Naciones Unidas A/CN.9/WG.IV/WP.88

Asamblea General

Distr. limitada
30 de enero de 2001
Español
Original: inglés

Comisión de las Naciones Unidas para el Derecho Mercantil Internacional
Grupo de Trabajo sobre Comercio Electrónico
38º período de sesiones
Nueva York, 12 a 23 de marzo de 2001

Firmas electrónicas

Proyecto de guía para la incorporación al derecho interno de la Ley Modelo de la CNUDMI para las Firmas Electrónicas

Nota de la Secretaría

1. Conforme a las decisiones adoptadas por la Comisión en sus períodos de sesiones 29º (1996)[1] y 30º (1997)[2], el Grupo de Trabajo sobre Comercio Electrónico dedicó sus períodos de sesiones 31º a 37º a la preparación del proyecto de Ley Modelo de la CNUDMI para las Firmas Electrónicas (en adelante denominado "Ley Modelo", "proyecto de Ley Modelo" o "nueva Ley Modelo"). En los documentos A/CN.9/437, 446, 454, 457, 465, 467 y 483 figuran los informes correspondientes a dichos períodos de sesiones. Al preparar la Ley Modelo, el Grupo de Trabajo observó que sería útil ofrecer, en un comentario, más información sobre dicha Ley. Siguiendo el criterio adoptado en la preparación de la Ley Modelo de la CNUDMI sobre Comercio Electrónico, recibió apoyo general la sugerencia de acompañar la nueva Ley Modelo de una guía para ayudar a los Estados a incorporarla a su derecho interno y aplicarla. La Guía, gran parte de la cual se extraería de los *trabajos preparatorios* de la Ley Modelo, también sería útil para otros usuarios de ésta.

2. En su 37º período de sesiones, el Grupo de Trabajo terminó la preparación de los proyectos de artículo de la Ley Modelo y analizó el proyecto de guía para la incorporación al derecho interno sobre la base de una nota de la Secretaría (A/CN.9/WG.IV/WP.86 y Add.1). Se pidió a la Secretaría que preparase una versión revisada del proyecto de guía que reflejase las decisiones adoptadas por el Grupo de Trabajo sobre la base de las diversas opiniones, sugerencias y preocupaciones expresadas en el 37º período de sesiones. Por falta de tiempo, el Grupo de Trabajo

no terminó sus deliberaciones sobre el proyecto de guía para la incorporación al derecho interno (véase el documento A/CN.9/483, párrs. 23 y 145 a 152). Se sugirió que el Grupo de Trabajo reservase cierto tiempo en su 38º período de sesiones para concluir ese tema del programa. Se observó que el proyecto de Ley Modelo, junto con el proyecto de guía para la incorporación al derecho interno, se presentaría a la Comisión para su examen y aprobación en el 34º período de sesiones de ésta, que se celebraría del 25 de junio al 13 de julio de 2001 en Viena.

3. El anexo a la presente nota contiene una versión revisada del proyecto de guía preparada por la Secretaría.

Anexo

LEY MODELO DE LA CNUDMI PARA LAS FIRMAS ELECTRÓNICAS

CON

LA GUÍA PARA SU INCORPORACIÓN AL DERECHO INTERNO

2001

Índice

Resolución de la Asamblea General .....

Primera Parte

LEY MODELO DE LA CNUDMI PARA LAS FIRMAS ELECTRÓNICAS (2001)

Página

Artículo 1. Ámbito de aplicación 7
Artículo 2. Definiciones 7
Artículo 3. Igualdad de tratamiento de las tecnologías para la firma 8
Artículo 4. Interpretación 8
Artículo 5. Modificación mediante acuerdo 8
Artículo 6. Cumplimiento del requisito de firma 8
Artículo 7. Cumplimiento de lo dispuesto en el artículo 6 9
Artículo 8. Proceder del firmante 9
Artículo 9. Proceder del prestador de servicios de certificación 10
Artículo 10. Fiabilidad 11
Artículo 11. Proceder de la parte que confía en el certificado 11
Artículo 12. Reconocimiento de certificados y firmas electrónicas extranjeros 11

Segunda Parte

GUÍA PARA LA INCORPORACIÓN AL DERECHO INTERNO DE LA LEY MODELO DE LA CNUDMI PARA LAS FIRMAS ELECTRÓNICAS (2001)

