NACIONES UNIDAS **A**

Asamblea General

A/CN.9/WG.IV/WP.84
Distr. LIMITADA
8 de diciembre de 1999
ESPAÑOL

Original: INGLÉS

COMISIÓN DE LAS NACIONES UNIDAS PARA
EL DERECHO MERCANTIL INTERNACIONAL
Grupo de Trabajo sobre Comercio Electrónico
36º período de sesiones
Nueva York, 14 a 25 de febrero de 2000

PROYECTO DE RÉGIMEN UNIFORME PARA LAS FIRMAS ELECTRÓNICAS

Nota de la Secretaría

ÍNDICE

V.99-90618

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 "proyecto de Régimen Uniforme para las Firmas Electrónicas" o "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 adoptada por la Ley Modelo de la CNUDMI sobre 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. 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[4].

10. El Grupo de Trabajo continuó la preparación del proyecto de Régimen Uniforme en su 35º período de sesiones (Viena, septiembre de 1999) sobre la base de una nota preparada por la Secretaría (A/CN.9/WG.IV/WP.82). El informe de ese período de sesiones figura en el documento A/CN.9/465.

11. La presente nota contiene los proyectos de artículo revisados a la luz de las deliberaciones y decisiones del Grupo de Trabajo, así como de la Comisión en su 32º período de sesiones, anteriormente reseñadas (véanse los párrafos 6 a 9 *supra*). Las disposiciones nuevamente revisadas van subrayadas. Para facilitar la consulta, se adjunta como anexo I de la presente nota un texto consolidado de los proyectos de artículo.

12. 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

13. 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*;

- Directiva de la CE: Directiva del Parlamento Europeo y del Consejo acerca de un marco común para las firmas electrónicas, adoptada el 30 de noviembre de 1999 (PE-CONS 3625/99);

- GUIDEC: Cámara de Comercio Internacional, “Uso general en el comercio internacional asegurado digitalmente”, 1997.

I. OBSERVACIONES GENERALES

14. 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.

15. 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.

16. 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).

17. 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 jurídico aparte.

18. 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.

19. 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". En el 35º período de sesiones del Grupo de Trabajo, se abogó en favor de retener el concepto de "firma electrónica refrendada" por considerarlo particularmente apto para dotar de certeza a la utilización de un determinado tipo de firmas electrónicas, concretamente las firmas numéricas aplicadas mediante una infraestructura de clave pública (ICP). Pero se adujo en contra que el concepto de "firma electrónica refrendada" daba una complejidad innecesaria a la estructura del Régimen Uniforme. Además, ese concepto se prestaría a interpretaciones erróneas al dar a entender que a diversos grados de fiabilidad técnica podría corresponder una gama igualmente diversificada de efectos jurídicos. Se expresó inquietud general ante el peligro de que se tomara la firma electrónica refrendada por un concepto jurídico bien definido, cuando no pasaba de ser una colección de criterios técnicos cuya observancia dotaría a un método de firma de mayor fiabilidad. Si bien el Grupo de Trabajo aplazó su decisión final sobre si el Régimen Uniforme debía o no basarse en el concepto de "firma electrónica refrendada", se convino en general en que, al preparar un proyecto revisado de Régimen Uniforme para reanudar las deliberaciones en un futuro período de sesiones, sería útil introducir en él una versión de los proyectos de artículo que no dependiera de ese concepto (A/CN.9/465, párr. 66).

20. 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 "firma electrónica refrendada" en el proyecto de artículo 2 b) se ha mantenido entre corchetes pero no se utiliza en ninguna de las disposiciones sustantivas del Régimen Uniforme. Cuando procede, las partes pertinentes de esa definición se han insertado en las disposiciones correspondientes. La finalidad de esta opción es ayudar al Grupo de Trabajo a decidir si deberían eliminarse 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 una posible modificación de la definición figuran en la parte correspondiente del artículo 2. Las observaciones sobre propuestas concretas se comentan en los párrafos correspondientes a los artículos respectivos.

21. Tal como acordó el Grupo de Trabajo en su 35º período de sesiones, este proyecto revisado de Régimen Uniforme se basa en el supuesto de que la referencia a situaciones en que "la ley requiere una firma" no se limita a los casos en que se utiliza una firma electrónica para cumplir con el requisito legal imperativo de que ciertos documentos han de ser firmados para ser válidos. Dado que la ley impone muy pocos requisitos de esta índole con respecto a los documentos utilizados en operaciones comerciales, el resultado práctico de esa interpretación errónea sería reducir indebidamente el alcance del Régimen Uniforme. De acuerdo con la interpretación de las palabras "la ley" adoptada por la Comisión en el párrafo 68 de la Guía para la incorporación de la Ley Modelo al derecho interno (según la cual debía entenderse que las palabras "la ley" no sólo se referían a "disposiciones de derecho legislativo o reglamentario sino también a otras normas de derecho jurisprudencial y de derecho procesal"), el Régimen Uniforme (y la Ley Modelo) tenían por objeto abarcar de manera muy amplia la utilización de firmas electrónicas, ya que la mayoría de los documentos utilizados en el contexto de operaciones comerciales probablemente tendrían que ajustarse, en la práctica, a los requisitos legales impuestos para la prueba por escrito (A/CN.9/465, párr. 67).

II. PROYECTOS DE ARTÍCULO SOBRE LAS FIRMAS ELECTRÓNICAS

Artículo 1. Ámbito de aplicación

El presente Régimen será aplicable a todo supuesto en el que se utilicen firmas electrónicas en el contexto* de actividades comerciales**. No derogará ninguna norma jurídica destinada a la protección del consumidor.

* La Comisión propone el texto siguiente para los Estados que deseen ampliar el ámbito de aplicación del presente Régimen:

"El presente Régimen será aplicable a todo supuesto en el que se utilicen firmas electrónicas, excepto en las situaciones siguientes: [...]."

** 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. 36 a 42;
A/CN.9/WG.IV/WP.82, párr. 21;
A/CN.9/457, párrs. 53 a 64.

Observaciones

22. Se han revisado las palabras iniciales del proyecto de artículo 1 a fin de garantizar la coherencia con el artículo 1 de la Ley Modelo (véase el documento A/CN.9/465, párr. 38). La nota* tiene por objeto reflejar la misma política adoptada en el contexto de la Ley Modelo, según la cual "nada en la Ley Modelo debería impedir a un Estado que al aplicarla ampliara su alcance a aplicaciones no comerciales del llamado comercio electrónico" (Guía para la incorporación de la Ley Modelo al derecho interno, párr. 26). El Grupo de Trabajo decidió en su 35º período de sesiones que esa política debería aplicarse también a supuestos en los que se utilizaran firmas electrónicas (ibíd., párr. 39).

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] [titular de la clave] [suscriptor] [titular del dispositivo de firma] [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.9/465, párr. 42;
A/CN.9/WG.IV/WP.82, párrs. 22 a 33;
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

23. En su 35º período de sesiones, el Grupo de Trabajo decidió aplazar el examen de las definiciones que figuran en el proyecto de artículo 2 hasta que hubiera concluido su examen de las disposiciones de fondo del Régimen Uniforme (A/CN.9/465, párr. 42).

