamente relacionada, con la propiedad de que la clave pública puede verificar la firma numérica que la clave privada cree;

Por "clave privada" se entenderá la clave o el juego de claves utilizado para crear una firma numérica;

Por “suscriptor” se entenderá la persona nombrada o identificada en un certificado expedido a su favor y que está en posesión de una clave privada que corresponde a una clave pública consignada en dicho certificado.

Artículo 3. [No discriminación] [Neutralidad respecto de la tecnología]

[Ninguna de las disposiciones del presente Régimen se aplicará] [Las disposiciones del presente Régimen no se aplicarán] de modo que excluya(n), restrinja(n) o prive(n) de efecto jurídico cualquier método [de firma] que cumpla los requisitos de [*del artículo 7 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico*].

Referencias a documentos de la CNUDMI

A/CN.9/457, párrs. 53 a 64

Observaciones

34. El proyecto de artículo 2 fue inicialmente propuesto en el 34º período de sesiones del Grupo de Trabajo como párrafo 3) de un artículo relativo a la autonomía de las partes (proyecto de artículo E, A/CN.9/457, párrs. 55 y 60). Dado que el párrafo 3) regulaba, más que la autonomía de las partes, las cuestiones de la no discriminación y la neutralidad respecto de la tecnología, se ha incluido en el presente proyecto como artículo aparte con los títulos “no discriminación” o “neutralidad respecto de la tecnología”. Las palabras “excluya, restrinja o discrimine” se han sustituido por las palabras “excluya, restrinja o prive de efecto jurídico” para describir con mayor precisión el propósito y el objeto de esta disposición. La referencia al artículo 7 de la Ley Modelo sobre Comercio Electrónico sería una referencia a dicha Ley Modelo incorporada a la legislación nacional.

Artículo 4. Interpretación

1) En la interpretación del presente Régimen Uniforme habrán de tenerse en cuenta su origen internacional y la necesidad de promover la uniformidad de su aplicación y la observancia de la buena fe en el comercio electrónico.

2) Las cuestiones relativas a materias que se rijan por el presente Régimen Uniforme y que no estén expresamente resueltas en él serán dirimidas de conformidad con los principios generales en que se inspira el Régimen Uniforme.

Observaciones

35. El proyecto de artículo 3 sigue el texto del artículo 3 de la Ley Modelo sobre Comercio Electrónico, añadiéndole las palabras “en el comercio electrónico”, y se incluye aquí para completar las disposiciones. El Grupo de Trabajo tal vez desee plantearse la cuestión de si el Régimen Uniforme debe completarse como texto independiente de la Ley Modelo, aunque mantenga una clara relación con ella. En caso de que el Grupo de Trabajo lo decida así, el artículo 3 puede ofrecer orientación a los tribunales y a otras autoridades nacionales o locales para la interpretación del Régimen Uniforme. El efecto previsto del artículo 3 sería promover la interpretación del texto uniforme, una vez incorporado a la legislación local, haciendo referencia a su carácter y a sus orígenes internacionales más que a los conceptos de la legislación local.

Artículo 5. Modificación mediante acuerdo

Variante A

[Las partes podrán convenir, expresa o implícitamente, en apartarse de algún aspecto del presente Régimen o en modificarlo,] [Por acuerdo expreso o implícito, se podrá hacer abstracción de cualquier aspecto del presente Régimen o modificarlo,] salvo si con ello se pueden perjudicar los derechos de terceros.

Variante B

1) El presente Régimen no afectará a ningún derecho de que gocen las partes a modificar mediante acuerdo cualquiera de las reglas de derecho a que se hace referencia en los artículos 6 y 7.

2) Las partes podrán convenir, expresa o implícitamente, en apartarse de algún aspecto de los artículos 9 a 12 del presente Régimen o en modificarlo, salvo si con ello se pueden perjudicar los derechos de terceros.

Referencias a documentos de la CNUDMI

A/CN.9/457, párrs. 53 a 64

Observaciones

36. La variante A del proyecto de artículo 5 refleja la decisión adoptada por el Grupo de Trabajo en su 34º período de sesiones de incluir en el texto, para futuras deliberaciones, una disposición que garantice la libertad de las partes para convenir en apartarse de las disposiciones del presente Régimen o en modificarlas únicamente a los efectos de transacciones entre dichas partes. No obstante, tal acuerdo no podrá afectar a los derechos de las partes que no intervengan en el acuerdo, es decir, los terceros. Esta disposición de autonomía se refiere únicamente al presente Régimen y no pretende afectar al orden público ni a las leyes imperativas aplicables a los contratos, como las disposiciones relativas a los contratos leoninos.

37. La variante B reconoce que las disposiciones de los artículos 6 y 7 del proyecto de Régimen Uniforme, que se basan en los artículos 7 y 8 de la Ley Modelo, incluyen referencias a disposiciones que pueden ser requisitos vinculantes de derecho interno no sujetos a modificación mediante acuerdo. El párrafo 1) permite la modificación mediante acuerdo cuando esos requisitos vinculantes de derecho interno puedan modificarse de tal forma. El texto repite el enunciado del párrafo 2) del artículo 4 de la Ley Modelo, que regula la misma cuestión.

38. El párrafo 2) de la variante B propugna una total autonomía de las partes con respecto a los artículos 9 a 12 del proyecto. Esta disposición se ha redactado con el criterio de que los artículos 9 a 12 del proyecto serían reglas de derecho sustantivo que serían aplicables cuando las partes contratantes no hubieran convenido en apartarse de la aplicación de esas disposiciones o en modificarlas. Las partes tendrían libertad para modificar o no seguir esas disposiciones. El párrafo 2) tiene la finalidad de asegurar que tal acuerdo no vaya en detrimento de terceros, pero no pretende invalidar ninguna parte del acuerdo entre las partes.

39. Las disposiciones relativas al reconocimiento transfronterizo no estarían sujetas a modificación mediante acuerdo, salvo en la medida en que lo dispusieran específicamente esas disposiciones.

40. El Grupo de Trabajo tal vez desee examinar el enunciado del proyecto de artículo 5 y las cuestiones que plantea respecto del cumplimiento de lo que podrían ser disposiciones vinculantes de los artículos 6 y 7 del proyecto. El Grupo de Trabajo tal vez desee examinar también el modo en que el principio de la autonomía de las partes debe aplicarse a los artículos 9 a 12 del proyecto. La disposición podría establecer, por ejemplo, reglas supletorias que fueran aplicables cuando no hubiera acuerdo en contrario entre las partes contratantes (desvinculación) o podría establecer reglas que las partes pudieran convenir en aplicar (adhesión).

Observaciones generales sobre los artículos 6 a 8 del proyecto

41. El Grupo de Trabajo, en el contexto de las deliberaciones de su 34º período de sesiones sobre el alcance del Régimen Uniforme (A/AC.9/457, párrs. 48 a 52), decidió concentrarse en las reglas para las tecnologías que se utilizaban actualmente en las transacciones comerciales, como las técnicas digitales en una infraestructura de clave pública. Por consiguiente, se decidió que el Grupo de Trabajo centrara sus debates en los artículos F a H (correspondientes a los artículos 9 a 12 del presente proyecto), en el contexto de las infraestructura de clave pública. Se aplazó el examen de los artículos A a D (correspondientes a los artículos 2, 6, 7 y 8 del presente proyecto) hasta que se hubieran examinado los artículos F a H. Se señaló que, en particular, el proyecto de artículo B (correspondiente, en esta revisión, al artículo 6 - Cumplimiento de los requisitos de firma), podía cumplir una importante función al definir el ámbito de aplicación de los artículos F a H. Se observó igualmente que el artículo E (correspondiente, en este proyecto, al artículo 5 - Modificación mediante acuerdo), que regulaba el principio de la autonomía de las partes, sería importante a la hora de examinar las obligaciones de las partes en los artículos F a H.

Artículo 6. [Cumplimiento de los requisitos de firma] [Presunción de firma]

Variante A

1) Cuando, en relación con un mensaje de datos, se utilice una firma electrónica refrendada, se presumirá que el mensaje de datos está firmado.

2) Cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos si se utiliza una firma electrónica que es tan fiable como sea apropiada para los fines para los que se generó o comunicó el mensaje de datos, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo pertinente.

[3) Cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos si se utiliza una firma electrónica refrendada.]

4) Los párrafos 2) y 3) serán aplicables tanto si el requisito en ellos previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que no exista una firma.

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

Variante B

1) Cuando, en relación con un mensaje de datos, se utilice [un método] [una firma electrónica] que:

a) sea exclusiva del titular de la firma [para los fines para los] [en el contexto en el] que se utilice;

[b) se pueda utilizar para identificar objetivamente al titular de la firma en relación con el mensaje de datos; y]

c) haya sido creada y consignada en el mensaje de datos por el titular de la firma o utilizando un medio bajo el control exclusivo del titular de la firma. [y por ninguna persona];

se presumirá que el mensaje de datos está firmado.

2) Cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos si se utiliza una firma electrónica que es tan fiable como sea apropiada para los fines para los que se generó o comunicó el mensaje de datos, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo pertinente.

3) El párrafo 2) será aplicable tanto si el requisito en ellos previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que no exista una firma.

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

Referencias a documentos de la CNUDMI

A/CN.9/457, párrs. 48 a 52;
A/CN.9/WG.IV/WP.80, párrs. 11 y 12

Observaciones

Variante A

42. La variante A dispone que cuando se utilice una firma electrónica refrendada en relación con un mensaje de datos, se podrá presumir que el mensaje de datos está firmado. En el párrafo 2) se reafirma el principio enunciado en el artículo 7 de la Ley Modelo en virtud del cual toda firma electrónica podrá cumplir el requisito legal de firma siempre y cuando satisfaga ciertas condiciones de fiabilidad. El Grupo de Trabajo recordará que en el párrafo 58 de la Guía para la incorporación de la Ley Modelo al derecho interno se especifican los factores que podrán tenerse en cuenta al determinar el nivel apropiado de fiabilidad. El párrafo 3), que dispone que las firmas electrónicas refrendadas cumplen esas condiciones y facilita el cumplimiento de los requisitos del artículo 7 de la Ley Modelo, figura entre corchetes en el presente proyecto. El Grupo de Trabajo tal vez desee examinar la cuestión de si aún es necesario mantener esa disposición en el texto, habida cuenta del párrafo 1).