Párrafos *Página*

Finalidad de la presente Guía 1-2 13

Capítulo I. Introducción a la Ley Modelo 3-85 13

I. FINALIDAD Y ORIGEN DE LA LEY MODELO 3-25 13
A. Finalidad 3-5 13
B. Antecedentes 6-11 14
C. Historia 12-25 16

II.	LA LEY MODELO COMO INSTRUMENTO DE ARMONIZACIÓN DE LEYES		26-28	19
III.	OBSERVACIONES GENERALES SOBRE LAS FIRMAS ELECTRÓNICAS		29-62	21
	A.	Funciones de las firmas	29-30	21
	B.	Firmas numéricas y otras firmas electrónicas	31-62	21
		1. Firmas electrónicas basadas en técnicas distintas de la criptografía de clave pública	33-34	22
		2. Firmas numéricas basadas en la criptografía de clave pública	35-62	23
		a) Terminología y conceptos técnicos	36-44	23
		i) Criptografía	36-37	23
		ii) Claves públicas y privadas	38-39	24
		iii) La función control	40	24
		iv) La firma numérica	41-42	25
		v) Verificación de la firma numérica	43-44	25
		b) Infraestructura de clave pública (ICP) y prestadores de servicios de certificación	45-61	25
		i) Infraestructura de clave pública (ICP)	50-52	27
		ii) Prestadores de servicios de certificación	53-61	28
		c) Sinopsis del proceso de la firma numérica	62	30
IV.	PRINCIPALES CARACTERÍSTICAS DE LA LEY MODELO		63-82	31
	A.	Naturaleza legislativa de la Ley Modelo	63-64	31
	B.	Relación con la Ley Modelo de la CNUDMI sobre Comercio Electrónico	65-68	32
		1. La Ley Modelo como instrumento jurídico independiente	65	32
		2. Plena coherencia entre la Ley Modelo y la Ley Modelo de la CNUDMI sobre Comercio Electrónico	66-67	32
		3. Relación con el artículo 7 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico	68	33
	C.	Régimen “marco” que se complementará con reglamentaciones técnicas y contratos	69-70	33
	D.	Mayor seguridad de las consecuencias jurídicas de las firmas electrónicas	71-76	34
	E.	Normas de conducta básicas para las partes interesadas	77-81	36
	F.	Marco de neutralidad respecto de los medios técnicos utilizables	82	37

V.	ASISTENCIA DE LA SECRETARÍA DE LA CNUDMI		83-85	37
	A.	Asistencia para la redacción de legislación	83-84	37
	B.	Información relativa a la interpretación de la legislación basada en la Ley Modelo	85	37
Capítulo II.	**Observaciones artículo por artículo**		86-155	39
Título			86	39
Artículo 1.		Ámbito de aplicación	87-91	39
Artículo 2.		Definiciones	92-105	41
Artículo 3.		Igualdad de tratamiento de las tecnologías para la firma	106	46
Artículo 4.		Interpretación	107-109	47
Artículo 5.		Modificación mediante acuerdo	110-113	48
Artículo 6.		Cumplimiento del requisito de firma	114-126	49
Artículo 7.		Cumplimiento de lo dispuesto en el artículo 6	127-131	54
Artículo 8.		Proceder del firmante	132-136	56
Artículo 9.		Proceder del prestador de servicios de certificación	137-141	58
Artículo 10.		Fiabilidad	142	60
Artículo 11.		Proceder de la parte que confía en el certificado	143-146	61
Artículo 12.		Reconocimiento de certificados y firmas electrónicas extranjeras	147-155	63

Primera parte

Ley Modelo de la CNUDMI para las firmas electrónicas (2001)

(aprobada por el Grupo de Trabajo de la CNUDMI sobre Comercio Electrónico en su 37º período de sesiones, celebrado del 18 al 29 de septiembre de 2000 en Viena)

Artículo 1. Ámbito de aplicación

La presente Ley será aplicable en todos los casos en 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 de la presente Ley:

"La presente Ley será aplicable en todos los casos en que se utilicen firmas electrónicas, excepto en las situaciones siguientes: [Y]."

** El término "comercial" deberá ser interpretado en forma lata de manera que abarque las cuestiones que dimanen de toda relación de índole comercial, sea o no contractual. Las relaciones de índole comercial comprenden, sin que esta lista sea taxativa, las operaciones siguientes: toda operación comercial de suministro o intercambio de bienes o servicios; acuerdos de distribución; representación o mandato comercial; facturaje (Afactoring@); arrendamiento con opción de compra (Aleasing@); construcción de obras; consultoría; ingeniería; concesión de licencias; inversiones; financiación; banca; seguros; acuerdos o concesiones de explotación; empresas conjuntas y otras formas de cooperación industrial o comercial; transporte de mercancías o de pasajeros por vía aérea, marítima y férrea o por carretera.

Artículo 2. Definiciones

Para los fines de la presente Ley:

a) Por "firma electrónica" se entenderán los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información contenida en el mensaje de datos;

b) Por "certificado" se entenderá todo mensaje de datos u otro registro que confirme el vínculo entre un firmante y los datos de creación de la firma;

c) Por "mensaje de datos" se entenderá la información generada, enviada, recibida o archivada 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;

d) Por “firmante” se entenderá la persona que posee los datos de creación de la firma y que actúa en nombre propio o de la persona a la que representa;

e) Por “prestador de servicios de certificación” se entenderá la persona que expide certificados y puede prestar otros servicios relacionados con las firmas electrónicas;

f) Por “parte que confía” se entenderá la persona que pueda actuar sobre la base de un certificado o de una firma electrónica.