Definición de "firma electrónica"

24. La definición de firma electrónica ha sido redactada 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]”) se incluyen 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”

25. En su 35º período de sesiones, el Grupo de Trabajo examinó si en el Régimen Uniforme debía utilizarse el concepto de “firma electrónica refrendada”. Se abogó en favor de retener el concepto de firma electrónica refrendada, por considerarlo particularmente apto para dotar de certeza a la utilización de un determinado tipo de firmas electrónicas, concretamente las firmas numéricas aplicadas mediante una infraestructura de clave pública (ICP). Pero se adujo en contra que el concepto de “firma electrónica refrendada” daba una complejidad innecesaria a la estructura del Régimen Uniforme. Además, ese concepto se prestaría a interpretaciones erróneas al dar a entender que a diversos grados de fiabilidad técnica podría corresponder una gama igualmente diversificada de efectos jurídicos. Se expresó inquietud general ante el peligro que se tomara la firma electrónica refrendada por un concepto jurídico bien definido, cuando no pasaba de ser una colección de criterios técnicos cuya observancia dotaría a un método de firma de mayor fiabilidad. Si bien el Grupo de Trabajo aplazó su decisión final sobre si el Régimen Uniforme debía o no basarse en el concepto de “firma electrónica refrendada”, se convino en general en que, al preparar un proyecto revisado de Régimen Uniforme para reanudar las deliberaciones en un futuro período de sesiones, sería útil introducir en él una versión de los proyectos de artículo que no dependiera de ese concepto (A/CN.9/465, párr. 66).

26. De conformidad con la decisión adoptada por el Grupo de Trabajo en su 34º período de sesiones (A/CN.9/457, párr. 39), la definición de “firma electrónica refrendada” incluye 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).

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

28. 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 del dispositivo de 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 Régimen Uniforme, por ejemplo, de los artículos 8, 9 y 11. 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.

29. 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 del dispositivo de 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.

30. 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 el proyecto de artículo 9 que prevé las obligaciones de "cada" titular del dispositivo de firma. Esta cuestión también se plantea en relación con la definición de "titular de la firma", que figura más adelante.

31. En el apartado iii) del párrafo b) las palabras "garantice con fiabilidad" tienen por objeto mantener la coherencia con la terminología del artículo 8 de la Ley Modelo.

Definición de "certificado"

32. Quizá sea necesaria una definición de "certificado" 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 del dispositivo de 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).

33. 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" o "dispositivo para la creación de firmas", 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"

34. 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"

35. 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, como se señala en el párrafo 30. En vista de la propuesta presentada

en el 35º período de sesiones del Grupo de Trabajo, en la presente nota la expresión "titular de la firma" se ha sustituido por "titular del dispositivo de firma" (véase el documento A/CN.9/465, párrs. 78 a 82).

Definición de "certificador de información"

36. 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 expiden certificados, debe quedar comprendida también la expedición de certificados como parte secundaria de la actividad de una entidad. Teniendo en cuenta una sugerencia formulada en el 35º período de sesiones del Grupo de Trabajo, en todo el resto del Régimen Uniforme el término "certificador de información" se ha sustituido por el término "proveedor de servicios de certificación" (A/CN.9/465, párr. 125). El Grupo de Trabajo tal vez desee tomar una decisión acerca de qué terminología debe utilizarse.

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.

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.
2. 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.

3. 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.
4. 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.
5. Por "dispositivo para la creación de firmas" se entenderá una dotación lógica o física configurada para ejecutar los datos de creación de firmas.
6. Por "dispositivo para la creación segura de firmas" se entenderá un dispositivo para la creación de firmas que cumple los requisitos estipulados en el anexo III.
7. Por "datos de verificación de firmas" se entenderán datos como códigos o claves criptográficas públicas que se utilizan para verificar la firma electrónica.
8. Por "dispositivo de verificación de firmas" se entenderá una dotación lógica o física configurada para ejecutar los datos de verificación de firmas.
9. 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.
10. Por "certificado apropiado" se entenderá un certificado que cumple los requisitos establecidos en el anexo I y ha sido proporcionado por un proveedor de servicios de certificación que cumple los requisitos establecidos en el anexo II;
11. Por "proveedor de servicios de certificación" se entenderá una entidad o persona física o jurídica que emite certificados o presta otros servicios relacionados con firmas electrónicas; [...].

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.

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).

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. [Neutralidad respecto de la tecnología] [Igualdad de tratamiento de las firmas]

Ninguna de las disposiciones del presente Régimen se aplicará de modo que excluya, restrinja o prive de efecto jurídico cualquier método [de firma electrónica] [que cumpla los requisitos mencionados en el párrafo 1) del artículo 6 del presente Régimen] [que sea tan fiable como sea apropiado 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] [o que de algún otro modo cumpla con los requisitos del derecho aplicable].

Referencias a documentos de la CNUDMI

A/CN.9/465, párrs. 43 a 48;
A/CN.9/WG.IV/WP.82, párr. 34;
A/CN.9/457, párrs. 53 a 64.

Observaciones

37. El proyecto de artículo 3 tiene por objeto reflejar algunas de las propuestas de redacción formuladas en el contexto del 35º período de sesiones del Grupo de Trabajo (A/CN.9/465, párrs. 47 y 48). Al examinar el

proyecto de artículo 3, el Grupo de Trabajo tal vez desee decidir si el Régimen Uniforme debe dejar claro que cualquier método que se utilice o contemple cuya finalidad no sea crear el equivalente funcional de una firma manuscrita jurídicamente significante (es decir, un método que cumpla con los requisitos del proyecto de artículo 6 o que de algún otro modo cumpla con los requisitos del derecho aplicable) no entra en el ámbito del Régimen Uniforme.

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.

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.

Referencias a documentos de la CNUDMI

A/CN.9/465, párrs. 49 y 50;
A/CN.9/WG.IV/WP.82, párr. 35.

Observaciones

38. El fondo del proyecto de artículo 4 ha sido acordado en líneas generales por el Grupo de Trabajo en su 35º período de sesiones (A/CN.9/465, párr. 50).

Artículo 5. [Modificación mediante acuerdo] [Autonomía de las partes] [Autonomía contractual]

Salvo que el presente Régimen o el derecho del Estado promulgante dispongan otra cosa, las partes podrán convenir en apartarse del presente Régimen o en modificarlo [modificar su efecto].

Referencias a documentos de la CNUDMI

A/CN.9/465, párrs. 51 a 61;
A/CN.9/WG.IV/WP.82, párrs. 36 a 40;
A/CN.9/457, párrs. 53 a 64.

Observaciones

39. El texto del proyecto de artículo 5 refleja una propuesta que fue ampliamente apoyada por el Grupo de Trabajo en su 35º período de sesiones (A/CN.9/465, párr. 59), con objeto de garantizar la autonomía de las partes para concertar acuerdos con el fin de apartarse de las disposiciones del presente Régimen o modificarlas. Esta disposición relativa a la autonomía se refiere tan sólo al presente Régimen y no tiene por objeto afectar a las leyes de orden público o a las disposiciones imperativas aplicables a los contratos, como las disposiciones relativas a los contratos leoninos.

40. El texto entre corchetes se ha incluido como posible formulación para ajustarse más al texto del artículo 6 de la Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías (denominada en adelante "Convención sobre la Compraventa"), tal como sugirió el Grupo de Trabajo (ibíd., párr. 61).

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

1) Cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos si se utiliza [un método] [una firma electrónica] que es tan fiable como sea apropiado 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.

2) El párrafo 1) será aplicable tanto si el requisito previsto en él está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que no exista una firma.

Variante A

3) Se presumirá que [un método] [una firma electrónica] es fiable a efectos del cumplimiento del requisito enunciado en el párrafo 1) si ese método garantiza que:

a) los datos utilizados para la creación de una firma electrónica son exclusivos del titular del dispositivo [para la creación] de firmas en el contexto en que se utilicen;

b) el titular del dispositivo [para la creación] de firmas [tiene] [tenía en el momento pertinente] el control exclusivo de dicho dispositivo;

c) la firma electrónica está vinculada [a la información] [al mensaje de datos o a la parte de ese mensaje] al que corresponde [de modo que garantice la integridad de esa información];

d) el titular del dispositivo [para la creación] de firmas está objetivamente identificado en el contexto [en que se utiliza el dispositivo] [del mensaje de datos].