Variante B

43. La finalidad de la variante B es establecer una presunción de firma y de cumplimiento del requisito legal de firma en el contexto de una única categoría de firma electrónica. Por consiguiente, no se hace referencia a la “firma electrónica refrendada”. El párrafo 1) de la variante B dispone que cuando se utilice un método en relación con un mensaje de datos y ese método cumpla ciertos requisitos, podrá presumirse que el mensaje de datos está firmado. Ese método debe cumplir las condiciones enunciadas en la definición de “firma electrónica refrendada” que figura en el proyecto de artículo 2 b), con excepción de la referencia a la integridad en el apartado b) iii). El apartado b) del párrafo 1) figura entre corchetes, ya que sólo sería necesario si en las palabras iniciales del párrafo 1) no se hiciera referencia a “una firma electrónica” sino a “un método”.

44. El Grupo de Trabajo tal vez desee considerar si debe limitarse el ámbito de aplicación del Régimen Uniforme a aquellos supuestos en los que se impongan requisitos legales de forma o en los que la ley prescriba ciertos efectos para la no observancia de ciertos requisitos de escritura o de firma. Conviene recordar que en la preparación de la Ley Modelo se examinó lo que debe entenderse por requisito de forma. El párrafo 68 de la Guía para la incorporación de la Ley Modelo al derecho interno observa que el empleo del término “la ley” en la Ley Modelo ha de entenderse como referido no sólo a toda norma de derecho sustantivo legal o reglamentario, sino también a toda disposición de derecho jurisprudencial y de derecho procesal. Por ello, el término “la ley” abarca también al régimen interno de la prueba. Cuando una norma de derecho interno no imponga determinado requisito, sino que prescriba ciertas consecuencias para la ausencia de, por ejemplo, un escrito o una firma, deberá considerarse que esa norma está englobada en el concepto que la Ley Modelo designa por el término “la ley”.

Referencias a legislación nacional y a otros textos

Singapur

Quinta parte. Firmas y documentos electrónicos seguros

Firma electrónica segura

17. Si, aplicando un procedimiento de seguridad prescrito o un procedimiento de seguridad comercialmente razonable convenido por las partes interesadas, puede comprobarse que, en el momento de realizarse, una firma electrónica

a) era exclusivamente de la persona que la utilizaba;
b) servía para identificar a dicha persona;
c) fue creada de un modo o con medios controlados exclusivamente por la persona que la utilizaba; y
d) estaba vinculada al documento electrónico con el que guardaba relación de modo que si el documento era modificado, la firma quedaría invalidada,

tal firma se considerará una firma electrónica segura.

Presunciones relativas a las firmas y los documentos electrónicos

18. [...]

2) En toda acción judicial referente a una firma electrónica segura se presumirá, a menos que se aduzcan pruebas en contrario, que

a) la firma electrónica segura es la firma de la persona con la que guarda relación; y
b) la firma electrónica segura fue adjuntada por esa persona con la intención de firmar o aprobar el documento electrónico.

Artículo 7. [Presunción de original]

1) Cuando, en relación con un mensaje de datos, [se utilice una firma electrónica refrendada] [se utilice una firma electrónica [un método] que ofrece alguna garantía fidedigna de que se ha conservado la integridad de la información a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma], se presumirá que el mensaje de datos es un original.

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

Referencias a documentos de la CNUDMI

A/CN.9/457, párrs. 48 a 52;
A/CN.9/WG.IV/WP.80, párrs. 13 y 14

Observaciones

45. La finalidad del proyecto de artículo 7 es confirmar su relación con el artículo 8 de la Ley Modelo y el requisito de integridad. En el párrafo 1) figuran dos opciones. La primera prevé que con la utilización de una firma electrónica refrendada, según la definición del proyecto de artículo 2 b), se establecerá la presunción de que el mensaje de datos es un original. En virtud de la segunda opción, cuando se utilice una firma electrónica o un método que ofrezca alguna garantía fidedigna de integridad, podrá presumirse que el mensaje de datos es un original. Si bien la forma original no siempre requiere una firma, la utilización de la forma de la firma electrónica, refrendada o no, puede servir para verificar la integridad del mensaje de datos o del registro.

Artículo 8. Determinación de la firma electrónica [refrendada]

1) *[El órgano o la entidad designada por este Estado como competente]* podrá determinar [que una firma electrónica es una firma electrónica refrendada] [qué [métodos] [firmas electrónicas] cumplen los requisitos de los artículos 6 y 7].

2) Toda determinación efectuada a tenor del párrafo 1) deberá ser conforme a las normas técnicas internacionales.

Referencias a documentos de la CNUDMI

A/CN.9/457, párrs. 48 a 52;
A/CN.9/WG.IV/WP.80, párr. 15

Observaciones

46. La finalidad del proyecto de artículo 8 es dejar claro que los Estados pueden designar un órgano o una entidad con la facultad para determinar las tecnologías concretas que podrán reconocerse como firmas electrónicas refrendadas. Las opciones previstas en el párrafo 1) tienen por objeto ajustar el proyecto de artículo 8 a las opciones que figuran en los artículos 6 y 7 revisados. La finalidad del párrafo 2) es alentar a los Estados a que, al adoptar decisiones conforme al párrafo 1), se atengan a las normas internacionales aplicables y faciliten así la armonización de las prácticas con respecto a las firmas electrónicas refrendadas y la utilización y el reconocimiento transfronterizo de las firmas.

Observaciones generales sobre los artículos 9 y 10 del proyecto

47. El Grupo de Trabajo tal vez desee examinar la relación existente en la práctica entre los artículos 9 y 10 del proyecto. Existen varias combinaciones posibles de las obligaciones previstas en el proyecto de artículo 9 y las consecuencias del incumplimiento de esas obligaciones, enunciadas en el proyecto de artículo 10. Dos de estas combinaciones servirán para ilustrar algunas de las cuestiones que cabe examinar.

48. En primer lugar, la situación en que el titular de la firma no incumple la obligación de actuar con la debida diligencia, prevista en el proyecto de artículo 9 1) c), pero aun así la firma queda en cierto modo en entredicho. El titular de la firma ignora este hecho, por lo que no da aviso al certificador de información, pero con ello es improbable que incumpla la obligación prevista en el proyecto de artículo 9 1) b). En virtud del proyecto de artículo 10, la parte que confiaba en la firma no podía saber que estaba en entredicho comprobando la información facilitada por el certificador de información, y podía fiarse de la firma. Esta situación plantea una serie de cuestiones: ¿es razonable que la parte que confía en la firma se fíe de tal situación? ¿La parte que se fía de la firma corre el riesgo derivado de esa confianza?¿Qué consecuencias tiene esa confianza para el titular de la firma? ¿Está el titular de la firma vinculado por lo que se haya firmado con la firma que está en entredicho?

49. En segundo lugar, la situación en que el titular de la firma incumple efectivamente la obligación de actuar con la debida diligencia, conforme al proyecto de artículo 9 1) c), y en que la firma queda en entredicho. El titular de la firma es consciente del hecho y da aviso al certificador de información. En virtud del proyecto de artículo 10, la parte que confiaba en la firma podía comprobar la información facilitada por el certificador, tras lo cual no podía confiar en la firma. Así pues, en virtud del proyecto de artículo 9 3), el titular de la firma es responsable del incumplimiento de las obligaciones del párrafo 2) y de la pérdida prevista en el párrafo 4). En esta situación, el resultado es mucho más claro que en la situación contemplada en el párrafo 48.

Artículo 9. [Responsabilidades] [obligaciones] del titular de la firma

1) El titular de la firma [tendrá la obligación de] [deberá]:

a) Actuar con la debida diligencia para velar por la exactitud y la integridad de todas las declaraciones materiales efectuadas por el titular de la firma que sean de interés para la expedición, suspensión o revocación de un certificado, o que estén consignadas en el certificado.

b) Dar aviso a quien corresponda sin demora injustificada en caso de que [tuviera conocimiento de que su firma ha quedado en entredicho] [su firma quedara o pudiera haber quedado en entredicho];

c) Actuar con la debida diligencia para mantener el control de su firma y evitar toda utilización no autorizada de la misma, a partir del momento en que el titular de la firma tenga el control exclusivo del dispositivo de firma.

2) Si [hay titulares comunes] [más de una persona tiene bajo su control] [la clave] [el dispositivo de firma], [los deberes] [las obligaciones] dimanantes del párrafo 1) tienen carácter solidario.

3) El titular de la firma será [responsable] del [incumplimiento de las obligaciones [los deberes] dimanantes del] [incumplimiento de los requisitos del] párrafo 1).

4) [La responsabilidad del titular de la firma no podrá exceder de la pérdida que el titular de la firma hubiera previsto o debiera haber previsto en el momento de su incumplimiento, tomando en consideración los hechos de que el titular de la firma tuvo o debió haber tenido conocimiento como consecuencias posibles del incumplimiento [de las obligaciones [de los deberes] dimanantes] del [de los requisitos del] párrafo 1).]

Referencias a documentos de la CNUDMI

A/CN.9/457, párrs. 65 a 98;
A/CN.9/WG.IV/WP.80, párrs. 18 y 19

Observaciones

Artículo 9, párrafo 1)

50. El párrafo 1) del proyecto de artículo 9 ha sido revisado de conformidad con las decisiones adoptadas por el Grupo de Trabajo en su 34º período de sesiones (A/CN.9/457, párrs. 73 a 92) . El Grupo de Trabajo expresó su preocupación por el hecho de que la obligación prevista en el apartado a) estuviera limitada al contexto del proceso de certificación (A/CN.9/457, párr. 92), ya que de otro modo la obligación podría interpretarse de forma amplia de modo que abarcara las declaraciones y manifestaciones hechas por el titular de la firma a la parte que confía en la firma. Dado que las declaraciones o manifestaciones efectuadas en el contexto de esta relación deberían estar sujetas al régimen del contrato pertinente, se ha reducido el alcance del apartado a) para limitar la obligación al contexto del proceso de expedición, suspensión o revocación de un certificado.

51. Se ha revisado el apartado b) incluyendo en él dos posibles textos acordados por el Grupo de Trabajo (A/CN.9.457, párr. 83). Las palabras “o debía haber sabido” no se han incluido en esta revisión por estimarse que sería difícil para el titular de la firma cumplir la obligación de dar aviso de algo que debiera haber sabido, pero que de hecho ignoraba.

52. El apartado c) se refiere no sólo a la obligación de evitar toda utilización no autorizada de la firma sino también a la obligación de mantener la clave bajo control. La disposición revisada se refiere también al momento a partir del cual existe la obligación de actuar con la debida diligencia. Ello refleja la opinión dominante en el Grupo de Trabajo de que, mientras que la obligación del titular de la clave de proteger la clave sólo debería plantearse respecto de los juegos de claves efectivamente protegidos por un certificado, la obligación del titular de la clave de proteger las claves certificadas de toda utilización indebida debía ser aplicable retroactivamente a partir del momento en que el titular de la firma obtuviera el control exclusivo del juego de claves (A/CN.9/457, párr. 67).