Artículo 3. Igualdad de tratamiento de las tecnologías para la firma

Ninguna de las disposiciones de la presente Ley, con la excepción del artículo 5, será aplicada de modo que excluya, restrinja o prive de efecto jurídico cualquier método para crear una firma electrónica que cumpla los requisitos enunciados en el párrafo 1) del artículo 6 o que cumpla de otro modo los requisitos del derecho aplicable.

Artículo 4. Interpretación

1) En la interpretación de la presente Ley habrán de tenerse en cuenta su origen internacional y la necesidad de promover la uniformidad en su aplicación y la observancia de la buena fe.

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

Artículo 5. Modificación mediante acuerdo

Las partes podrán hacer excepciones a la presente Ley o modificar sus efectos mediante acuerdo, salvo que ese acuerdo no sea válido o eficaz conforme al derecho aplicable.

Artículo 6. Cumplimiento del requisito de firma

1) Cuando la ley exija la firma de una persona, ese requisito quedará cumplido en relación con un mensaje de datos si se utiliza una firma electrónica que, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo aplicable, sea tan fiable como resulte apropiado a los fines para los cuales se generó o comunicó ese mensaje.

2) El párrafo 1) será aplicable tanto si el requisito a que se refiere está expresado en la forma de una obligación como si la ley simplemente prevé consecuencias para el caso de que no haya firma.

3) La firma electrónica se considerará fiable a los efectos del cumplimiento del requisito a que se refiere el párrafo 1) si:

a) los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante;

b) los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante;

c) es posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma; y

d) cuando uno de los objetivos del requisito legal de firma consista en dar seguridades en cuanto a la integridad de la información a que corresponde, es posible detectar cualquier alteración de esa información hecha después del momento de la firma.

4) Lo dispuesto en el párrafo 3) se entenderá sin perjuicio de la posibilidad de que cualquier persona:

a) demuestre de cualquier otra manera, a los efectos de cumplir el requisito a que se refiere el párrafo 1), la fiabilidad de una firma electrónica; o

b) aduzca pruebas de que una firma electrónica no es fiable.

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

Artículo 7. Cumplimiento de lo dispuesto en el artículo 6

1) [La persona, el órgano o la entidad, del sector público o privado, a que el Estado promulgante haya expresamente atribuido competencia] podrá determinar qué firmas electrónicas cumplen lo dispuesto en el artículo 6.

2) La determinación que se haga con arreglo al párrafo 1) deberá ser compatible con las normas o criterios internacionales reconocidos.

3) Lo dispuesto en el presente artículo se entenderá sin perjuicio de la aplicación de las normas del derecho internacional privado.

Artículo 8. Proceder del firmante

1) Cuando puedan utilizarse datos de creación de firmas para crear una firma con efectos jurídicos, cada firmante deberá:

a) actuar con diligencia razonable para evitar la utilización no autorizada de sus datos de creación de la firma;

b) dar aviso sin dilación indebida a cualquier persona que, según pueda razonablemente prever, pueda considerar fiable la firma electrónica o prestar servicios que la apoyen si:

i) sabe que los datos de creación de la firma han quedado en entredicho; o

ii) las circunstancias de que tiene conocimiento dan lugar a un riesgo considerable de que los datos de creación de la firma hayan quedado en entredicho;

c) cuando se emplee un certificado para refrendar la firma electrónica, actuar con diligencia razonable para cerciorarse de que todas las declaraciones que haya hecho en relación con su ciclo vital o que hayan de consignarse en él sean exactas y cabales.

2) El firmante incurrirá en responsabilidad por el incumplimiento de los requisitos enunciados en el párrafo 1).

Artículo 9. Proceder del prestador de servicios de certificación

1) Cuando un prestador de servicios de certificación preste servicios para apoyar una firma electrónica que pueda utilizarse como firma con efectos jurídicos, ese prestador de servicios de certificación deberá:

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

b) actuar con diligencia razonable para cerciorarse de que todas las declaraciones importantes que haya hecho en relación con el ciclo vital del certificado o que estén consignadas en él sean exactas y cabales;

c) proporcionar medios de acceso razonablemente fácil que permitan a la parte que confía en el certificado determinar mediante éste:

i) la identidad del prestador de servicios de certificación;

ii) que el firmante nombrado en el certificado tenía bajo su control los datos de creación de la firma en el momento en que se expidió el certificado;

iii) que los datos de creación de la firma eran válidos en la fecha en que se expidió el certificado o antes de ella;

d) proporcionar medios de acceso razonablemente fácil que, según proceda, permitan a la parte que confía en el certificado determinar mediante éste o de otra manera:

i) el método utilizado para identificar al firmante;

ii) cualquier limitación en los fines o el valor respecto de los cuales puedan utilizarse los datos de creación de la firma o el certificado;

iii) si los datos de creación de la firma son válidos y no están en entredicho;

iv) cualquier limitación en cuanto al ámbito o el alcance de la responsabilidad indicada por el prestador de servicios de certificación;

v) si existe un medio para que el firmante dé aviso de que los datos de creación de la firma están en entredicho, conforme a lo dispuesto en el apartado b) del párrafo 1) del artículo 8;

vi) si se ofrece un servicio de revocación oportuna del certificado;

e) cuando se ofrezcan servicios conforme al inciso v) del apartado d), proporcionar un medio para que el firmante dé aviso conforme al apartado b) del párrafo 1) del artículo 8 y, cuando se ofrezcan servicios en virtud del inciso vi) del apartado d), cerciorarse de que exista un servicio de revocación oportuna del certificado;

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

2) El prestador de servicios de certificación incurrirá en responsabilidad por el incumplimiento de los requisitos enunciados en el párrafo 1).