Variante B

3) A falta de prueba en contrario, se presumirá que la utilización de una firma electrónica demuestra:

a) la conformidad de la firma electrónica con la norma de fiabilidad enunciada en el párrafo 1);

b) la identidad del presunto signatario; y

c) la aprobación por el presunto signatario de la información a la que corresponde la firma electrónica.

4) La presunción enunciada en el párrafo 3) será válida únicamente en el caso de que:

a) la persona que pretende confiar en la firma electrónica notifique al presunto signatario que se confía en la firma electrónica [como equivalente de la firma manuscrita del presunto signatario] [como prueba de los elementos indicados en el párrafo 3)]; y

b) el presunto signatario no comunique prontamente a la persona que efectúe una notificación tal como se prevé en el apartado a) las razones por las que no debe confiarse en la firma electrónica [como equivalente de la firma manuscrita del presunto signatario] [como prueba de los elementos indicados en el párrafo 3)].

Variante C

3) A falta de prueba en contrario, se presumirá que la utilización de una firma electrónica demuestra:

a) la conformidad de la firma electrónica con la norma de fiabilidad enunciada en el párrafo 1);

b) la identidad del presunto signatario; y

c) la aprobación por el presunto signatario de la información a la que corresponde la firma electrónica.

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

Referencias a documentos de la CNUDMI

A/CN.9/465, párrs. 62 a 82;
A/CN.9/WG.IV/WP.82, párrs. 42 a 44;
A/CN.9/457, párrs. 48 a 52;
A/CN.9/WG.IV/WP.80, párrs. 11 y 12.

Observaciones

41. Los párrafos 1) y 2) y el último párrafo del proyecto de artículo 6 introducen disposiciones tomadas de los artículos 7 1) b), 7 2) y 7 3) de la Ley Modelo, respectivamente. En la definición de “firma electrónica” que figura en el proyecto de artículo 2 a) se incluyen expresiones inspiradas por el artículo 7 1) a) de la Ley Modelo. Sin embargo, en el proyecto de artículo 2 a) se describe un método que “pueda” ser utilizado para cumplir las funciones de una firma indicadas en el artículo 7 1) a) de la Ley Modelo. En caso de que desee hacer hincapié en que la principal finalidad del párrafo 1) es prever el caso en que se utiliza como firma (es decir, con la intención de crear el equivalente funcional de una firma manuscrita) algún tipo de firma electrónica (incluidos los métodos de autenticación “no refrendados”), el Grupo de Trabajo puede estimar más apropiado reproducir el texto íntegro del artículo 7 1) de la Ley Modelo. El párrafo 1) podría decir lo siguiente:

“1) Cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos:

a) si se utiliza [un método] [una firma electrónica] para identificar a esa persona y para indicar que esa persona aprueba la información que figura en el mensaje de datos; y

b) si [ese método] [esa firma electrónica] es tan fiable como sea apropiado 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”.

42. En el 35º período de sesiones del Grupo de Trabajo se sugirió que tal vez fuera necesario incluir en el proyecto de artículo 6 una disposición del siguiente tenor: “Las consecuencias jurídicas de la utilización de una

firma serán igualmente aplicables al empleo de firmas electrónicas" (véase el documento A/CN.9/465, párr. 74). El Grupo de Trabajo quizás desee examinar en qué medida ese concepto de equivalencia entre firmas manuscritas y electrónicas debe expresarse detalladamente en las disposiciones del Régimen Uniforme o si podría ser suficiente (y más coherente con la Ley Modelo) indicar en la guía para la incorporación del Régimen Uniforme al derecho interno (que se preparará más adelante) que, al interpretar el párrafo 1), debe tenerse presente que la finalidad de esa disposición era garantizar que, cuando se derivara una consecuencia jurídica de la utilización de una firma manuscrita, debía derivarse la misma consecuencia de la utilización de una firma electrónica fiable.

43. Como se indicó en el informe del 35º período de sesiones del Grupo de Trabajo (A/CN.9/465, párr. 64), el párrafo 1), en la medida en que reproduce el artículo 7 1) de la Ley Modelo, se refiere a la determinación de lo que constituye un método de firma fiable a la luz de todas las circunstancias del caso. Conforme al artículo 7 de la Ley Modelo esa determinación sólo puede ser efectuada por un tribunal u otro verificador de los hechos que intervenga *ex post*, posiblemente mucho tiempo después de haberse utilizado la firma electrónica. En cambio, el beneficio esperado del Régimen Uniforme en favor de ciertas técnicas, consideradas particularmente fiables independientemente de las circunstancias en que se utilizan, es crear certeza (ya sea mediante una presunción o una regla de fondo), en el momento de utilizarse una determinada técnica de firma electrónica o antes de esa utilización (*ex ante*), de que se obtendrían con ella efectos jurídicos equivalentes a los de una firma manuscrita. Esa es la finalidad del párrafo 3).

44. La Variante A del párrafo 3) se basa en un texto propuesto y examinado en el 35º período de sesiones del Grupo de Trabajo (A/CN.9/465, párrs. 78 a 82) para expresar criterios objetivos de fiabilidad técnica de las firmas electrónicas. En el apartado c) se ha expresado la vinculación necesaria entre la firma y la información firmada a fin de evitar la implicación de que la firma electrónica podría aplicarse tan sólo al contenido íntegro de un mensaje de datos. De hecho, la información que se firma, en muchos casos, será tan sólo una parte de la información contenida en el mensaje de datos.

45. Al examinar las Variantes B y C, el Grupo de Trabajo tal vez desee aclarar, como cuestión de principio, si el Régimen Uniforme, al establecer los criterios de "fiabilidad" de una firma electrónica, debería ocuparse exclusivamente de las cuestiones de fiabilidad técnica previstas en la Variante A o si deberían tenerse en cuenta otros factores, como alternativa o añadido a la Variante A.

46. La Variante B es el resultado de una propuesta formulada en el 35º período de sesiones del Grupo de Trabajo (A/CN.9/465, párrs. 74 y 75). Si la adopción de la Variante B entraña la eliminación de todo vínculo entre un determinado nivel de fiabilidad técnica, por una parte, y las consecuencias jurídicas que resultarían de la utilización de firmas electrónicas, por otra, el efecto de los párrafos 3) y 4) sería crear, a favor de cualquier técnica que pudiera utilizarse para producir una firma electrónica, lo que en ocasiones se ha denominado una "presunción de bajo nivel", es decir, una presunción que podría ser fácilmente rebatida por el presunto signatario mediante una simple declaración. El Grupo de Trabajo quizás desee decidir, como cuestión de principio, si el intercambio de notificaciones previsto en la Variante B puede imponerse de manera realista a quienes utilizan firmas electrónicas, y si ese intercambio de notificaciones sería un método tan fácil de utilizar como se prevé y tendría como resultado una certeza predeterminada en cuanto a los efectos jurídicos de las firmas electrónicas.

47. La Variante C es el resultado de una propuesta formulada en el 35º período de sesiones del Grupo de Trabajo (A/CN.9/465, párr. 76). A diferencia de la Variante B, no ofrece un mecanismo para rebatir fácilmente la presunción que crea. En vista de que la "prueba en contrario" podría requerir investigaciones costosas y detalladas de los diversos dispositivos y procedimientos técnicos que intervienen en la creación de la firma electrónica, el efecto de la Variante C sería crear una presunción muy fuerte en cuanto a la efectividad jurídica de cualquier técnica utilizada para producir una firma electrónica.