Párrafo 2)

53. El párrafo 2) ha sido agregado al proyecto de artículo 9 con objeto de aclarar la obligación de debida diligencia en la situación en que puede haber más de un titular de la misma clave. El Grupo de Trabajo tal vez desee examinar esta disposición y su relación con los requisitos de control exclusivo previstos en el artículo 2.

Párrafo 3)

54. Este párrafo ha sido revisado de conformidad con las decisiones adoptadas por el Grupo de Trabajo en su 34º período de sesiones (A/CN.9/457, párrs. 93 a 98). Se ha omitido la referencia a las "consecuencias del incumplimiento [por parte del titular de la firma] de las obligaciones dimanantes del párrafo 1)" por las siguientes razones: i) para evitar debates sobre si la obligación incumplida era contractual, y ii) para evitar toda incertidumbre que pudiera plantear la palabra "consecuencias", ya que con ella podía darse a entender que se trataba de todas las posibles consecuencias sin reflejar el hecho de que esas posibles consecuencias podían estar muy lejos del incumplimiento de la obligación.

Párrafo 4)

55. Este párrafo se basa en el artículo 74 de la Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías y se ha incluido en el texto para que lo examine el Grupo de Trabajo. El párrafo establece una norma basada en la previsibilidad de los daños, pero se limita al incumplimiento de las obligaciones del titular de la firma previstas en el párrafo 1). Durante el 34º período de sesiones (A/CN.9/457, párrs. 93 a 98), algunos miembros del Grupo de Trabajo se declararon preocupados por el hecho de que la responsabilidad que pudiera derivarse de un contrato de compraventa de mercaderías no era la misma que la que pudiera derivarse de la utilización de una firma, y no podía cuantificarse del mismo modo. También se señaló que la regla de la previsibilidad tal vez no resultara apropiada en el contexto de la relación contractual entre el titular de la firma y el certificador de información, aunque quizá lo fuera en el contexto de la relación entre el titular de la firma y una parte que confía en ella. El Grupo de Trabajo tal vez desee examinar estas cuestiones en sus ulteriores deliberaciones sobre este proyecto de artículo y estudiar asimismo la relación entre los artículos 9 y 10 del proyecto.

Referencias a legislación nacional y a otros textos

Párrafo 1) a) - Declaraciones materiales

Directrices de la Asociación de Abogados de los Estados Unidos (ABA)

4.2 Obligaciones del suscriptor
Todas las declaraciones materiales que haga un suscriptor a una autoridad certificadora, incluida toda la información que posea el suscriptor y que se consigne en el certificado, debe ser lo más exacta posible, según le conste al suscriptor, independientemente de si esas declaraciones son confirmadas o no por la autoridad certificadora.

GUIDEC

VII. Garantía de un mensaje
7. Declaraciones destinadas a un certificador
El suscriptor deberá comunicar con precisión al certificador todos los hechos que sean pertinentes en relación con el certificado.

Illinois

Artículo 20. Deberes de los suscriptores
Sección 20-101. Obtención de un certificado
Todas las declaraciones materiales efectuadas por una persona con conocimiento de causa a una autoridad certificadora con el fin de obtener un certificado, nombrando a tal persona como suscriptor, deben ser exactas y completas, según le conste a esa persona.

Sección 20-105. Aceptación de un certificado

[...]
b) Al aceptar un certificado, el suscriptor nombrado en el certificado hace saber a cualquier persona que confía razonablemente en la información consignada en el certificado, de buena fe y durante su período de validez, que:

1) el suscriptor tiene legalmente en su poder la clave privada que corresponde a la clave pública consignada en el certificado;

2) todas las declaraciones hechas por el suscriptor a la autoridad certificadora que guarda información con la información consignada en el certificado son veraces; y

3) toda la información consignada en el certificado de la que tiene conocimiento el suscriptor es veraz.

Singapur

Novena parte. Derechos de los suscriptores
Obtención de un certificado
37. Todas las declaraciones materiales que haga un suscriptor a una autoridad certificadora con el fin de obtener un certificado, incluida toda la información que posea el suscriptor y que se consigne en el certificado, serán exactas y completas, según le conste al suscriptor, independientemente de si esas declaraciones son confirmadas o no por la autoridad certificadora.

Párrafo 1) b) - Aviso

Directrices de la Asociación de Abogados de los Estados Unidos (ABA)

4.4 Iniciación de la suspensión o revocación
El suscriptor que ha aceptado un certificado debe solicitar a la autoridad certificadora que lo haya expedido que suspenda o revoque el certificado si ha quedado en entredicho la clave privada que corresponde a la clave pública consignada en el certificado.

Illinois

Artículo 20. Deberes de los suscriptores
Sección 20-110. Revocación de un certificado
Salvo si en otra regla de derecho aplicable se dispone otra cosa, en caso de que una clave privada correspondiente a la clave pública consignada en un certificado válido se pierda, sea robada o resulte accesible para una persona no autorizada o quede de otro modo en entredicho durante el período de validez del certificado, el suscriptor que tenga conocimiento de tales hechos deberá solicitar prontamente a la autoridad certificadora que ha expedido el certificado que lo revoque y publique un aviso de revocación en todas las entidades de registro en que el suscriptor haya autorizado previamente la publicación del certificado, o difunda un aviso razonable de la revocación.

Sección 10-125. Creación y control de dispositivos de firma
Salvo si otra regla de derecho aplicable dispone otra cosa, siempre que la creación, la validez o la fiabilidad de una firma electrónica creada mediante un procedimiento de seguridad adecuado en virtud de [...] dependan del carácter secreto o del control de un dispositivo de firma del signatario:

1) la persona que genere o cree el dispositivo de firma deberá hacerlo de forma fidedigna;

2) el signatario y todas las otras personas con acceso legal a tal dispositivo de firma deberán actuar con la debida diligencia para mantener el control y el carácter secreto del dispositivo y protegerlo de todo acceso, revelación o uso no autorizados durante el período en que la confianza en una firma creada por tal dispositivo sea razonable;

3) en caso de que el signatario, u otra persona con acceso legal al dispositivo de firma, sepa o tenga motivos para saber que el carácter secreto o el control del dispositivo de firma ha quedado en entredicho, esa persona deberá hacer un esfuerzo razonable por avisar prontamente a todas las personas que, según conste a dicha persona, puedan resultar perjudicadas por tal situación o, de disponerse de un mecanismo apropiado de publicación [...], por dar a conocer que el dispositivo está en entredicho y que se desautorizan todas las firmas creadas a partir de ese momento.

Singapur

Iniciación de la suspensión o revocación
40. Todo suscriptor que haya aceptado un certificado deberá pedir lo antes posible a la autoridad certificadora que lo expidió que suspenda o revoque el certificado si la clave privada que corresponde a la clave pública consignada en el certificado queda en entredicho.

Párrafo 1) c). Utilización no autorizada

Directrices de la Asociación de Abogados de los Estados Unidos (ABA)

4.3 Salvaguardia de la clave privada
Durante el período de validez de un certificado, el suscriptor no pondrá en entredicho la clave privada correspondiente a una clave pública consignada en dicho certificado y deberá también evitar que quede en entredicho durante todo período de suspensión.

GUIDEC

VII. Garantía de un mensaje
6. Salvaguardia de un dispositivo de garantía
Si una persona asegura un mensaje mediante un dispositivo, esa persona deberá, como mínimo, actuar con la debida diligencia para prevenir toda utilización no autorizada del dispositivo.

Illinois

Sección 10-125. Creación y control de dispositivos de firma
Salvo si otra regla de derecho aplicable dispone otra cosa, siempre que la creación, la validez o la fiabilidad de una firma electrónica creada mediante un procedimiento de seguridad adecuado en virtud de [...] dependan del carácter secreto o del control de un dispositivo de firma del signatario:

1) la persona que genere o cree el dispositivo de firma deberá hacerlo de forma fidedigna;

2) el signatario y todas las otras personas con acceso legal a tal dispositivo de firma deberán actuar con la debida diligencia para mantener el control y el carácter secreto del dispositivo y protegerlo de todo acceso, revelación o uso no autorizados durante el período en que la confianza en una firma creada por tal dispositivo sea razonable;

3) en caso de que el signatario, o cualquier otra persona con acceso legal al dispositivo de firma, sepa o tenga motivos para saber que el carácter secreto o el control del dispositivo de firma ha quedado en entredicho, esa persona deberá hacer un esfuerzo razonable por avisar prontamente a todas las personas que, según conste a dicha persona, puedan resultar perjudicadas por tal situación o, de disponerse de un mecanismo apropiado de publicación [...], por dar a conocer que el dispositivo está en entredicho y que se desautorizan todas las firmas creadas a partir de ese momento.

Párrafos 3) y 4)- Responsabilidad

Minnesota

325K.12 Declaraciones y obligaciones al aceptar certificados
Subd.4 Indemnización a cargo del suscriptor
Al aceptar un certificado, el suscriptor se compromete a indemnizar a la autoridad certificadora que lo expidió por las pérdidas o perjuicios causados con la publicación de un certificado sobre la base de:
1) una presentación falsa y material de los hechos por el suscriptor;
2) la omisión por el suscriptor de un hecho material si la declaración o la omisión fueron efectuadas con intención de engañar a la autoridad certificadora o a la persona que confía en el certificado, o con negligencia grave. La indemnización prevista en el presente artículo no podrá eludirse ni limitarse su alcance por vía contractual. No obstante, se podrán estipular en un contrato nuevas condiciones coherentes para la indemnización.

Singapur

Novena parte. Deberes de los suscriptores
Control de la clave privada
39. 1) Al aceptar un certificado expedido por una autoridad certificadora, el suscriptor nombrado en el certificado asume la obligación de actuar con la debida diligencia para mantener el control de la clave privada que corresponda a la clave pública consignada en dicho certificado y prevenir su revelación a toda persona no autorizada a crear la firma numérica del suscriptor.
2) Esta obligación seguirá vigente durante el período de validez del certificado y durante cualquier período de suspensión del mismo.

Artículo 10. Confianza en las firmas electrónicas refrendadas

1) Toda persona [tendrá] derecho a [no] confiar en una firma electrónica refrendada en la medida en que [sea] [no sea] razonable hacerlo.