Artículo 10. Fiabilidad

A los efectos del apartado f) del párrafo 1) del artículo 9, para determinar si los sistemas, procedimientos o recursos humanos utilizados por un prestador de servicios de certificación son fiables, y en qué medida lo son, podrán tenerse en cuenta los factores siguientes:

a) los recursos humanos y financieros, incluida la existencia de un activo;

b) la calidad de los sistemas de equipo y programas informáticos;

c) los procedimientos para la tramitación del certificado y las solicitudes de certificados, y la conservación de registros;

d) la disponibilidad de información para los firmantes nombrados en el certificado y para las partes que confíen en éste;

e) la periodicidad y el alcance de la auditoría por un órgano independiente;

f) la existencia de una declaración del Estado, de un órgano de acreditación o del prestador de servicios de certificación respecto del cumplimiento o la existencia de los factores que anteceden; y

g) cualesquiera otros factores pertinentes.

Artículo 11. Proceder de la parte que confía en el certificado

Serán de cargo de la parte que confía en el certificado las consecuencias jurídicas que entrañe el hecho de que no haya tomado medidas razonables para:

a) verificar la fiabilidad de la firma electrónica; o

b) cuando la firma electrónica esté refrendada por un certificado:

i) verificar la validez, suspensión o revocación del certificado; y

ii) tener en cuenta cualquier limitación en relación con el certificado.

Artículo 12. Reconocimiento de certificados y firmas electrónicas extranjeros

1) Al determinar si un certificado o una firma electrónica produce efectos jurídicos, o en qué medida los produce, no se tomará en consideración:

a) el lugar en que se haya expedido el certificado o en que se haya creado o utilizado la firma electrónica; ni

b) el lugar en que se encuentre el establecimiento del expedidor o firmante.

2) Todo certificado expedido fuera *[del Estado promulgante]* producirá los mismos efectos jurídicos en *[el Estado promulgante]* que todo certificado expedido en *[el Estado promulgante]* si presenta un grado de fiabilidad sustancialmente equivalente.

3) Toda firma electrónica creada o utilizada fuera *[del Estado promulgante]* producirá los mismos efectos jurídicos en *[el Estado promulgante]* que toda firma electrónica creada o utilizada en *[el Estado promulgante]* si presenta un grado de fiabilidad sustancialmente equivalente.

4) A efectos de determinar si un certificado o una firma electrónica presentan un grado de fiabilidad sustancialmente equivalente para los fines de párrafo 2), o del párrafo 3), se tomarán en consideración las normas internacionales reconocidas y cualquier otro factor pertinente.

5) Cuando, sin perjuicio de lo dispuesto en los párrafos 2), 3) y 4), 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, salvo que ese acuerdo no sea válido o eficaz conforme al derecho aplicable.

Segunda parte

Guía para la incorporación al derecho interno de la Ley Modelo de la CNUDMI para las Firmas Electrónicas (2001)

Finalidad de la presente Guía

1. Al preparar y aprobar la Ley Modelo de la CNUDMI para las Firmas Electrónicas (también denominado en la presente publicación "Ley Modelo" o "nueva Ley Modelo"), la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) tuvo presente que la Ley Modelo ganaría en eficacia para los Estados que fueran a modernizar su legislación si se facilitaba a los órganos ejecutivos y legislativos de los Estados la debida información de antecedentes y explicativa que les ayudara a aplicar la Ley Modelo. La Comisión fue además consciente de la probabilidad de que la Ley Modelo fuera aplicada por algunos Estados poco familiarizados con las técnicas de comunicación reguladas en la Ley Modelo. La presente Guía, que en gran parte está inspirada en los *trabajos preparatorios* de la Ley Modelo, servirá también para orientar a otros usuarios del texto, como jueces, árbitros, profesionales y miembros del mundo académico. Esa información podría también ayudar a los Estados a determinar si existe alguna disposición de la Ley Modelo que tal vez conviniera modificar en razón de alguna circunstancia nacional particular. En la preparación de la Ley Modelo se partió del supuesto de que el proyecto de Ley Modelo iría acompañado de una guía. Por ejemplo, se decidió que ciertas cuestiones no serían resueltas en el texto de la Ley Modelo sino en la guía que había de orientar a los Estados en la incorporación de la Ley Modelo a su derecho interno. En la información presentada en esta Guía se explica cómo las disposiciones incluidas en la Ley Modelo enuncian los rasgos mínimos esenciales de un instrumento legislativo destinado a lograr los objetivos de la Ley Modelo.