Referencias a legislación nacional y otros textos

Directiva de la Comunidad Europea

Artículo 5
Efectos jurídicos de las firmas electrónicas
1. Los Estados Miembros garantizarán que las firmas electrónicas avanzadas que se basan en un certificado apropiado y se crean mediante un dispositivo para la creación segura de firmas:
a) cumplen los requisitos jurídicos de una firma en relación con datos en forma electrónica de la misma manera que una firma manuscrita cumple esos requisitos en relación con datos sobre soporte de papel; y
b) son admisibles como prueba en procedimientos judiciales.
2. Los Estados Miembros garantizarán que no se niegue la efectividad jurídica ni la admisibilidad como prueba en procedimientos judiciales de una firma electrónica por la simple razón de que:
- es en forma electrónica, o
- no se basa en un certificado apropiado, o
- no se basa en un certificado apropiado expedido por un proveedor acreditado de servicios de certificación, o
- no ha sido creada mediante un dispositivo para la creación segura de firmas.

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) Se presumirá que un mensaje de datos es en su forma original cuando, en relación con ese mensaje de datos, se utilice [un método] [una firma electrónica] [de acuerdo con el artículo 6] que:

a) 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; y

b) de requerirse que la información sea presentada, dicha información puede ser mostrada a la persona a quien se deba presentar;

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

Referencias a documentos de la CNUDMI

A/CN.9/465, párrs. 83 a 89;
A/CN.9/WG.IV/WP.82, párr. 45;
A/CN.9/457, párrs. 48 a 52;
A/CN.9/WG.IV/WP.80, párrs. 13 y 14.

Observaciones

48. El texto del proyecto de artículo 7 es el resultado de la decisión adoptada por el Grupo de Trabajo en su 35º período de sesiones (A/CN.9/465, párr. 89). La finalidad del proyecto de artículo 7 es confirmar la conexión con el artículo 8 de la Ley Modelo y el requisito de la integridad. En su redacción actual, el párrafo 1) no implica ningún vínculo entre la función de conservar la integridad de la información y la función de la firma indicada en el proyecto de artículo 6. La independencia de los dos artículos, que pueden aplicarse conjuntamente o por separado a diversas técnicas de autenticación, se basa en un reconocimiento del hecho de que, en un soporte de papel, la dos funciones pueden también concebirse por separado.

Artículo 8. Cumplimiento de los artículos 6 y 7

Variante A

1) *[El órgano o la entidad designada por el Estado promulgante como competente]* podrá determinar qué métodos 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.

Variante B

1) Cabrá determinar que uno o más métodos de firma electrónica 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.9/465, párrs. 90 a 98;
A/CN.9/WG.IV/WP.82, párr. 46;
A/CN.9/457, párrs. 48 a 52;
A/CN.9/WG.IV/WP.80, párr. 15.

Observaciones

49. 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 beneficiarse de las presunciones establecidas en los proyectos de artículo 6 y 7. Según decidió el Grupo de Trabajo en su 35º período de sesiones,

el proyecto de artículo 8 no debía interpretarse de manera que prohibiera a los usuarios, por ejemplo, utilizar técnicas que no cumplieran con los requisitos enunciados en los proyectos de artículo 6 y 7, si así lo acordaban entre ellos. Las partes también deberían ser libres para probar, ante un tribunal judicial o arbitral, que el método de firma por ellas seleccionado cumplía con los requisitos de los proyectos de artículo 6 y 7, aun cuando no hubiera sido objeto de una determinación previa a tal efecto. No debía considerarse que el proyecto de artículo 8 recomendaba a los Estados un único procedimiento para lograr el reconocimiento de una tecnología de firma, sino que más bien indicaba los límites aplicables en el supuesto de que un Estado deseara adoptar ese enfoque. Quizás fuera necesario explicitar claramente esas consideraciones, posiblemente en una guía para la incorporación del Régimen Uniforme al derecho interno (véase el documento A/CN.9/465, párr. 93).

50. La finalidad de las Variantes A y B es alentar a los Estados a que garanticen que las determinaciones efectuadas a tenor del párrafo 1) se ajustan a las normas internacionales aplicables, facilitando así la armonización de las prácticas con respecto a las firmas electrónicas refrendadas y la utilización y reconocimiento de firmas a través de las fronteras. La Variante A se refiere a una posible intervención del Estado en la designación de un órgano o entidad competente para evaluar la fiabilidad técnica de las técnicas de firma (independientemente de que ese órgano sea una entidad pública o privada). La Variante B, a fin de no recalcar excesivamente la función del Estado en las determinaciones mencionadas en el párrafo 1), deja abierta la posibilidad de que el órgano o autoridad designado para evaluar la fiabilidad técnica de las técnicas de firma sea establecido por el Estado (como órgano estatal o entidad privada) o dependa solamente de la industria.

51. Una propuesta formulada en el contexto del 35º período de sesiones del Grupo de Trabajo (a saber, que "toda determinación que se efectúe debería tener en cuenta no sólo si determinados métodos cumplían con los requisitos de los proyectos de artículo 6 y 7 sino también el grado o medida en que se cumplían dichos requisitos") no se ha reflejado en la versión revisada del proyecto de artículo 8. El Grupo de Trabajo quizá desee aclarar si se considera que un requisito como la utilización de una firma manuscrita (o la presentación de un documento original) podría satisfacerse sólo en parte con respecto a un documento procesado en un medio electrónico, lo que parecería apartarse del criterio de la equivalencia funcional adoptado durante la preparación de la Ley Modelo y el Régimen Uniforme. Si la intención del Grupo de Trabajo es simplemente indicar que una firma electrónica (o un método que garantice la integridad) no se aplica necesariamente a todo el contenido de un mensaje de datos pero debería poder aplicarse tan sólo a una parte seleccionada de la información contenida en un determinado mensaje, es fácil hacer constar dicha indicación en la guía para la incorporación del Régimen Uniforme al derecho interno.

Artículo 9. Responsabilidades del titular del dispositivo de firma

1) Cada titular del dispositivo de firma deberá:

a) Actuar con diligencia razonable para evitar la utilización no autorizada de su dispositivo de firma;

b) Dar aviso a quien corresponda sin demora injustificada en caso de que:

i) el titular del dispositivo de firma tenga conocimiento de que el dispositivo de firma ha quedado en entredicho; o
ii) las circunstancias conocidas por el titular del dispositivo de firma den lugar a un riesgo sustancial de que el dispositivo de firma pueda haber quedado en entredicho;

c) [Cuando se utilice un certificado para avalar el dispositivo de firma,] [Cuando el dispositivo de firma entrañe la utilización de un certificado,] actuar con diligencia razonable para velar por la exactitud

y la integridad de todas las declaraciones pertinentes efectuadas por el titular del dispositivo de firma que sean de interés para el [ciclo vital del] certificado, o que deban consignarse en el certificado.

2) El titular del dispositivo de firma será responsable del incumplimiento de los requisitos del párrafo 1).

Referencias a documentos de la CNUDMI

A/CN.9/465, párrs. 99 a 108;
A/CN.9/WG.IV/WP.82, párrs. 50 a 55;
A/CN.9/457, párrs. 65 a 98;
A/CN.9/WG.IV/WP.80, párrs. 18 y 19.

Observaciones

52. El fondo del proyecto de artículo 9 ha sido aprobado en general por el Grupo de Trabajo en su 35º período de sesiones. En el párrafo 1) se ha introducido la referencia a "cada" titular a fin de reflejar la opinión general de que en determinados casos podía ser injusto disponer que cada uno de los titulares del dispositivo fuese responsable de la totalidad de la pérdida eventualmente resultante de la utilización no autorizada del dispositivo (por ejemplo, en caso de utilización no autorizada de un dispositivo de firma social en manos de varios empleados). En consecuencia, cada titular debería ser tan sólo responsable en la medida en que personalmente no hubiera cumplido con los requisitos del párrafo 1) (véase el documento A/CN.9/465, párr. 105).