2) Para determinar si [es] [no es] razonable confiar, deberá tenerse en cuenta, en su caso, lo siguiente:

a) La naturaleza de la operación correspondiente que la firma tenga por objeto avalar;

b) Si la parte que confía ha adoptado las medidas adecuadas para determinar la fiabilidad de la firma;

c) Si la parte que confía sabía o debía haber sabido que la firma estaba en entredicho o había sido revocada;

d) Todo acuerdo o trato que la parte que confía tenga con el suscriptor o todo uso comercial aplicable;

e) Todo otro factor pertinente.

Artículo 11. Confianza en los certificados

1) Toda persona [tendrá] derecho a [no] confiar en un certificado en la medida en que [sea] [no sea] razonable hacerlo.

2) Para determinar si [es] [no es] razonable confiar, deberá tenerse en cuenta, en su caso, lo siguiente:

a) Toda restricción a que esté sujeto el certificado;

b) Si la parte que confía ha adoptado las medidas adecuadas para determinar la fiabilidad del certificado, consultando eventualmente una lista de revocaciones de certificados;

c) Todo acuerdo o trato que la parte que confía tenga con el certificador de información o el suscriptor o todo uso comercial aplicable;

d) [Todo otro] [Todos los demás] factor[es] pertinente[s].

Referencias a documentos de la CNUDMI

A/CN.9/457, párrs. 99 a 107;
A/CN.9/WG.IV/WP.80, párrs. 20 y 21

Observaciones

56. Los artículos 10 y 11 del proyecto, que regulan los criterios para confiar en firmas electrónicas refrendadas y certificados, respectivamente, han sido revisados para tener en cuenta la opinión predominante en el Grupo de Trabajo durante su 34º período de sesiones (A/CN.9/457, párr. 107). Si bien inicialmente estas disposiciones figuraban en un solo artículo relativo a la confianza en las firmas y la confianza en las firmas avaladas por un certificado, en el presente proyecto se han disgregado los dos conceptos debido a las distintas consideraciones que se aplican a cada una de las situaciones. El Grupo de Trabajo tal vez desee examinar la conveniencia de incluir en el texto una disposición sobre la confianza en los certificados, además de la disposición sobre la confianza en las firmas, especificando en cada caso las consideraciones que justificarían una confianza razonable.

57. El Grupo de Trabajo expresó cierta inquietud por la posibilidad de que al formularse los artículos 10 y 11 del proyecto como derechos a tener confianza pudieran presumirse ciertos efectos jurídicos, mientras que al determinarse los factores que debían tenerse en cuenta al decidir si era razonable confiar podría dejarse de lado la cuestión del efecto jurídico que la firma o el certificado podrían tener. Por otra parte, se opinó que la formulación de los artículos como derechos a tener confianza suponía una ventaja que no existía en la Ley Modelo y no establecía un efecto

jurídico en lo que a la validez de la firma se refiere. El Grupo de Trabajo convino en que los artículos revisados del proyecto tenían una faceta positiva y otra negativa y especificaban los factores que debían tomarse en consideración en el caso de las firmas y en el de los certificados.

58. También se expresó cierta preocupación por la relación entre los artículos 10 y 11 del proyecto y el artículo 13 de la Ley Modelo y también por la posibilidad de que, al leerse conjuntamente, los artículos 9, 10 y 11 del proyecto establecieran una regla sobre la atribución. El Grupo de Trabajo tal vez desee estudiar la relación de los artículos 10 y 11 con el proyecto de artículo 9 y con el artículo 13 de la Ley Modelo.

Referencias a legislación nacional y a otros textos

Directrices de la Asociación de Abogados de los Estados Unidos (ABA)

5.3 Firmas numéricas no fidedignas
1) [...]
2) A menos que una ley o un contrato dispongan otra cosa, la parte que confía asumirá el riesgo de que una firma numérica no sea válida como firma o autenticación del mensaje firmado, si la confianza en la firma numérica no es razonable en las circunstancias del caso de conformidad con los factores enumerados en la directriz 5.4 (confianza razonable).

5.4 Confianza razonable
Entre los factores importantes para determinar si es razonable la confianza de un receptor en un certificado y en firmas numéricas verificables mediante la clave pública consignada en el certificado figuran los siguientes:
1) los hechos que la parte que confía conoce o de los que tiene conocimiento, incluidos los hechos enumerados en el certificado o incorporados a él por remisión,
2) el valor o la importancia del mensaje numéricamente firmado, si se conoce,
3) el trato entre la persona que confía y el suscriptor y los indicios existentes de fiabilidad o de falta de fiabilidad, además de la firma numérica,
4) los usos comerciales, particularmente en el comercio realizado con sistemas fidedignos u otros medios informáticos.

2.3 Previsibilidad de la confianza en certificados
Es de prever que las personas que confíen en una firma numérica confiarán asimismo en un certificado válido que contenga la clave pública con la que se pueda verificar la firma numérica.

GUIDEC

VIII. Certificación
1. Efecto de un certificado válido
Toda persona podrá confiar en un certificado válido por presentar con precisión el hecho o los hechos que en él se exponen si a dicha persona no le consta que el certificador haya incumplido un requisito material de la práctica de mensajes asegurados.

Singapur

Sexta parte. Efecto de las firmas numéricas
Firmas numéricas no fidedignas
22. A menos que una ley o un contrato dispongan otra cosa, la persona que confía en un documento electrónico numéricamente firmado asumirá el riesgo de que la firma numérica no sea válida como firma o como autenticación del documento electrónico firmado, si la confianza en la firma numérica no es razonable en las circunstancias del caso habida cuenta de los siguientes factores:
a) los hechos que conozca o de que tenga constancia la persona que confía en el documento electrónico numéricamente firmado, incluidos los hechos consignados en el certificado o incorporados a él por remisión;
b) el valor o la importancia del documento electrónico numéricamente firmado, si se conoce;
c) el trato concertado entre la persona que confía en el documento electrónico numéricamente firmado y el suscriptor, así como los indicios existentes de fiabilidad o de falta de fiabilidad, además de la firma numérica; y
d) todo uso comercial, particularmente en el comercio realizado con sistemas fidedignos u otros medios electrónicos.

Artículo 12. [Responsabilidades] [obligaciones] del certificador de información

1) [Todo certificador de información] [tendrá la obligación de [deberá]] [, entre otras cosas]:

a) actuar en función de las declaraciones que haga con respecto a sus prácticas;

b) adoptar medidas razonables para determinar la exactitud de todo hecho o dato que el certificador de información certifique en el certificado, [incluida la identidad del titular de la firma];

c) proporcionar medios razonablemente accesibles que permitan a la parte interesada averiguar:

i) la identidad del certificador de información;

ii) que la persona [nombrada] [cuyo nombre se especifica] en el certificado posee [en el momento pertinente] [la clave privada correspondiente a la clave pública] [el dispositivo de firma] que se menciona en el certificado;

[iii) que las claves son un par de claves complementarias];

iv) el método utilizado para identificar al titular de la firma;

v) toda limitación de los fines o del valor con los que pueda utilizarse la firma; y

vi) si el dispositivo de firma es válido y no está en entredicho;

d) proporcionar a los titulares de firmas un medio para dar aviso de que una firma electrónica refrendada está en entredicho y asegurar el funcionamiento de un servicio puntual de revocación;

e) actuar con la debida diligencia para velar por la exactitud y la integridad de todas las declaraciones materiales efectuadas por el certificador de información que sean de interés para la expedición, suspensión o revocación de un certificado, o que estén consignadas en el certificado;

f) utilizar sistemas, procedimientos y recursos humanos fiables para prestar sus servicios.

Variante X

2) El certificador de información será [responsable] del [incumplimiento de las obligaciones [los deberes] dimanantes del] [incumplimiento de los requisitos del] párrafo 1).

3) La responsabilidad del certificador de información no podrá exceder de la pérdida que el certificador de información hubiera previsto o debiera haber previsto en el momento de su incumplimiento, tomando en consideración los hechos de que el certificador de información tuvo o debió haber tenido conocimiento como consecuencias posibles del incumplimiento [de las obligaciones [de los deberes] dimanantes del] [de los requisitos del] párrafo 1).

Variante Y

2) A reserva de lo dispuesto en el párrafo 3), cuando los daños y perjuicios sean imputables a información incorrecta o errónea consignada en el certificado, todo certificador de información será responsable de los daños y perjuicios sufridos por:

a) toda parte que haya celebrado un contrato con el certificador de información para la expedición de un certificado; o por

b) toda persona que confíe razonablemente en un certificado expedido por el certificador de información.

3) El certificador de información no será responsable en virtud del párrafo 2:

a) cuando, y en la medida en que, haya incluido en el certificado una declaración por la que limite el alcance o la magnitud de su responsabilidad a una determinada persona; o

b) si demuestra que [no actuó con negligencia] [adoptó todas las medidas razonables para prevenir los daños].

Referencias a documentos de la CNUDMI

A/CN.9/457, párrs. 108 a 119;
A/CN.9/WG.IV/WP.80, párrs. 22 a 24

Observaciones

59. El proyecto de artículo 12 ha sido revisado de conformidad con las decisiones adoptadas por el Grupo de Trabajo en su 34º período de sesiones (A/CN.9/457, párrs. 108 a 119).

Párrafo 1)

60. Para las palabras iniciales del párrafo 1) figuran varias opciones. En la primera existe la posibilidad de redactar la disposición con los términos “tendrá la obligación de” o con el término “deberá”. La segunda opción prevé la posibilidad de agregar las palabras “entre otras cosas”. Si se emplean estas últimas palabras, el proyecto de artículo 12 establecerá una lista ilustrativa pero no delimitada de obligaciones. Si bien este enunciado podría parecer engorroso para los certificadores de información, el Grupo de Trabajo consideró que no sería incompatible con la regla general actualmente aplicable a los certificadores de información en muchos ordenamientos jurídicos. Si se omitieran las palabras “entre otras cosas”, el proyecto de artículo 12 establecería una lista exhaustiva de obligaciones del certificador de información que permitiría determinar el alcance exacto de la responsabilidad del certificador de información y evitar las dificultades que pudiera plantear un enunciado distinto en países en que el certificador de información no está sujeto a la regla general de la debida diligencia.

61. Las obligaciones concretas enunciadas en el párrafo 1) han sido ampliadas para tener en cuenta las opiniones del Grupo de Trabajo (A/CN.9/457, párrs. 112 a 114). Con respecto al apartado c), la información que debe proporcionarse por “medios razonablemente accesibles” consiste en información que la parte que confía pueda esperar razonablemente que figure en un certificado e información que sólo puede obtenerse por remisión a alguna otra fuente como las listas de revocaciones de certificados. El Grupo de Trabajo tal vez desee estudiar la posibilidad de que parte de esta información deba especificarse para su inclusión en un certificado y de incluir en el Régimen Uniforme una regla adicional que fije el contenido mínimo de un certificado.