2. La presente Guía para la incorporación al derecho interno de la Ley Modelo ha sido preparada por la Secretaría conforme a la solicitud formulada por la CNUDMI en la clausura de su 34º período de sesiones, celebrado en 2001. Está basada en las deliberaciones y decisiones de la Comisión en dicho período de sesiones[8], en el que se aprobó la Ley Modelo, así como en las observaciones del Grupo de Trabajo sobre Comercio Electrónico, que llevó a cabo la labor preparatoria.

Capítulo I. Introducción a la Ley Modelo

I. Finalidad y origen de la Ley Modelo

A. Finalidad

3. El creciente empleo de técnicas de autenticación electrónica en sustitución de las firmas manuscritas y de otros procedimientos tradicionales de autenticación ha planteado la necesidad de crear un marco jurídico específico para reducir la incertidumbre con respecto a las consecuencias jurídicas que pueden derivarse del empleo de dichas técnicas modernas (a las que puede denominarse en general

"firmas electrónicas"). El riesgo de que distintos países adopten criterios legislativos diferentes en relación con las firmas electrónicas exige disposiciones legislativas uniformes que establezcan las normas básicas de lo que constituye en esencia un fenómeno internacional, en el que es fundamental la interoperabilidad jurídica (y técnica).

4. Partiendo de los principios fundamentales que subyacen en el artículo 7 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico (denominada siempre en la presente publicación "Ley Modelo de la CNUDMI sobre Comercio Electrónico") con respecto al cumplimiento de la función de la firma en el ámbito electrónico, la finalidad de la Ley Modelo es ayudar a los Estados a establecer un marco legislativo moderno, armonizado y equitativo para abordar de manera más eficaz las cuestiones relativas a las firmas electrónicas. Como complemento modesto pero importante a la Ley Modelo de la CNUDMI sobre Comercio Electrónico, la Ley Modelo ofrece normas prácticas para comprobar la fiabilidad técnica de las firmas electrónicas. Además, la Ley Modelo ofrece un vínculo entre dicha fiabilidad técnica y la eficacia jurídica que cabe esperar de una determinada firma electrónica. La Ley Modelo supone una contribución importante a la Ley Modelo de la CNUDMI sobre Comercio Electrónico al adoptar un criterio conforme al cual puede determinarse previamente (o evaluarse con anterioridad a su empleo) la eficacia jurídica de una determinada técnica de creación de una firma electrónica. Así pues, la Ley Modelo tiene como finalidad mejorar el entendimiento de las firmas electrónicas y la seguridad de que puede confiarse en determinadas técnicas de creación de firma electrónica en operaciones de importancia jurídica. Además, al establecer con la flexibilidad conveniente una serie de normas básicas de conducta para las diversas partes que puedan participar en el empleo de firmas electrónicas (es decir, firmantes, terceros que actúen confiando en el certificado y terceros prestadores de servicios), la Ley Modelo puede ayudar a configurar prácticas comerciales más armoniosas en el ciberespacio.

5. Los objetivos de la Ley Modelo, entre los que figuran el de permitir o facilitar el empleo de firmas electrónicas y el de conceder igualdad de trato a los usuarios de documentación consignada sobre papel y a los de información consignada en soporte informático, son fundamentales para promover la economía y la eficacia del comercio internacional. Al incorporar a su derecho interno los procedimientos que se recogen en la Ley Modelo (y la Ley Modelo de la CNUDMI sobre Comercio Electrónico) para todo supuesto en que las partes opten por emplear medios electrónicos de comunicación, el Estado promulgante creará un entorno jurídico neutro para todo medio técnicamente viable de comunicación comercial.

B. Antecedentes

6. La Ley Modelo supone un nuevo paso en una serie de instrumentos internacionales aprobados por la CNUDMI, que se centran especialmente en las necesidades del comercio electrónico o que se prepararon teniendo en cuenta las necesidades de los medios de comunicación modernos. Dentro de la primera categoría, la de instrumentos concretos adaptados al comercio electrónico, se encuentra la Guía jurídica de la CNUDMI sobre transferencias electrónicas de fondos (1987), la Ley Modelo de la CNUDMI sobre Transferencias Internacionales de Crédito (1992) y la Ley Modelo de la CNUDMI sobre Comercio Electrónico

(1996 y 1998). En la segunda categoría figuran todas las convenciones y convenios internacionales y demás instrumentos legislativos aprobados por la CNUDMI desde 1978, en todos los cuales se promueve un menor formalismo y se recogen definiciones de “escrito” cuya finalidad es abarcar las comunicaciones inmateriales.