53. El párrafo 2) se basa en la conclusión a que llegó el Grupo de Trabajo en su 35º período de sesiones de que podría ser difícil lograr el consenso en cuanto a las consecuencias que pudieran derivarse de la responsabilidad del titular del dispositivo de firma. Según el contexto en que se utilizase la firma electrónica, esas consecuencias podrían ir, conforme al derecho vigente, desde que el titular del dispositivo de firma quedase vinculado por el contenido del mensaje hasta la obligación de pagar daños y perjuicios. En consecuencia, el párrafo 2) simplemente establece el principio de que el titular del dispositivo de firma debería responder del incumplimiento de los requisitos del párrafo 1) y deja que la ley aplicable fuera del ámbito del Régimen Uniforme en cada Estado promulgante se ocupe de las consecuencias jurídicas que acarrearía esa responsabilidad (ibíd., párr. 108). También se expresó la opinión de que en el proyecto de artículo 9 debería haberse introducido una norma basada en un criterio de previsibilidad del daño (de un tenor similar al del artículo 74 de la Convención sobre la Compraventa y que reafirmara una norma básica que se aplicaría en muchos países conforme a la legislación directamente aplicable) (ibíd., párr. 107).

Referencias a legislación nacional y a otros textos

Párrafo 1) a) - declaraciones pertinentes

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

4.2 Obligaciones del suscriptor
Todas las declaraciones pertinentes que haga un suscriptor a una autoridad certificadora, incluida toda la información que pose a 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 pertinentes 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.

Párrafo 2) - 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. Responsabilidades del proveedor de servicios de certificación

1) Todo proveedor de servicios de certificación deberá:

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

b) obrar con la debida diligencia para velar por la exactitud y la integridad de todas las declaraciones pertinentes efectuadas por el proveedor de servicios de certificación que sean de interés para el ciclo vital del certificado o que estén consignadas en el certificado;

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

i) la identidad del proveedor de servicios de certificación;

ii) que la persona nombrada en el certificado posee, en el momento pertinente, el dispositivo de firma que se menciona en el certificado;

iii) el método utilizado para identificar al titular del dispositivo de firma;

iv) toda limitación de los fines o del valor con los que pueda utilizarse el dispositivo de firma; y

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

d) Proporcionar a los titulares de dispositivos de firmas un medio para dar aviso de que un dispositivo de firma está en entredicho y asegurar el funcionamiento de un servicio puntual de revocación;

e) Utilizar sistemas, procedimientos y recursos humanos fiables para prestar sus servicios.

2) Para determinar si ciertos sistemas, procedimientos o recursos humanos son fiables a efectos del apartado e) del párrafo 1), y en qué grado lo son, se tomarán en consideración 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 el proveedor de servicios de certificación 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 del proveedor de servicios de certificación y la ley del Estado promulgante.

3) Todo certificado dará a conocer:

a) la identidad del proveedor de servicios de certificación;

b) que la persona nombrada en el certificado posee, en el momento pertinente, el dispositivo de firma que se menciona en el certificado;

c) que el dispositivo de firma gozaba de validez en el momento en que se expidió el certificado o antes de esa fecha;

d) toda limitación de los fines o del valor con los que pueda utilizarse el certificado; y

e) toda limitación del alcance o de la cuantía de la responsabilidad que el proveedor de servicios de certificación acepte frente a toda persona.

Variante X

4) El proveedor de servicios de certificación será responsable del incumplimiento de los requisitos del párrafo 1).

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

Variante Y

4) El proveedor de servicios de certificación será responsable del incumplimiento de los requisitos del párrafo 1).

5) Al evaluarse la pérdida, deberán tomarse en consideración los siguientes factores:

a) el costo de obtención del certificado;

b) la naturaleza de la información que se certifique;

c) la existencia de alguna limitación de los fines con los que pueda utilizarse el certificado y el alcance de dicha limitación;

d) la existencia de alguna declaración que restrinja el alcance o la cuantía de la responsabilidad del proveedor de servicios de certificación; y

e) toda culpa concurrente de la parte que confía en el certificado que contribuya a la pérdida.

Variante Z

4) Cuando los daños y perjuicios sean imputables a información incorrecta o errónea consignada en el certificado, todo proveedor de servicios de certificación será responsable de los daños y perjuicios sufridos por:

a) toda parte que haya celebrado un contrato con el proveedor de servicios de certificación para la expedición de un certificado; o por

b) toda persona que confíe razonablemente en un certificado expedido por el proveedor de servicios de certificación.

5) El proveedor de servicios de certificación no será responsable en virtud del párrafo 2):

a) cuando, y en la medida en que, haya incluido en el certificado una declaración que limite el alcance o la magnitud de su responsabilidad frente a toda persona pertinente; 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.9/465, párrs. 123 a 142 (proyecto de artículo 12);
A/CN.9/WG.IV/WP.82, párrs. 59 a 68 (proyecto de artículo 12);
A/CN.9/457, párrs. 108 a 119;
A/CN.9/WG.IV/WP.80, párrs. 22 a 24.

Observaciones

54. El proyecto de artículo 10 (antes proyecto de artículo 12) ha sido revisado de conformidad con las decisiones adoptadas por el Grupo de Trabajo en su 35º período de sesiones.

55. El Grupo de Trabajo, en su anterior período de sesiones, consideró que el fondo del párrafo 1) era generalmente aceptable, a reserva de algunas pequeñas modificaciones de forma. El párrafo 2) es el resultado de una propuesta formulada en dicho período de sesiones en el sentido de que las características del proveedor de servicios de certificación descritas en el proyecto de artículo 13 no sólo debían tenerse en cuenta en relación

con entidades extranjeras sino que también debían ser aplicables a los proveedores de servicios de certificación del propio país (A/CN.9/465, párr. 136).

56. El párrafo 3) es el resultado de una propuesta, acogida también con considerable interés por el Grupo de Trabajo en su anterior período de sesiones, según la cual el proyecto de artículo 12 debía establecer una regla adicional que fijara el contenido mínimo de un certificado (ibíd., párr. 135). Si bien los elementos que debe contener un certificado se enumeran en un párrafo aparte, es dudoso que el párrafo 1) c) y el párrafo 3) deban mantenerse como disposiciones separadas. El Grupo de Trabajo tal vez desee aclarar si esas dos listas deben refundirse, presumiblemente en el párrafo 1) c), que podría empezar con un texto como el siguiente: “indicar en cada certificado ...”.

57. Los párrafos 4) y 5) regulan la responsabilidad del proveedor de servicios de certificación.

58. En las Variantes X e Y, el párrafo 4) establece la norma de que el proveedor de servicios de certificación es responsable del incumplimiento de las obligaciones o deberes previstos en el párrafo 1), pero deja que sea el derecho nacional el que determine cuáles podrían ser las consecuencias de ese incumplimiento.

59. El párrafo 5) de la Variante X establece la norma de la previsibilidad del daño sobre la base del artículo 74 de la Convención sobre la Compraventa. Este párrafo limita la cuantía de la responsabilidad del proveedor de servicios de certificación que podría derivarse de los párrafos 1) y 2). En la Variante Y, el párrafo 5) se basa en una sugerencia hecha en el 35º período de sesiones del Grupo de Trabajo (A/CN.9/465, párr. 140), según la cual el Régimen Uniforme, sin interferir en el funcionamiento del derecho interno, podría enunciar una lista de factores que habrían de tenerse en cuenta al aplicar la legislación nacional a los proveedores de servicios de certificación.