62. En los incisos ii) y iii) del apartado c) del párrafo 1) figuran las expresiones “par de claves” y “dispositivo de firma”. A fin de asegurar que el Régimen Uniforme sea neutral con respecto a la tecnología, el Grupo de Trabajo tal vez desee optar por un enunciado neutral con respecto a la tecnología como “dispositivo de firma”, en vez de “par de claves”, ya que estos últimos términos se refieren específicamente a las firmas numéricas. La expresión “par de claves” puede ser apropiada en la definición de “certificado” cuando se trata de certificados utilizados únicamente en el contexto de firmas numéricas.

63. El inciso iii) del apartado c) del párrafo 1), propuesto en el anterior período de sesiones, ha sido incluido en el texto del artículo, pero el Grupo de Trabajo tal vez desee examinar si se trata de un requisito adecuado. Si la clave

pública consignada en el certificado corresponde a la clave privada que posee el titular de la firma y existe, por lo tanto, una correspondencia matemática entre ambas claves, no se entiende qué funcionalidad adicional se lograría con el requisito de que el par de claves sea "un par de claves complementarias". También cabe dudar de si el certificador de información podría facilitar información, además de la requerida en el inciso ii) del apartado c), que indicara esa funcionalidad adicional.

Párrafos 2) y 3)

64. La variante X establece la regla de que el certificador de información es responsable del incumplimiento de las obligaciones o deberes dimanantes del párrafo 1), pero deja en manos del derecho interno la determinación de las consecuencias de tal incumplimiento. En este proyecto revisado de artículo 12 se han omitido las palabras "las consecuencias de" por las mismas razones con las que se justificó su supresión en el párrafo 3) del proyecto de artículo 9, es decir: i) para evitar debates sobre si la obligación incumplida era contractual; y ii) para evitar toda incertidumbre que pudiera plantear la palabra "consecuencias", ya que con ella podía darse a entender que se trataba de todas las posibles consecuencias sin reflejar el hecho de que esas posibles consecuencias podían estar muy lejos del incumplimiento de la obligación.

65. Tras la revisión del párrafo 1) con dos posibles variantes (una lista exhaustiva de obligaciones o una lista ilustrativa pero no delimitada de obligaciones), el Grupo de Trabajo tal vez desee examinar si la variante X sería más apropiada en caso de que se adoptara el párrafo 1) en forma de lista exhaustiva, y no de lista no delimitada.

66. El párrafo 3) de la variante X establece una regla de previsibilidad de los daños basada en el artículo 74 de la Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías. Este párrafo limita el alcance de la responsabilidad del certificador de información que pudiera derivarse de los párrafos 1) y 2).

Variante Y

67. Muchos miembros del Grupo de Trabajo (A/CN.9/457, párr. 115) coincidieron en estimar que sería apropiado crear una disposición uniforme que no se limitara a remitir al derecho aplicable y que previera una responsabilidad general por negligencia, sujeta a posibles exenciones contractuales (siempre y cuando la limitación no fuera gravemente inequitativa) y con la posibilidad de que el certificador de información quedara exento de responsabilidad si demostraba haber cumplido las obligaciones previstas en el párrafo 1). El párrafo 2) de la variante Y regula la cuestión de la persona ante la que puede ser responsable el certificador de información. El párrafo 3) prevé una norma que permite al certificador de información invocar eventuales limitaciones de la responsabilidad previstas en el certificado o demostrar que no actuó con negligencia o que adoptó medidas razonables para prevenir los daños.

68. Al igual que en la variante X, el Grupo de Trabajo tal vez desee estudiar si la disposición propuesta en la variante Y sería apropiada si en el párrafo 1) se previera una lista exhaustiva de obligaciones, pero no en el caso de que las obligaciones no estuvieran delimitadas. Tal vez desee examinar también si en el proyecto de párrafo 2) de la variante Y debe puntualizarse que la responsabilidad del certificador de información sólo puede derivarse de su incumplimiento de las obligaciones del párrafo 1).

Referencias a la legislación nacional y a otros textos

Artículo 12, párrafo 1) - Obligaciones generales

Directrices de la Asociación de Abogados de los Estados Unidos (ABA)

3. Autoridades certificadoras

3.1 La autoridad certificadora debe utilizar sistemas fidedignos
En el cumplimiento de sus servicios, la autoridad certificadora deberá utilizar sistemas fidedignos.

3.2 Revelación
1) La autoridad certificadora deberá revelar toda declaración de interés sobre prácticas de certificación y dar a conocer la revocación o suspensión de un certificado expedido por la autoridad certificadora.
2) La autoridad certificadora deberá actuar con la debida diligencia para informar a las personas que, según le conste, puedan resultar afectadas por la revocación o suspensión del certificado expedido por dicha autoridad certificadora.
3) [...]
4) En caso de que produzca un hecho que afecte material o negativamente a la fiabilidad del sistema de una autoridad certificadora o al certificado por ella expedido, la autoridad certificadora deberá actuar con la debida diligencia para informar a las personas que, según le conste, puedan resultar afectadas por tal hecho, o actuar de conformidad con los procedimientos especificados en su declaración de prácticas de certificación.

3.7 Declaraciones de la autoridad certificadora en el certificado
Al expedir un certificado, la autoridad certificadora hace saber a las personas que confían razonablemente en el certificado o en una firma numérica, verificable mediante la clave pública consignada en el certificado, que la autoridad certificadora, de conformidad con la declaración aplicable de prácticas de certificación de la que la persona interesada tiene conocimiento, ha confirmado que
1) La autoridad certificadora, al expedir el certificado, ha cumplido con todos los requisitos aplicables de las presentes Directrices y, si la autoridad certificadora ha publicado el certificado o lo ha puesto en conocimiento de la persona que confía razonablemente en él, que el suscriptor cuyo nombre figura en el certificado lo ha aceptado;
2) El suscriptor cuyo nombre figura en el certificado posee la clave privada correspondiente a la clave pública consignada en el certificado;
3) [...]
4) La clave pública y la clave privada del suscriptor constituyen un par de claves complementarias; y
5) Toda la información consignada en el certificado es exacta, a menos que la autoridad certificadora haya declarado en el certificado que la exactitud de la información especificada no está confirmada, o que haya incorporado por remisión al certificado palabras en tal sentido.

Además, la autoridad certificadora manifiesta que en el certificado no se ha omitido ningún hecho material que, de ser conocido, pudiera afectar negativamente a la fiabilidad de las declaraciones que ha efectuado en virtud de la presente directriz.

3.9 Suspensión de un certificado a petición del suscriptor
A menos que un contrato celebrado entre la autoridad certificadora y el suscriptor disponga otra cosa, la autoridad certificadora deberá suspender un certificado lo antes posible cuando lo solicite una persona que la autoridad certificadora tenga motivos razonables para considerar que es
1) El suscriptor cuyo nombre figura en el certificado;
2) La persona debidamente autorizada a actuar en nombre de tal suscriptor; o
3) La persona que actúa en nombre de dicho suscriptor, que no está disponible.

3.10 Revocación de un certificado a petición del suscriptor
La autoridad certificadora que haya expedido un certificado deberá revocarlo a petición del suscriptor cuyo nombre figure en el certificado, cuando la autoridad certificadora haya confirmado
1) que la persona que solicita la revocación es el suscriptor cuyo nombre figura en el certificado que debe revocarse; o
2) si el solicitante actúa como mandatario, que el solicitante tiene suficiente autoridad para llevar a cabo la revocación.

3.11 Revocación o suspensión sin el consentimiento del suscriptor
La autoridad certificadora podrá suspender o revocar un certificado independientemente de si el suscriptor mencionado en él da su consentimiento, cuando la autoridad certificadora confirme que
1) un hecho material expuesto en el certificado es falso;
2) no se cumplió un requisito material para la expedición del certificado; o
3) la clave privada o la fiabilidad del sistema fidedigno de la autoridad certificadora han quedado en entredicho de modo que resulta afectada materialmente la fiabilidad del certificado.
Una vez realizada la suspensión o revocación, la autoridad certificadora deberá informar sin dilación al suscriptor cuyo nombre figure en el certificado suspendido o revocado.

3.12 Aviso de suspensión o revocación
Una vez suspendido o revocado un certificado, la autoridad certificadora deberá publicar sin demora un aviso de la suspensión o revocación si el certificado fue publicado y, en cualquier caso, deberá revelar la suspensión o revocación a toda parte interesada que solicite información.

Proyecto de Directiva de la CE

Anexo II. Requisitos para los proveedores de servicios de certificación que expiden certificados apropiados
Los proveedores de servicio de certificación deberán:
a) demostrar la fiabilidad necesaria para ofrecer servicios de certificación;
b) asegurar el funcionamiento de un directorio rápido y seguro y de un servicio inmediato de revocación;
ba) asegurar que pueda determinarse la fecha y hora, cuando se expida o revoque un certificado;
c) verificar con medios apropiados y de conformidad con el derecho interno la identidad y, en su caso, los atributos concretos de la persona para la que se expida un certificado apropiado;
d) emplear a personal que posea los conocimientos especializados, la experiencia y las calificaciones necesarias para los servicios ofrecidos, en particular la competencia a nivel directivo, los conocimientos en tecnología de firmas electrónicas, así como en procedimientos de seguridad adecuados; deberán también aplicar procedimientos y procesos administrativos y de gestión adecuados que correspondan a las normas reconocidas;
e) utilizar sistemas y productos fidedignos que estén protegidos de toda alteración y que deberán garantizar la seguridad técnica y criptográfica de los procesos que apoyen;
f) adoptar medidas contra la falsificación de certificados y, en casos en que el proveedor de servicios de certificación genere datos de creación de firmas, garantizar el carácter confidencial durante el proceso de generación de dichos datos;
g) mantener suficientes recursos financieros para funcionar de conformidad con los requisitos enunciados en la presente directiva y, en particular, para afrontar los riesgos de responsabilidad en caso de daños y perjuicios, por ejemplo, suscribiendo un seguro adecuado;
h) registrar toda la información pertinente sobre un certificado apropiado durante un período adecuado, en particular para aportar pruebas de certificación en caso de actuaciones judiciales. Este registro podrá hacerse de forma electrónica;
i) no almacenar ni copiar datos de creación de firmas de la persona a la que el proveedor de servicios de certificación haya ofrecido servicios básicos de gestión;
j) antes de iniciar una relación contractual con una persona que le solicite un certificado para apoyar su firma electrónica, informar a esa persona con un medio de comunicación duradero de las condiciones exactas para la utilización del certificado, incluidas las eventuales limitaciones de la utilización del certificado, la existencia de una acreditación voluntaria y los procedimientos para la presentación de quejas y la solución de controversias. Esta información deberá presentarse en un escrito que podrá transmitirse por medios electrónicos en un lenguaje fácilmente comprensible. También deberán comunicarse partes pertinentes de esta información a los terceros que confíen en el certificado y que soliciten dicha información;
k) utilizar sistemas fidedignos para almacenar certificados de forma verificable de modo que
- sólo puedan registrar y modificar datos las personas autorizadas;
- pueda comprobarse la autenticidad de la información;
- los certificados estén a disposición del público y puedan consultarse únicamente en los casos en que se haya obtenido el consentimiento del titular del certificado; y
- el operador del sistema se percate de todo cambio técnico que pueda poner en peligro estos requisitos de seguridad.