7. El instrumento más conocido de la CNUDMI en el ámbito del comercio electrónico es la Ley Modelo de la CNUDMI sobre Comercio Electrónico. Su preparación a comienzos del decenio de 1990 fue consecuencia del creciente empleo de medios modernos de comunicación, tales como el correo electrónico y el intercambio electrónico de datos (EDI) para la realización de operaciones comerciales internacionales. Se vio que las nuevas tecnologías se habían desarrollado con rapidez y seguirían desarrollándose a medida que continuara difundiéndose el acceso a soportes técnicos como las autopistas de la información y la Internet. No obstante, la comunicación de datos de cierta transcendencia jurídica en forma de mensaje sin soporte de papel podría verse obstaculizada por ciertos impedimentos legales al empleo de mensajes electrónicos, o por la incertidumbre que pudiera haber sobre la validez o eficacia jurídica de esos mensajes. La CNUDMI ha preparado la Ley Modelo de la CNUDMI sobre Comercio Electrónico para facilitar el creciente empleo de los medios de comunicación modernos. La finalidad de la Ley Modelo de la CNUDMI sobre Comercio Electrónico es la de ofrecer al legislador nacional un conjunto de reglas aceptables en el ámbito internacional que le permitan eliminar algunos de esos obstáculos jurídicos con miras a crear un marco jurídico que permita un desarrollo más seguro de las vías electrónicas de negociación designadas por el nombre de “comercio electrónico”.

8. La decisión de la CNUDMI de formular un régimen legal modelo para el comercio electrónico se debió a que el régimen aplicable en ciertos países a la comunicación y archivo de información era inadecuado o se había quedado anticuado, al no haberse previsto en ese régimen las modalidades propias del comercio electrónico. En algunos casos, la legislación vigente impone o supone restricciones al empleo de los medios de comunicación modernos, por ejemplo, al prescribir el empleo de documentos “escritos”, “firmados” u “originales”. Con respecto a los conceptos de documentos “escritos”, “firmados” u “originales”, la Ley Modelo de la CNUDMI sobre Comercio Electrónico adoptó un enfoque basado en la equivalencia funcional.

9. Cuando se estaba preparando la Ley Modelo de la CNUDMI sobre Comercio Electrónico, unos cuantos países habían adoptado reglas especiales para regular determinados aspectos del comercio electrónico. Pero no existía una legislación general del comercio electrónico. De ello podría resultar incertidumbre acerca de la naturaleza jurídica y la validez de la información presentada en otra forma que no fuera la de un documento tradicional sobre papel. Además, la necesidad de un marco legal seguro y de prácticas eficientes se hacía sentir no sólo en aquellos países en los que se estaba difundiendo el empleo del EDI y del correo electrónico, sino también en otros muchos países en los que se había difundido el empleo del fax, el télex y otras técnicas de comunicación parecidas.

10. Además, la Ley Modelo de la CNUDMI sobre Comercio Electrónico podía ayudar a remediar los inconvenientes que dimanaban del hecho de que un régimen legal interno inadecuado pudiera obstaculizar el comercio internacional, al depender una parte importante de ese comercio de la utilización de técnicas de comunicación modernas. En gran medida, la diversidad de los regímenes internos aplicables a esas

técnicas de comunicación y la incertidumbre que ocasione esa disparidad puede contribuir a limitar el acceso de las empresas a los mercados internacionales.

11. Añádase a ello que, la Ley Modelo de la CNUDMI sobre Comercio Electrónico puede resultar un valioso instrumento, en el ámbito internacional, para interpretar ciertos convenios y otros instrumentos internacionales existentes que impongan obstáculos jurídicos al empleo del comercio electrónico, al prescribir, por ejemplo, que se han de consignar por escrito ciertos documentos o cláusulas contractuales. Caso de adoptarse la Ley Modelo de la CNUDMI sobre Comercio Electrónico como regla de interpretación al respecto, los Estados partes en esos instrumentos internacionales dispondrían de un medio para reconocer la validez del comercio electrónico sin necesidad de tener que negociar un protocolo para cada uno de esos instrumentos internacionales en particular.

C. Historia

12. Tras aprobar la Ley Modelo de la CNUDMI sobre Comercio Electrónico, 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 sobre Comercio Electrónico que examinara la conveniencia y viabilidad de preparar un régimen uniforme sobre los temas mencionados. Se convino en que el régimen uniforme que había que preparar se refiriera a cuestiones tales como: la base jurídica que sustenta los procesos de certificación, incluida la tecnología incipiente de autenticación y certificación digitales; la aplicabilidad del proceso de certificación; la asignación del riesgo y la responsabilidad de los usuarios, proveedores y terceros en el contexto del uso de técnicas de certificación; las cuestiones concretas relativas a la certificación mediante el uso de registros y la incorporación por remisión[3].