60. La Variante Z no se examinó durante el 35º período de sesiones del Grupo de Trabajo. Tiene su origen en un sentimiento expresado en diversas ocasiones en el 34º período de sesiones del Grupo de Trabajo (A/CN.9/457, párr. 115), de que sería apropiado crear una disposición uniforme que no se limitara a remitir al derecho aplicable y previera una responsabilidad general por negligencia, sujeta a posibles exenciones contractuales (siempre que la limitación no fuera manifiestamente injusta) y con la posibilidad de que el proveedor de servicios de certificación quedara exento de responsabilidad si demostraba haber cumplido las obligaciones previstas en el párrafo 1). El párrafo 4) de la Variante Z regula la cuestión de la persona ante la cual puede ser responsable el proveedor de servicios de certificación. El párrafo 5) prevé una norma que permite al proveedor de servicios de certificación 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 (A/CN.9/WG.IV/WP.82, párr. 67).

Referencias a legislación nacional y a otros textos

Párrafos 1), 2) y 3) - 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.

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;
c) asegurar que puedan determinarse con precisión la fecha y hora, cuando se expida o revoque un certificado;
d) 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;
e) emplear a personal que posea los conocimientos especializados, la experiencia y las calificaciones necesarias para los servicios prestados, 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 administrativos y de gestión adecuados que correspondan a las normas reconocidas;
f) 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;
g) 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;
h) 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;
i) 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;
j) no almacenar ni copiar datos de creación de firmas de la persona a la que el proveedor de servicios de certificación haya prestado servicios básicos de gestión;
k) antes de iniciar una relación contractual con una persona que 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, que podrá transmitirse por medios electrónicos, deberá presentarse por un escrito y 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;
l) 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.

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) tas 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.

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.

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) actuará 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.

Párrafos 4) y 5) - 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.

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 entidad o persona física o jurídica que confíe razonablemente en ese certificado en lo que respecta:

a) a la exactitud de toda la información consignada en el certificado apropiado en el momento de su expedición y al hecho de que el certificado consigna todos los datos prescritos para un certificado apropiado;
b) al hecho de que, en el momento de expedirse el certificado, el signatario identificado en el certificado apropiado poseía los datos de creación de firmas correspondientes a los datos de verificación de firmas especificados o mencionados en el certificado;
c) al 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.

2. 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 entidad o persona física o jurídica 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 un certificado apropiado los límites de la utilización de ese certificado, límites que deben ser discernibles por terceros. El proveedor de servicios de certificación no será responsable de los daños y perjuicios derivados de una utilización del certificado apropiado que rebase los límites impuestos.

4. Los Estados Miembros velarán por que el proveedor de servicios de certificación indique en el certificado apropiado un límite del valor de las transacciones para las que pueda utilizarse el certificado, límite que debe ser discernible por terceros. El proveedor de servicios de certificación no será responsable de los daños y perjuicios debidos al hecho de haber rebasado este límite máximo.
5. Las disposiciones de los párrafos 1 a 4 serán sin perjuicio de la Directiva 93/13/EEC del Consejo, de 5 de abril de 1993, relativa a las condiciones injustas en los contratos con consumidores.

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 11. Confianza en las firmas electrónicas

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

2) [Para determinar si no es razonable confiar,] [Para determinar si era razonable que una persona hubiese confiado en la firma electrónica,] deberá tenerse en cuenta, en su caso, lo siguiente:

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

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

c) si la parte que confía tomó medidas para averiguar si la firma electrónica estaba avalada por un certificado;

d) si la parte que confía sabía o debía haber sabido que el dispositivo de firma electrónica estaba en entredicho o había sido revocado;

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

f) todos los demás factores pertinentes.

Artículo 12. Confianza en los certificados

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

2) [Para determinar si no es razonable confiar,] [Para determinar si era razonable que una persona hubiese confiado en la información de un certificado,] 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 o suspensiones de certificados;

c) todo acuerdo o trato que la parte que confía tenga o tuviera en el momento pertinente con el proveedor de servicios de certificación o el suscriptor o todo uso comercial aplicable;

d) todos los demás factores pertinentes.

Variante A

3) Si, dadas las circunstancias del caso, no es razonable confiar en la firma electrónica habida cuenta de los factores indicados en el párrafo 1), la parte que confía asume el riesgo de que la firma no sea válida.

Variante B

3) Si, dadas las circunstancias del caso, no es razonable confiar en la firma habida cuenta de los factores indicados en el párrafo 1), la parte que confía no podrá reclamar contra el titular del dispositivo de firma o el proveedor de servicios de certificación.

Referencias a documentos de la CNUDMI

A/CN.9/465, párrs. 109 a 122 (proyectos de artículo 10 y 11);
A/CN.9/WG.IV/WP.82, párrs. 56 a 58 (proyectos de artículo 10 y 11);
A/CN.9/457, párrs. 99 a 107;

A/CN.9/WG.IV/WP.80, párrs. 20 y 21.

Observaciones

61. Los proyectos de artículo 11 y 12, que tratan respectivamente de la confianza razonable en las firmas electrónicas y los certificados, han sido objeto de algunas pequeñas modificaciones de redacción de resultas de las deliberaciones del Grupo de Trabajo en su 35º período de sesiones. Si bien la opinión prevaleciente del Grupo de Trabajo en su 34º período de sesiones fue que debían incluirse en el Régimen Uniforme disposiciones relativas a las obligaciones de la parte que iba a confiar en un certificado, en el 35º período de sesiones se expresaron algunas dudas acerca de la utilidad del concepto de "confianza", que se refiere tanto al mensaje como a la firma, y que podría suscitar cuestiones difíciles en el marco del derecho de las obligaciones y la necesidad de atribución del riesgo (véase el documento A/CN.9/465, párr. 111). El Grupo de Trabajo tal vez desee decidir, como cuestión de principio, si el Régimen Uniforme debe establecer expresamente obligaciones vinculantes para las partes que confían. Si se entiende que los artículos 11 y 12 establecen obligaciones para las partes que confían, quizás sea preciso seguir examinando las consecuencias del incumplimiento de esas obligaciones. Si se entiende que los artículos 11 y 12 se limitan a establecer un simple "código de conducta", sin abordar las consecuencias eventuales de la no observancia de la conducta indicada (veáse el documento A/CN.9/465, párr. 113), lo más apropiado sería incluir las sugerencias relativas a la conducta de la parte que confía en algún texto explicativo como la guía para la incorporación del Régimen Uniforme al derecho interno.

62. Las Variantes A y B, que se basan en el supuesto de que el Régimen Uniforme debe regular eventuales consecuencias jurídicas en el caso de que una parte que confía no actúe con la debida diligencia al evaluar la fiabilidad de una firma electrónica (tanto si esa firma electrónica está avalada por un certificado como si no lo está), tienen como finalidad reflejar las dos propuestas formuladas a ese respecto en el 35º período de sesiones del Grupo de Trabajo (A/CN.9/465, párr. 117).

63. El Grupo de Trabajo quizás desee seguir examinando la relación entre los proyectos de artículo 11 y 12, por una parte, y el proyecto de artículo 6, por otra.

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 13. Reconocimientos de certificados y firmas electrónicas extranjeras

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

2) Los certificados expedidos por un proveedor de servicios de certificación extranjero se reconocerán como jurídicamente equivalentes a los expedidos por proveedores de servicios de certificación que funcionen conforme a ... *[la ley del Estado promulgante]* cuando las prácticas de los proveedores de servicios de certificación extranjeros ofrezcan un grado de fiabilidad por lo menos equivalente al requerido de los proveedores de servicios de certificación 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 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 con otros Estados.]

4) Al determinar la equivalencia, deberán tenerse en cuenta, si procede, [los factores indicados en el párrafo 2) del artículo 10] [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].

5) Sin perjuicio de lo dispuesto en los párrafos 2) y 3), las partes en transacciones comerciales y de otra índole podrán hacer constar que se debe utilizar un determinado proveedor de servicios de certificación, una determinada clase de proveedores de servicios de certificación o clase de certificados en relación con los mensajes o las firmas presentados a esas partes.