Alemania

§5 Expedición de certificados
1) El certificador deberá verificar con fiabilidad la identidad de las personas que soliciten un certificado. Confirmará la atribución de una clave criptográfica pública a una persona identificada mediante un certificado de clave criptográfica y mantendrá en todo momento el acceso a esos certificados, así como a los certificados de atribución, a los que tendrán acceso todas las personas a través de canales de comunicación públicos de forma verificada y con el asentimiento del titular de la clave criptográfica.
2) A petición del solicitante de un certificado, el certificador registrará la información relativa a la facultad del solicitante para representar a un tercero o a su licencia profesional o de otro tipo en el certificado de clave criptográfica o en un certificado de atribución, en la medida en que se demuestre con fiabilidad esta licencia o el consentimiento del tercero a que se registre la facultad de representación.
3) A petición de un solicitante, el certificador consignará un seudónimo en el certificado, en lugar del nombre del solicitante.
4) El certificador adoptará medidas para evitar que los certificados puedan ser imitados o falsificados de una forma que no resulte visible. Además, adoptará medidas para garantizar el carácter confidencial de la firma privadas. El certificador no podrá conservar claves de firmas privadas.
5) El certificador encomendará a personal fiable las actividades de certificación y utilizará componentes técnicos, de conformidad con el párrafo 14, para hacer accesibles las claves de las firmas y crear certificados, así como componentes técnicos que posibiliten la verificación de certificados conforme a lo dispuesto en la segunda frase del párrafo 1.

§6 Obligación de dar instrucciones
El certificador dará instrucciones al solicitante, en virtud del párrafo 1 de la sección 5, acerca de las medidas necesarias para contribuir a la seguridad de las firmas numéricas y a la fiabilidad de su verificación. Asimismo, dará instrucciones al solicitante acerca de los componentes técnicos que cumplan los requisitos de los párrafos 1 y 2 de la sección 14 y acerca de la atribución de

las firmas numéricas creadas con una clave de firma privada. Indicará al solicitante que puede ser necesario volver a firmar los datos con firmas numéricas antes de que la seguridad de una firma disminuya con el tiempo.

§8 Bloqueo de certificados

1) El certificador bloqueará un certificado a petición del titular de la clave de la firma o del representante de éste, si el certificado fue expedido sobre la base de información falsa con arreglo a la sección 7, cuando el certificador haya concluido sus actividades y no sean continuadas por otro certificador, o cuando la autoridad ordene el bloqueo en virtud de la segunda frase del párrafo 5 de la sección 13. Al ordenarse el bloqueo se indicará el momento a partir del cual será aplicable. No está permitido el bloqueo retroactivo.

GUIDEC

VIII Certificación

2. Exactitud de las declaraciones consignadas en un certificado

El certificador deberá confirmar la exactitud de todos los hechos expuestos en un certificado válido, a menos que del certificado se desprenda que una parte de la información no ha sido verificada.

3. Fiabilidad de un certificador

El certificador deberá:

a) Utilizar sólo sistemas de información y procesos tecnológicamente fiables y personal fidedigno para expedir certificados, suspender o revocar certificados de clave pública y, en su caso, salvaguardar sus claves privadas;

b) Carecer de conflictos de intereses que pudieran restarle fiabilidad al expedir, suspender y revocar un certificado;

c) Abstenerse de contribuir al incumplimiento de un deber por parte del suscriptor;

d) Abstenerse de actos u omisiones que mermen de forma considerable la fiabilidad razonable y previsible de un certificado válido;

e) Actuar de forma fidedigna con el suscriptor y las personas que confíen en un certificado válido.

4. Notificación de prácticas y problemas

El certificador deberá actuar con la debida diligencia para avisar a la persona previsiblemente afectada de:

a) Toda declaración material de prácticas de certificación, y de

b) Todo hecho que afecte a la fiabilidad de un certificado que haya expedido o a su capacidad para prestar sus servicios.

8. Suspensión de un certificado de clave pública previa solicitud

El certificador que haya expedido un certificado deberá suspenderlo sin demora a petición de la persona que se identifique como suscriptor cuyo nombre figure en un certificado de clave pública o como persona que esté en condiciones de saber si la seguridad de la clave privada de un suscriptor está en entredicho, como pudiera ser un representante, empleado, socio comercial o allegado familiar del suscriptor.

9. Revocación de un certificado de clave pública previa solicitud.

El certificador que haya expedido un certificado de clave pública deberá revocarlo sin demora:

a) Tras recibir una solicitud de revocación enviada por el suscriptor cuyo nombre figure en el certificado o por el representante autorizado de dicho suscriptor; y

b) Tras confirmar que la persona que solicita la revocación es ese suscriptor o un representante del suscriptor que está facultado para solicitar la revocación.

10. Suspensión o revocación de un certificado de clave pública sin previo consentimiento

El certificador que haya expedido un certificado de clave pública deberá revocarlo si:

a) El certificador confirma que un hecho material consignado en el certificado es falso;

b) El certificador confirma que la fiabilidad del sistema de información del certificador está en entredicho de tal modo que afecta materialmente a la fiabilidad del certificado.

El certificador podrá suspender un certificado sobre el que se planteen dudas razonables durante el período necesario para realizar una investigación que sea suficiente para confirmar si se dan los motivos de revocación previstos en el presente artículo.

11. Aviso de revocación o suspensión de un certificado de clave pública

Inmediatamente después de que el certificador haya suspendido o revocado un certificado de clave pública, el certificador deberá notificar debidamente dicha revocación o suspensión.

Illinois

Artículo 15. Efecto de una firma numérica

Sección 15-301. Servicios fidedignos

Salvo si en su declaración de prácticas de certificación se dispone explícitamente otra cosa, la autoridad certificadora y la persona que administre un registro deberán mantener su funcionamiento y prestar sus servicios de forma fidedigna.

Sección 15-305. Revelación

a) Para cada certificado expedido por una autoridad certificadora con la intención de que terceros confíen en él para verificar la firma numérica creada por suscriptores, la autoridad certificadora deberá publicar o hacer llegar al suscriptor y a todas las partes que confíen en el certificado:

1) En su caso, su declaración pertinente de prácticas de certificación; y

2) Su certificado en el que se identifique a la autoridad certificadora como suscriptora y que contenga la clave pública correspondiente a la clave privada utilizada por la autoridad certificadora para firmar numéricamente el certificado (su "certificado de autoridad certificadora").

b) En caso de que se produzca un hecho que afecte material y negativamente a las operaciones o al sistema de la autoridad certificadora, a su certificado de autoridad certificadora o a cualquier otro aspecto de su capacidad para funcionar de forma fidedigna, la autoridad certificadora deberá actuar de conformidad con los procedimientos que rigen este supuesto y que se especifican en su declaración de prácticas de certificación o, a falta de tales procedimientos, deberá actuar con la debida diligencia para avisar a las personas que, según conste a la autoridad certificadora, puedan resultar perjudicadas por tal hecho.

Sección 15-310. Expedición de un certificado

La autoridad certificadora sólo podrá expedir un certificado a un futuro suscriptor para que los terceros puedan verificar las firmas numéricas creadas por el suscriptor después de que:

1) la autoridad certificadora haya recibido del futuro suscriptor una solicitud de expedición; y de que

2) la autoridad certificadora:

A) haya cumplido los procedimientos y prácticas pertinentes que, en su caso, se enuncien en su declaración aplicable de prácticas de certificación; o

B) de no existir ninguna declaración de prácticas de certificación sobre estas cuestiones, haya confirmado de forma fidedigna que:

i) el futuro suscriptor es la persona cuyo nombre debe figurar en el certificado que ha de expedirse;

ii) la información consignada en el certificado que deba expedirse es exacta; y

iii) el futuro suscriptor es titular legal de una clave privada con la que puede crear una firma numérica, y la clave pública que figurará en el certificado puede utilizarse para verificar toda firma numérica adjuntada con dicha clave privada.

Sección 15-315. Declaraciones efectuadas al expedir un certificado

a) Al expedir un certificado con la intención de que los terceros puedan confiar en él para verificar las firmas numéricas creadas por el suscriptor, la autoridad certificadora declara al suscriptor, y a cualquier persona que confíe razonablemente en la información consignada en el certificado, de buena fe y durante su período de validez, que:

1) la autoridad certificadora ha tramitado, aprobado, y expedido, y administrará y, si es necesario, revocará el certificado de conformidad con su declaración aplicable de prácticas de certificación, recogida en el certificado o incorporada a él por remisión, o de que tenga conocimiento tal persona, o en su lugar, de conformidad con la presente ley o con la jurisdicción que rija la expedición del certificado;

2) la autoridad certificadora ha verificado la identidad del suscriptor conforme a lo previsto en el certificado o en su declaración aplicable de prácticas de certificación o, en su lugar, que la autoridad certificadora ha verificado la identidad del suscriptor de forma fidedigna;

3) la autoridad certificadora ha comprobado que la persona que solicita el certificado es titular de la clave privada que corresponde a la clave pública consignada en el certificado; y

4) salvo si en el certificado o en su declaración aplicable de prácticas de certificación se dispone explícitamente otra cosa, según consta a la autoridad certificadora, en la fecha en que se expidió el certificado, toda otra información consignada en el certificado es exacta y no induce materialmente a error.

b) Si la autoridad certificadora expidió el certificado conforme al régimen de otra jurisdicción, la autoridad certificadora presenta también todas las garantías y declaraciones que sean en su caso aplicables en virtud de la ley que rija su expedición.