13. En su 30º período de sesiones (1997), la Comisión tuvo ante sí el informe del Grupo de Trabajo acerca de la labor de su 31º período de sesiones (A/CN.9/437). El Grupo de Trabajo indicó a la Comisión que había logrado un consenso en relación con la importancia y la necesidad de proceder a la armonización de la legislación en ese ámbito. El Grupo de Trabajo no había adoptado una decisión firme respecto de la forma y el contenido de su labor al respecto, si bien había llegado a la conclusión preliminar de que era viable emprender la preparación de un proyecto de régimen uniforme sobre cuestiones relacionadas con las firmas numéricas y las entidades certificadoras, y posiblemente sobre cuestiones conexas. El Grupo de Trabajo recordó que, al margen de las cuestiones de las firmas numéricas y las entidades certificadoras, también podía ser necesario examinar las cuestiones siguientes en el ámbito del comercio electrónico: alternativas técnicas a la criptografía de clave pública; cuestiones generales relacionadas con las funciones desempeñadas por los terceros proveedores de servicios; y la contratación electrónica (A/CN.9/437, párrs. 156 y 157). La Comisión hizo suyas las conclusiones a las que había llegado el Grupo de Trabajo y le encomendó la preparación de un régimen uniforme sobre las cuestiones jurídicas de las firmas numéricas y las autoridades certificadoras.

14. Con respecto a la forma y al alcance exactos del régimen uniforme, la Comisión convino de manera general en que no era posible adoptar una decisión al respecto en una etapa tan temprana. Se opinó que, si bien el Grupo de Trabajo

podría concentrar su atención en las cuestiones de las firmas numéricas, en vista de la función predominante aparentemente desempeñada por la criptografía de clave pública en la práctica más reciente en materia de comercio electrónico, el régimen uniforme que se preparara debería atenerse al criterio de neutralidad adoptado en la Ley Modelo de la CNUDMI sobre Comercio Electrónico en lo relativo a los diversos medios técnicos disponibles. Por ello, el régimen uniforme no debería desalentar el recurso a otras técnicas de autenticación. Además, al ocuparse de la criptografía de clave pública, tal vez fuera preciso que el régimen uniforme diera cabida a diversos grados de seguridad y reconociera diversos efectos jurídicos y grados de responsabilidad según cuáles fueran los servicios prestados en el contexto de las firmas numéricas. Respecto de las entidades certificadoras, si bien la Comisión reconoció el valor de las normas de fiabilidad o seguridad fijadas por el mercado, predominó el parecer de que el Grupo de Trabajo podría considerar el establecimiento de un conjunto de normas mínimas que las entidades certificadoras habrían de respetar estrictamente, particularmente en casos en los que se solicitara una certificación de validez transfronteriza[4].

15. El Grupo de Trabajo empezó a preparar el régimen uniforme (que luego se aprobó como la Ley Modelo) en su 32º período de sesiones a partir de una nota preparada por la Secretaría (A/CN.9/WG.IV/WP.73).

16. 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, en sus períodos de sesiones 31º y 32º había tropezado con evidentes dificultades para llegar a una concepción común de las nuevas cuestiones jurídicas planteadas por la mayor utilización de las firmas numéricas y otras firmas electrónicas. Se observó también que todavía no se había llegado a un consenso respecto del modo de abordar estas cuestiones en un marco jurídico internacionalmente aceptable. No obstante, la Comisión consideró, en general, que los progresos logrados hacían pensar que el proyecto de régimen uniforme para las firmas electrónicas iba adquiriendo gradualmente una configuración viable.

17. La Comisión reafirmó la decisión de su 30º período de sesiones sobre la viabilidad de preparar ese régimen uniforme, e indicó que confiaba en que el Grupo de Trabajo llevaría adelante su labor en su 33º período de sesiones sobre la base del proyecto revisado que había preparado la Secretaría (A/CN.9/WG.IV/WP.76). En el curso del debate, la Comisión observó con satisfacción que el Grupo de Trabajo gozaba de general reconocimiento como foro internacional de especial importancia para intercambiar opiniones sobre los problemas jurídicos del comercio electrónico, y para buscar soluciones a esos problemas[5].

18. El Grupo de Trabajo siguió examinando el régimen uniforme en sus períodos de sesiones 33º (1998) y 34º (1999) sobre la base de las notas preparadas por la Secretaría (A/CN.9/WG.IV/WP.76 y A/CN.9/WG.IV/WP.79 y 80). Los informes de dichos períodos de sesiones figuran en los documentos A/CN.9/454 y 457.

19. En su 32º período de sesiones (1999), la Comisión tuvo ante sí el informe del Grupo de Trabajo acerca de la labor de esos dos períodos de sesiones (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 se había enfrentado con dificultades para formar un consenso con respecto a la política legislativa en que debía basarse el régimen uniforme.

20. 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. Según esa opinión, el régimen uniforme, tal y como ahora lo concebía el Grupo de Trabajo, hacía demasiado hincapié en las técnicas de la firma numérica y, en la esfera de la firma numérica, en una aplicación específica de ésta que requería la certificación de terceros. Por tanto, se sugirió que la labor del Grupo de Trabajo respecto de las firmas electrónicas se limitase a las cuestiones jurídicas de la certificación de validez transfronteriza o se aplazara completamente hasta que las prácticas del mercado se hubiesen establecido con mayor claridad. Se expresó una opinión conexa en el sentido de que, para los fines del comercio internacional, casi todas las cuestiones jurídicas emanadas de la utilización de las firmas electrónicas ya estaban resueltas en la Ley Modelo de la CNUDMI sobre Comercio Electrónico (véase *supra*, párr. 28). Si bien podía ser necesario 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.