6) Cuando, sin perjuicio de lo dispuesto en los párrafos 2) y 3), las partes acuerden entre sí la utilización de determinados tipos de firmas electrónicas y certificados, [se reconocerá que ese acuerdo es suficiente a efectos del reconocimiento transfronterizo]. [Al determinar si, o en qué medida, una firma electrónica o un certificado surten efectos jurídicos, deberá tenerse en cuenta cualquier acuerdo entre las partes en la transacción en que se utilice esa firma o certificado.]

Referencias a documentos de la CNUDMI

A/CN.9/465, párrs. 21 a 35;
A/CN.9/WG.IV/WP.82, párrs. 69 a 71;
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, párrs. 74 a 89 (proyecto de artículo I); y
A/CN.9/WG.IV/WP.71, párrs. 73 a 75.

Observaciones

64. Si bien en el 35º período de sesiones del Grupo de Trabajo se apoyó en general el principio de la no discriminación enunciado en el párrafo 1), se expresaron dudas acerca de si resultaba apropiado referirse al país de origen. Se expresó el parecer de que la referencia al país de origen restringía demasiado el alcance de la regla de no discriminación y dejaba abierta la posibilidad de discriminar por varios otros motivos, cosa que no era de desear. Se expresó también el parecer de que, de hecho, podía haber casos en los que el país de origen de la firma o del certificado fuera un factor esencial para el reconocimiento. Sin embargo, no obtuvo apoyo una propuesta de sustituir el texto actual según el cual no debía tomarse en consideración el país de origen por un texto que indicara que la determinación del efecto jurídico de una firma electrónica no debía basarse "únicamente" en el país de origen (véase el documento A/CN.9/465, párrs. 23 y 24). El Grupo de Trabajo tal

vez desee decidir, como cuestión de principio, si en el proyecto de artículo 13 debe incluirse una declaración precisa del principio de no discriminación o si la expresión de ese principio debe figurar como referencia más general en un preámbulo o en una guía para la incorporación del Régimen Uniforme al derecho interno.

65. Los párrafos 2), 3), 4) y 5) fueron acordados en gran medida por el Grupo de Trabajo en su anterior período de sesiones al considerar que enunciaban una regla idónea para el reconocimiento de los certificados y firmas extranjeros (ibíd., párr. 34). En lo que respecta a los factores que se enumeran en el párrafo 4), podría ser suficiente remitir al proyecto de artículo 10 si se utilizaban los mismos factores para determinar la fiabilidad de los sistemas utilizados por los proveedores nacionales de servicios de certificación. El párrafo 5) refleja una opinión general del Grupo de Trabajo de que debe concederse a las partes en transacciones comerciales y de otra índole el derecho a elegir el proveedor de servicios de certificación, la clase de proveedores de servicios de certificación o la clase de certificados que deseen utilizar en relación con los mensajes o firmas que reciban. Mediante la referencia a las partes en transacciones comerciales o de otra índole se pretende incluir a los organismos gubernamentales que actúen como entidades comerciales.

66. El párrafo 6) contiene sugerencias para expresar la decisión adoptada por el Grupo de Trabajo en su 35º período de sesiones de que en el proyecto de artículo 13 deberían reconocerse los acuerdos entre las partes interesadas acerca del empleo de determinados tipos de firmas electrónicas o certificados como fundamento suficiente para el reconocimiento transfronterizo (en lo que concierne a dichas partes) de las firmas o certificados así convenidos (A/CN.9/465, párr. 34).

67. El Grupo de Trabajo quizá desee decidir, como cuestión de principio, si el proyecto de artículo 13 debe referirse tanto a los certificados como a las firmas.

Referencias a legislación nacional y a otros textos

Directiva de la CE

Artículo 7 Aspectos internacionales

1. Los Estados Miembros velarán por que los certificados expedidos como certificados apropiados para el público por un proveedor 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 si:

a) 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; o

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

c) el certificado o el proveedor de servicios de certificación están reconocidos en virtud 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].

Anexo I. PROYECTO DE RÉGIMEN UNIFORME PARA LAS FIRMAS ELECTRÓNICAS

(Texto consolidado de los proyectos de artículo 1 a 13 examinados en la parte II de la presente nota)

Artículo 1. Ámbito de aplicación

El presente Régimen será aplicable a todo supuesto en el que se utilicen firmas electrónicas en el contexto* de actividades comerciales**. No derogará ninguna norma jurídica destinada a la protección del consumidor.

* La Comisión propone el texto siguiente para los Estados que deseen ampliar el ámbito de aplicación del presente Régimen:

"El presente Régimen será aplicable a todo supuesto en el que se utilicen firmas electrónicas, excepto en las situaciones siguientes: [...]."

** 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.

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] [titular de la clave] [suscriptor] [titular del dispositivo de firma] [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].

Artículo 3. [Neutralidad respecto de la tecnología] [Igualdad de tratamiento de las firmas]

Ninguna de las disposiciones del presente Régimen se aplicará de modo que excluya, restrinja o prive de efecto jurídico cualquier método [de firma electrónica] [que cumpla los requisitos mencionados en el párrafo 1) del artículo 6 del presente Régimen] [que sea tan fiable como sea apropiado 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] [o que de algún otro modo cumpla con los requisitos del derecho aplicable].

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.

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.

Artículo 5. [Modificación mediante acuerdo] [Autonomía de las partes] [Autonomía contractual]

Salvo que el presente Régimen o el derecho del Estado promulgante dispongan otra cosa, las partes podrán convenir en apartarse del presente Régimen o en modificarlo [modificar su efecto].

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

1) Cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos si se utiliza [un método] [una firma electrónica] que es tan fiable como sea apropiado 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.

2) El párrafo 1) será aplicable tanto si el requisito previsto en él está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que no exista una firma.

Variante A

3) Se presumirá que [un método] [una firma electrónica] es fiable a efectos del cumplimiento del requisito enunciado en el párrafo 1) si ese método garantiza que:

a) los datos utilizados para la creación de una firma electrónica son exclusivos del titular del dispositivo [para la creación] de firmas en el contexto en que se utilicen;

b) el titular del dispositivo [para la creación] de firmas [tiene] [tenía en el momento pertinente] el control exclusivo de dicho dispositivo;

c) la firma electrónica está vinculada [a la información] [al mensaje de datos o a la parte de ese mensaje] al que corresponde [de modo que garantice la integridad de esa información];

d) el titular del dispositivo [para la creación] de firmas está objetivamente identificado en el contexto [en que se utiliza el dispositivo] [del mensaje de datos].

Variante B

3) A falta de prueba en contrario, se presumirá que la utilización de una firma electrónica demuestra:

a) la conformidad de la firma electrónica con la norma de fiabilidad enunciada en el párrafo 1);

b) la identidad del presunto signatario; y

c) la aprobación por el presunto signatario de la información a la que corresponde la firma electrónica.

4) La presunción enunciada en el párrafo 3) será válida únicamente en el caso de que:

a) la persona que pretende confiar en la firma electrónica notifique al presunto signatario que se confía en la firma electrónica [como equivalente de la firma manuscrita del presunto signatario] [como prueba de los elementos indicados en el párrafo 3)]; y

b) el presunto signatario no comunique prontamente a la persona que efectúe una notificación tal como se prevé en el apartado a) las razones por las que no debe confiarse en la firma electrónica [como equivalente de la firma manuscrita del presunto signatario] [como prueba de los elementos indicados en el párrafo 3)].

Variante C

3) A falta de prueba en contrario, se presumirá que la utilización de una firma electrónica demuestra:

a) la conformidad de la firma electrónica con la norma de fiabilidad enunciada en el párrafo 1);

b) la identidad del presunto signatario; y

c) la aprobación por el presunto signatario de la información a la que corresponde la firma electrónica.