Sección 15-320. Revocación de un certificado

a) Durante el período de validez de un certificado, la autoridad certificadora que lo haya expedido deberá revocar el certificado de conformidad con las políticas y los procedimientos que rijan la revocación y que se especifiquen en su declaración aplicable de prácticas de certificación o, a falta de tales políticas y procedimientos, lo antes posible:

1) después de recibir del suscriptor mencionado en el certificado una solicitud de revocación, y después de confirmar que la persona que solicita la revocación es el suscriptor o es el representante del suscriptor que está facultado para solicitar la revocación;

2) después de recibir una copia certificada del certificado de defunción de un suscriptor, o después de confirmar con otras pruebas fidedignas que el suscriptor ha fallecido;

3) después de que se le presenten documentos a través de los cuales se disuelva una empresa suscriptora, o después de que se confirme mediante otras pruebas que la empresa suscriptora ha sido disuelta o ha dejado de existir;

4) después de que se le presente una orden de revocación dictada por un tribunal de la jurisdicción competente; o

5) después de que la autoridad certificadora confirme que:

A) un hecho material expuesto en el certificado es falso;

B) no se cumplió un requisito material para la expedición del certificado;

C) la clave privada o el funcionamiento del sistema de la autoridad certificadora están en entredicho de tal modo que resulta materialmente afectada la fiabilidad del certificado; o

D) la clave privada del suscriptor está en entredicho.

b) Al efectuar la revocación, la autoridad certificadora debe dar aviso al suscriptor y a las partes que confían en el certificado, de conformidad con las políticas y los procedimientos que rigen el aviso de revocación y que figuren en su declaración aplicable de prácticas de certificación, o, a falta de tales políticas y procedimientos, avisar sin demora al suscriptor, publicar sin demora un aviso de revocación en todas las entidades de registro en que la autoridad certificadora haya hecho publicar anteriormente el certificado, y, en cualquier caso, comunicar la revocación a toda parte interesada que solicite información al respecto.

Singapur

Octava parte. Deberes de las autoridades certificadoras

Sistema fidedigno

27. Toda autoridad certificadora deberá utilizar sistemas fidedignos en la prestación de sus servicios.

Revelación

28. 1) La autoridad certificadora revelará

a) el certificado que contenga la clave pública correspondiente a la clave privada utilizada por esa autoridad certificadora para firmar numéricamente otro certificado (denominado en esta sección certificado de la autoridad certificadora);

b) toda declaración pertinente de prácticas de certificación;

c) todo aviso de revocación o suspensión de su certificado de autoridad certificadora; y

d) cualquier otro hecho que afecte material y negativamente a la fiabilidad del certificado que la autoridad haya expedido o a la capacidad de dicha autoridad para prestar sus servicios.

2) En caso de producirse un hecho que afecte material y negativamente a la fiabilidad del sistema de la autoridad certificadora o a su certificado de autoridad certificadora, la autoridad certificadora:

a) actuará con la debida diligencia para informar a toda persona que, según le conste, pueda resultar afectada por tal hecho; o

b) actuar de conformidad con los procedimientos que rijan tales hechos, según lo dispuesto en su declaración de prácticas de certificación.

Expedición de un certificado

29. 1) La autoridad certificadora sólo podrá expedir un certificado a un futuro suscriptor después de que la autoridad certificadora:

a) haya recibido del futuro suscriptor una solicitud de expedición; y

b) haya cumplido

i) todas las prácticas y todos los procedimientos enunciados en la declaración sobre prácticas de certificación, de haber efectuado tal declaración, incluidos los procedimientos para la identificación del futuro suscriptor; o

ii) a falta de declaración, de prácticas de certificación, las condiciones enumeradas en el párrafo 2).

2) A falta de declaración de prácticas de certificación, la autoridad certificadora confirmará por su cuenta o por medio de un representante autorizado que:

a) el futuro suscriptor es la persona que debe figurar en el certificado que ha de expedirse;

b) si el futuro suscriptor actúa por medio de uno o varios representantes, el suscriptor autorizó al representante a conservar la clave privada del suscriptor y a solicitar la expedición de un certificado en que se consigne la correspondiente clave pública;

c) la información consignada en el certificado que debe expedirse es exacta;

d) el futuro suscriptor es el titular legal de la clave privada correspondiente a la clave pública que se consignará en el certificado;

e) el futuro suscriptor posee una clave privada con la que puede crear una firma numérica; y

f) la clave pública que se consignará en el certificado puede utilizarse para verificar una firma numérica adjuntada con la clave privada que está en posesión del futuro suscriptor.

Declaraciones efectuadas al expedirse el certificado

30. 1) Al expedir un certificado, la autoridad certificadora declara a cualquier persona que confíe razonablemente en el certificado o en la firma numérica verificable mediante la clave pública consignada en el certificado que la autoridad certificadora

ha expedido el certificado de conformidad con la eventual declaración aplicable de prácticas de certificación incorporada al certificado por remisión, o de la que la persona interesada tiene conocimiento.

2) A falta de tal declaración de prácticas de certificación, la autoridad certificadora declara que ha confirmado que:

a) la autoridad certificadora ha cumplido con todos los requisitos aplicables de la presente ley al expedir el certificado, y si la autoridad certificadora ha publicado el certificado o lo ha dado a conocer a tal persona, que el suscriptor cuyo nombre figura en el certificado lo ha aceptado;

b) el suscriptor cuyo nombre figura en el certificado posee la clave privada correspondiente a la clave pública consignada en el certificado;

c) la clave pública y la clave privada del suscriptor constituyen un par de claves complementarias;

d) toda la información consignada en el certificado es exacta, a menos que la autoridad certificadora haya manifestado en el certificado que la exactitud de la información especificada no está confirmada, o que haya incorporado por remisión al certificado una declaración en tal sentido; y

e) la autoridad certificadora no tiene conocimiento de ningún hecho material, que de haberse incluido en el certificado, hubiera restado fiabilidad a las declaraciones de los párrafos a) a d).

3) Cuando exista una declaración aplicable de prácticas de certificación que haya sido incorporada al certificado por remisión, o de la que la persona interesada tenga conocimiento, el párrafo 2) será aplicable en la medida en que las declaraciones no estén en contradicción con la declaración de prácticas de certificación.

Suspensión de un certificado

31. A menos que la autoridad certificadora y el suscriptor convengan otra cosa, la autoridad certificadora que haya expedido un certificado suspenderá el certificado lo antes posible después de recibir una solicitud de la persona que la autoridad certificadora tenga motivos razonables para considerar:

a) el suscriptor cuyo nombre figura en el certificado;

b) una persona debidamente autorizada a actuar en nombre de tal suscriptor; o

c) una persona que actúa en nombre de ese suscriptor, que no está disponible.

Revocación de un certificado

32. La autoridad certificadora revocará un certificado por ella expedido

a) tras recibir del suscriptor mencionado en el certificado una solicitud de revocación; y tras confirmar que la persona que solicita la revocación es el suscriptor, o es un representante del suscriptor facultado para solicitar la revocación;

b) tras recibir una copia certificada del certificado de defunción del suscriptor, o tras confirmar mediante otras pruebas que el suscriptor ha fallecido; o

c) tras serle presentados documentos referentes a la disolución de la empresa suscriptora, o tras confirmar con otras pruebas que la empresa suscriptora ha quedado disuelta o ha dejado de existir.

Revocación sin el consentimiento del suscriptor

33. 1) La autoridad certificadora revocará el certificado, independientemente de si el suscriptor mencionado en el certificado da su consentimiento, cuando la autoridad certificadora confirme que:

a) un hecho material expuesto en el certificado es falso;

b) no se ha cumplido un requisito para la expedición del certificado;

c) la clave privada o la fiabilidad del sistema de la autoridad certificadora están en entredicho de tal modo que la fiabilidad del certificado queda sustancialmente mermada;

d) un determinado suscriptor ha fallecido; o

e) una sociedad suscriptora ha sido disuelta, ha suspendido su funcionamiento o ha dejado de existir.

2) Al efectuar tal revocación, salvo en los casos previstos en los apartados d) y e) del párrafo 1), la autoridad certificadora avisará de inmediato al suscriptor cuyo nombre figure en el certificado revocado.

Aviso de suspensión

34. 1) Inmediatamente después de que la autoridad certificadora haya suspendido un certificado, la autoridad certificadora publicará un aviso firmado en que se dé cuenta de la suspensión en la entidad de registro especificada en el certificado a efectos de publicación del aviso de suspensión.

2) Cuando se especifique más de una entidad de registro, la autoridad certificadora publicará avisos firmados de la suspensión en todas esas entidades.

Aviso de revocación

35. 1) Inmediatamente después de que la autoridad certificadora haya revocado un certificado, la autoridad certificadora publicará un aviso firmado de la revocación en la entidad de registro especificada en el certificado a efectos de publicación de avisos de revocación.

2) Cuando se especifique más de una entidad de registro, la autoridad certificadora publicará avisos firmados de la revocación en todas esas entidades.

Artículo 12, párrafos 2) y 3) - Responsabilidad

Directrices de la Asociación de Abogados de los Estados Unidos (ABA)

3.14 Responsabilidad de la autoridad certificadora que cumple
La autoridad certificadora que cumpla las presentes Directrices y cualquier ley o contrato aplicable no será responsable de las pérdidas
1) sufridas por el suscriptor de un certificado expedido por dicha autoridad certificadora, o por cualquier otra persona; o
2) sufridas por haber confiado en un certificado expedido por la autoridad certificadora, en una firma numérica verificable por remisión a una clave pública consignada en un certificado, o en información consignada en dicho certificado o en un registro.

Proyecto de Directiva de la CE

Artículo 6. Responsabilidad
1. Como mínimo, los Estados Miembros velarán por que el proveedor de servicios de certificación, al expedir un certificado destinado al público cumpliendo los requisitos o al garantizar un certificado al público, sea responsable de los daños y perjuicios causados a toda persona que confíe razonablemente en el certificado y concretamente en:
a) la exactitud de toda la información consignada en el certificado en el momento de su expedición;
b) [....]
c) el hecho de que, en el momento de expedirse el certificado, la persona cuyo nombre figura en el certificado poseía los datos de creación de firmas correspondientes a los datos de verificación de firmas especificados o mencionados en el certificado;
d) el hecho de que los datos de creación de firmas y los datos de verificación de firmas pueden utilizarse de forma complementaria cuando el proveedor de servicios de certificación haya generado ambos tipos de datos;
a menos que el proveedor de servicios de certificación demuestre que no ha actuado con negligencia.
1a) Como mínimo, los Estados Miembros velarán por que el proveedor de servicios de certificación que haya expedido un certificado como certificado para el público cumpliendo los requisitos sea responsable de los daños y perjuicios causados a toda persona que confíe razonablemente en el certificado al no haberse registrado la revocación del certificado, a menos que el proveedor de servicios de certificación demuestre que no ha actuado con negligencia.
3. Los Estados Miembros asegurarán que el proveedor de servicios de certificación indique en el certificado que cumpla los requisitos los límites que afecten a la utilización de un determinado certificado, límites que deben ser discernibles por terceros. El proveedor de servicios de certificación no será responsable de los daños y perjuicios derivados de un uso contrario de un certificado que prevea tales límites.
4. Los Estados Miembros velarán por que el proveedor de servicios de certificación indique en el certificado que cumpla los requisitos un límite del valor de las transacciones para las que pueda utilizarse el certificado.

Missouri

Sección 17.1
Al especificar un límite recomendado de confianza en el certificado, la autoridad certificadora que lo expide y el suscriptor que lo acepta recomiendan a las personas que sólo confíen en el certificado si el riesgo total no es superior al límite recomendado de confianza.

Sección 17.2
A menos que la autoridad certificadora renuncie a la aplicación de la presente subsección, la autoridad certificadora titular de licencia
1) no será responsable de las pérdidas sufridas por haberse confiado en una firma numérica falsa o falsificada de un suscriptor si, con respecto a la firma numérica falsa o falsificada, la autoridad certificadora ha cumplido con todos los requisitos materiales de las secciones 1 a 27 de la presente ley;
2) no será responsable de sumas superiores al límite recomendado de confianza que se especifique en el certificado en caso de
a) pérdidas sufridas por haber confiado en una exposición falsa de algún hecho en el certificado que la autoridad certificadora deba confirmar; o
b) incumplimiento de la sección 10 de la presente ley al expedir el certificado;
3) será responsable únicamente por daños y perjuicios directos de compensación en acciones judiciales de resarcimiento por las pérdidas sufridas por haber confiado en el certificado. Estos daños y perjuicios no incluirán:
a) los daños y perjuicios punitivos o ejemplares;
b) los daños y perjuicios por pérdida de beneficios, ahorros u oportunidades; o

c) los daños y perjuicios por dolor o sufrimiento.

Singapur

Límites de responsabilidad para autoridades certificadoras titulares de licencias

45. A menos que la autoridad certificadora titular de licencia renuncie a la aplicación de la presente sección, la autoridad certificadora titular de licencia

a) no será responsable de ninguna pérdida sufrida por haberse confiado en la firma numérica falsa o falsificada de un suscriptor si, con respecto a la firma numérica falsa o falsificada, la autoridad certificadora titular de licencia ha cumplido los requisitos de la presente ley;

b) no será responsable de sumas superiores al límite recomendado de confianza que se especifique en el certificado en caso de

i) pérdidas sufridas por haber confiado en una exposición falsa de algún hecho en el certificado que la autoridad certificadora deba confirmar; o

ii) incumplimiento de las secciones 29 y 30 al expedir el certificado.

Artículo 13. Reconocimiento de certificados y firmas extranjeros

1) Al determinar si, o en qué medida, un certificado [una firma] surte efectos jurídicos, no se tomará en consideración el lugar en que se haya expedido el certificado [la firma] ni el Estado en que el expedidor tenga su establecimiento.

Variante A

2) Los certificados emitidos por un certificador de información extranjero se reconocerán como jurídicamente equivalentes a los emitidos por los certificadores de información que funcionen conforme a ... *[la ley del Estado promulgante]* cuando las prácticas del certificador extranjero ofrezcan un grado de fiabilidad por lo menos equivalente al requerido de los certificadores de conformidad con ... *[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) Las firmas 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 que cumplen con ... *[la ley del Estado promulgante]* cuando las leyes del otro Estado requieran un grado de fiabilidad por lo menos equivalente al requerido por esas 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].

4) Sin perjuicio de lo dispuesto en el párrafo anterior, las partes en transacciones comerciales y de otra índole podrán hacer constar que se debe utilizar un certificador de información, una clase de certificadores de información o una clase de certificados en relación con los mensajes o las firmas presentados a esas partes.

Variante B

2) Los certificados emitidos por un certificador de información extranjero se reconocerán como jurídicamente equivalentes a los certificados expedidos por certificadores de información sujetos a ... *[la ley del Estado promulgante]* cuando las prácticas del certificador de información extranjero ofrezca un grado de fiabilidad por lo menos equivalente al requerido de los certificadores de información sujetos a ... *[la ley del Estado promulgante]*.

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

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

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

b) fiabilidad de los sistemas de equipo y programas informáticos;

c) procedimientos para la tramitación de certificados y solicitudes de certificados y conservación de registros;

d) disponibilidad de información para los [firmantes] [titulares] identificados en certificados y para posibles partes que se fíen de los certificados;

e) regularidad y detalle de la auditoría hecha por un órgano independiente;

f) existencia de una declaración del Estado, un órgano acreditador o la autoridad certificadora acerca del cumplimiento o la existencia de lo antedicho;

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

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

Referencias a los documentos de la CNUDMI

A/CN.9/454; párr. 173;
A/CN.9/446; párrs. 196 a 207 (proyecto de artículo 19);
A/CN.9/WG.IV/WP.73, párr. 75;
A/CN.9/437, párr. 74 a 89 (proyecto de artículo I); y
A/AC.9/WG.IV/WP.71, párrs. 73 a 75.

Observaciones

69. El proyecto de artículo 13 regula las cuestiones que se trataron en el 31º período de sesiones del Grupo de Trabajo y que entonces se denominó “reconocimiento transfronterizo” (véase A/CN.9/437, párrs. 77 y 78). El párrafo 1) se basa en una propuesta formulada en el 34º período de sesiones del Grupo de Trabajo (A/CN.9/457, párr. 120) para que el Grupo de Trabajo se planteara la introducción de un artículo que prohibiera la discriminación de los certificados en función del lugar de expedición.

70. La variante A se basa en una sugerencia de combinación de varios párrafos que se formuló en el 32º período de sesiones del Grupo de Trabajo (véase A/CN.9/446, párrs. 197 a 204). El texto especifica las condiciones en el Estado promulgante para reconocer los certificados expedidos por certificadores de información extranjeros, así como las firmas sujetas a la legislación de otro Estado. El párrafo 4) refleja la opinión general del Grupo de Trabajo de que debe reconocerse a las partes en transacciones comerciales y de otro tipo el derecho a elegir el certificador de información, la clase de certificador de información o la clase de certificado que deseen utilizar para los mensajes o firmas que reciban. En el concepto de partes en transacciones comerciales y de otra índole entrarían también los órganos gubernamentales con funciones comerciales.

71. En la variante B figura una lista ilustrativa de criterios que deben tenerse en cuenta al evaluar la fiabilidad de certificados extranjeros.

Referencias a legislación nacional y a otros textos

Proyecto de Directiva de la CE

Artículo 7 Aspectos internacionales

1. Los Estados Miembros velarán por que los certificados expedidos para el público y cumpliendo los requisitos por un roveedor de servicios de certificación establecido en un tercer país sean reconocidos como jurídicamente equivalentes a los certificados expedidos por un proveedor de servicios de certificación establecido en la Comunidad Europea:

a) si el proveedor de servicios de certificación cumple los requisitos establecidos en la presente Directiva y ha sido acreditado en el contexto de un plan de acreditación voluntaria establecido en un Estado Miembro de la Comunidad Europea; o

b) si un proveedor de servicios de certificación establecido en la Comunidad, que cumpla los requisitos enunciados en la presente Directiva, garantiza el certificado; o

c) si el certificado o el proveedor de servicios de certificación están reconocidos conforme al régimen de un acuerdo bilateral o multilateral entre la Comunidad y terceros países u organizaciones internacionales.

2. A fin de facilitar los servicios de certificación transfronteriza con terceros países y el reconocimiento jurídico de firmas electrónicas avanzadas creadas en terceros países, la Comisión hará, en su caso, las propuestas pertinentes para lograr la efectiva aplicación de las normas y de los acuerdos internacionales aplicables a los servicios de certificación. En particular y cuando resulte necesario, presentará propuestas al Consejo sobre mandatos apropiados para la negociación de acuerdos bilaterales y multilaterales con terceros países y organizaciones internacionales. El Consejo decidirá por mayoría cualificada.

Alemania

§15 Certificados extranjeros

1) Las firmas numéricas que puedan verificarse mediante una clave criptográfica pública para la que exista un certificado extranjero de otro Estado Miembro de la Unión Europea o de otro Estado contratante del Tratado sobre el Espacio Económico Europeo serán equivalentes a las firmas numéricas reguladas por la presente ley, siempre y cuando se demuestre que tienen un nivel equivalente de seguridad.

2) El párrafo 1 se aplicará también a otros Estados que hayan celebrado acuerdos supranacionales o internacionales de reconocimiento de certificados.

Illinois

Artículo 25. Utilización de firmas y registros electrónicos por organismos estatales

Sección 25-115. Compatibilidad

En la medida en que sea razonable en función de las circunstancias, las reglas adoptadas por el Departamento de Servicios Centrales de Gestión o por un organismo estatal en relación con la utilización de registros electrónicos o firmas electrónicas se redactarán de forma que se aliente y promueva la coherencia y la armonía con requisitos similares adoptados por organismos gubernamentales de otros Estados y por las entidades gubernamentales federales.

Singapur

Décima parte. Reglamentación de las autoridades certificadoras

Reconocimiento de las autoridades certificadoras extranjeras

43. El Ministro podrá dictar disposiciones en virtud de las cuales el contralor podrá reconocer autoridades certificadoras cuyas sedes se encuentren fuera del territorio de Singapur y que cumplan los requisitos prescritos para cada uno de los siguientes fines:

a) el límite recomendado de confianza eventualmente especificado en un certificado expedido por la autoridad certificadora;

b) la presunción a que se hace referencia en las secciones 20 b) ii) [tratamiento de las firmas numéricas como firmas electrónicas seguras en ciertas circunstancias] y 21 [presunción de que el certificado es correcto si es aceptado por el suscriptor].

Notas

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

2/ Ibíd., *quincuagésimo segundo período de sesiones, Suplemento Nº 17* (A/52/17), párrs. 249 a 251.

3/ Ibíd., *quincuagésimo tercer período de sesiones, Suplemento Nº 17* (A/53/17), párr. 208.