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

[Artículo 7. Presunción de original

1) Se presumirá que un mensaje de datos es en su forma original cuando, en relación con ese mensaje de datos, se utilice [un método] [una firma electrónica] [de acuerdo con el artículo 6] que:

a) 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; y

b) de requerirse que la información sea presentada, dicha información puede ser mostrada a la persona a quien se deba presentar;

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

Artículo 8. Cumplimiento de los artículos 6 y 7

Variante A

1) *[El órgano o la entidad designada por el Estado promulgante competente]* podrá determinar qué métodos 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.

Variante B

1) Cabrá determinar que uno o más métodos de firma electrónica 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.

Artículo 9. Responsabilidades del titular del dispositivo de firma

1) Cada titular del dispositivo de firma deberá:

a) Actuar con diligencia razonable para evitar la utilización no autorizada de su dispositivo de firma:

b) Dar aviso a quien corresponda sin demora injustificada en caso de que:

i) el titular del dispositivo de firma tenga conocimiento de que el dispositivo de firma ha quedado en entredicho; o
ii) las circunstancias conocidas por el titular del dispositivo de firma den lugar a un riesgo sustancial de que el dispositivo de firma pueda haber quedado en entredicho;

c) [Cuando se utilice un certificado para avalar el dispositivo de firma,] [Cuando el dispositivo de firma entrañe la utilización de un certificado,] actuar con diligencia razonable para velar por la exactitud y la integridad de todas las declaraciones pertinentes efectuadas por el titular del dispositivo de firma que sean de interés para el [ciclo vital del] certificado, o que deban consignarse en el certificado.

2) El titular del dispositivo de firma será responsable del incumplimiento de los requisitos del párrafo 1).

Artículo 10. Responsabilidades del proveedor de servicios de certificación

1) Todo proveedor de servicios de certificación deberá:

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

b) obrar con la debida diligencia para velar por la exactitud y la integridad de todas las declaraciones pertinentes efectuadas por el proveedor de servicios de certificación que sean de interés para el ciclo vital del certificado o que estén consignadas en el certificado;

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

i) la identidad del proveedor de servicios de certificación;

ii) que la persona nombrada en el certificado posee, en el momento pertinente, el dispositivo de firma que se menciona en el certificado;

iii) el método utilizado para identificar al titular del dispositivo de firma;

iv) toda limitación de los fines o del valor con los que pueda utilizarse el dispositivo de firma; y

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

d) Proporcionar a los titulares de dispositivos de firmas un medio para dar aviso de que un dispositivo de firma está en entredicho y asegurar el funcionamiento de un servicio puntual de revocación;

e) Utilizar sistemas, procedimientos y recursos humanos fiables para prestar sus servicios.

2) Para determinar si ciertos sistemas, procedimientos o recursos humanos son fiables a efectos del apartado e) del párrafo 1), y en qué grado lo son, se tomarán en consideración 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 el proveedor de servicios de certificación 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 del proveedor de servicios de certificación y la ley del Estado promulgante.

3) Todo certificado dará a conocer:

a) la identidad del proveedor de servicios de certificación;

b) que la persona nombrada en el certificado posee, en el momento pertinente, el dispositivo de firma que se menciona en el certificado;

c) que el dispositivo de firma gozaba de validez en el momento en que se expidió el certificado o antes de esa fecha;

d) toda limitación de los fines o del valor con los que pueda utilizarse el certificado; y

e) toda limitación del alcance o de la cuantía de la responsabilidad que el proveedor de servicios de certificación acepte frente a toda persona.

Variante X

4) El proveedor de servicios de certificación será responsable del incumplimiento de los requisitos del párrafo 1).

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

Variante Y

4) El proveedor de servicios de certificación será responsable del incumplimiento de los requisitos del párrafo 1).

5) Al evaluarse la pérdida, deberán tomarse en consideración los siguientes factores:

a) el costo de obtención del certificado;

b) la naturaleza de la información que se certifique;

c) la existencia de alguna limitación de los fines con los que pueda utilizarse el certificado y el alcance de dicha limitación;

d) la existencia de alguna declaración que restrinja el alcance o la cuantía de la responsabilidad del proveedor de servicios de certificación; y

e) toda culpa concurrente de la parte que confía en el certificado que contribuya a la pérdida.

Variante Z

4) Cuando los daños y perjuicios sean imputables a información incorrecta o errónea consignada en el certificado, todo proveedor de servicios de certificación será responsable de los daños y perjuicios sufridos por:

a) toda parte que haya celebrado un contrato con el proveedor de servicios de certificación para la expedición de un certificado; o por

b) toda persona que confíe razonablemente en un certificado expedido por el proveedor de servicios de certificación.

5) El proveedor de servicios de certificación no será responsable en virtud del párrafo 2):

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

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

Artículo 11. Confianza en las firmas electrónicas

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

2) [Para determinar si no es razonable confiar,] [Para determinar si era razonable que una persona hubiese confiado en la firma electrónica,] deberá tenerse en cuenta, en su caso, lo siguiente:

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

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

c) si la parte que confía tomó medidas para averiguar si la firma electrónica estaba avalada por un certificado;

d) si la parte que confía sabía o debía haber sabido que el dispositivo de firma electrónica estaba en entredicho o había sido revocado;

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

f) todos los demás factores pertinentes.

Artículo 12. Confianza en los certificados

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

2) [Para determinar si no es razonable confiar,] [Para determinar si era razonable que una persona hubiese confiado en la información de un certificado,] 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 o suspensiones de certificados;

c) todo acuerdo o trato que la parte que confía tenga o tuviera en el momento pertinente con el proveedor de servicios de certificación o el suscriptor o todo uso comercial aplicable;

d) todos los demás factores pertinentes.

Variante A

3) Si, dadas las circunstancias del caso, no es razonable confiar en la firma electrónica habida cuenta de los factores indicados en el párrafo 1), la parte que confía asume el riesgo de que la firma no sea válida.

Variante B

3) Si, dadas las circunstancias del caso, no es razonable confiar en la firma habida cuenta de los factores indicados en el párrafo 1), la parte que confía no podrá reclamar contra el titular del dispositivo de firma o el proveedor de servicios de certificación.

Artículo 13. Reconocimientos de certificados y firmas electrónicas extranjeras

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

2) Los certificados expedidos por un proveedor de servicios de certificación extranjero se reconocerán como jurídicamente equivalentes a los expedidos por proveedores de servicios de certificación que funcionen conforme a ... *[la ley del Estado promulgante]* cuando las prácticas de los proveedores de servicios de certificación extranjeros ofrezcan un grado de fiabilidad por lo menos equivalente al requerido de los proveedores de servicios de certificación 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 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 con otros Estados.]

4) Al determinar la equivalencia, deberán tenerse en cuenta, si procede, [los factores indicados en el párrafo 2) del artículo 10] [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].

5) Sin perjuicio de lo dispuesto en los párrafos 2) y 3), las partes en transacciones comerciales y de otra índole podrán hacer constar que se debe utilizar un determinado proveedor de servicios de certificación, una determinada clase de proveedores de servicios de certificación o clase de certificados en relación con los mensajes o las firmas presentados a esas partes.

6) Cuando, sin perjuicio de lo dispuesto en los párrafos 2) y 3), las partes acuerden entre sí la utilización de determinados tipos de firmas electrónicas y certificados, [se reconocerá que ese acuerdo es suficiente a efectos del reconocimiento transfronterizo]. [Al determinar si, o en qué medida, una firma electrónica o un certificado surten efectos jurídicos, deberá tenerse en cuenta cualquier acuerdo entre las partes en la transacción en que se utilice esa firma o certificado.]

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.

4/ Ibíd., quincuagésimo cuarto período de sesiones, Suplemento Nº 17 (A/54/17), párrs. 308 a 314.