21. Según la opinión ampliamente predominante, el Grupo de Trabajo debía continuar su tarea sobre la base de su mandato original. 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 certificadoras y los terceros que confían en el certificado) correspondía a un posible modelo de ICP, otros modelos eran concebibles, por ejemplo, en los 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 de la Ley Modelo 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 confiar. 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 que dos de esas funciones las desempeñase la misma persona (por ejemplo, cuando la entidad certificadora fuese asimismo el tercero que confían en el certificado). 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 en una etapa ulterior de una norma plenamente neutral respecto de los medios técnicos utilizados (ibíd., párr. 68).

22. Tras un debate, la Comisión reafirmó sus decisiones anteriores en cuanto a la viabilidad de preparar un régimen uniforme y expresó su confianza en la posibilidad de que el Grupo de Trabajo alcanzara progresos aún mayores en sus próximos períodos de sesiones[6].

23. El Grupo de Trabajo continuó con su labor en sus períodos de sesiones 35º (septiembre de 1999) y 36º (febrero de 2000) sobre la base de las notas preparadas por la Secretaría (A/CN.9/WG.IV/WP.82 y 84). En su 33º período de sesiones (2000), la Comisión tuvo ante sí el informe del Grupo de Trabajo acerca de la labor de esos dos períodos de sesiones (A/CN.9/465 y 467). Se observó que el Grupo de Trabajo había aprobado, en su 36º período de sesiones, los proyectos de artículos 1 y 3 a 12 del régimen uniforme. Se dijo que quedaban algunas cuestiones que debían aclararse ante la decisión del Grupo de Trabajo de suprimir el concepto de firma electrónica refrendada del proyecto de régimen uniforme. Se expresó, la inquietud de que, dependiendo de la decisión que adoptara el Grupo de Trabajo con respecto a los proyectos de artículos 2 y 13, pudiera ser necesario volver a examinar el resto de las disposiciones del proyecto a fin de evitar que se creara una situación en la que la norma fijada por el régimen uniforme se aplicara de forma igual a las firmas electrónicas que aseguraban un alto nivel de seguridad y a los certificados de bajo valor que pudieran emplearse en el ámbito de las comunicaciones electrónicas cuya finalidad no era producir efectos jurídicos importantes.

24. Tras el debate, la Comisión expresó su reconocimiento por la labor realizada por el Grupo de Trabajo y por los progresos logrados en la preparación del proyecto de régimen uniforme. Se instó al Grupo de Trabajo a que, en su 37º período de sesiones, finalizara la labor relativa al régimen uniforme y examinara el proyecto de guía para su incorporación al derecho interno que prepararía la Secretaría[7].

25. El Grupo de Trabajo concluyó la preparación del régimen uniforme en su 37º período de sesiones (celebrado en septiembre de 2000). El informe de ese período de sesiones figura en el documento A/CN.9/483. El Grupo de Trabajo examinó igualmente el proyecto de guía para la incorporación al derecho interno. Se pidió a la Secretaría que prepara una versión revisada del proyecto de guía que reflejase las decisiones adoptadas por el Grupo de Trabajo, sobre la base de las diversas opiniones, sugerencias y preocupaciones expresadas en el presente período de sesiones. A falta de tiempo, el Grupo de Trabajo no terminó sus deliberaciones sobre el proyecto de guía para la incorporación al derecho interno. Se convino en que el Grupo de Trabajo reservase cierto tiempo en su 38º período de sesiones para terminar ese tema del programa. Se observó que el régimen uniforme (en la forma de un proyecto de Ley Modelo de la CNUDMI para las Firmas Electrónicas), junto con el proyecto de guía para la incorporación al derecho interno, se presentaría a la Comisión para su examen y aprobación en el 34º período de sesiones (2001) de ésta. *[Nota de la Secretaría: la presente sección en la que figura la historia de la Ley Modelo tendrá que completarse, y posiblemente se hará algo más concisa, una vez que la Comisión lleve a cabo el examen final y apruebe la Ley Modelo]*.

II. La Ley Modelo como instrumento de armonización de leyes

26. Al igual que la Ley Modelo de la CNUDMI sobre Comercio Electrónico, la Ley Modelo reviste la forma de un texto legislativo que se recomienda a los Estados

para que lo incorporen a su derecho interno. A diferencia de un convenio o convención internacional, la legislación modelo no requiere que el Estado promulgante lo notifique a las Naciones Unidas o a otros Estados que asimismo puedan haberlo promulgado. No obstante, se recomienda encarecidamente a los Estados que informen a la Secretaría de la CNUDMI de la promulgación de la Ley Modelo (o de cualquier otra ley modelo elaborada por la CNUDMI).

27. Al incorporar el texto de una ley modelo en su derecho interno, los Estados pueden modificar o excluir algunas de sus disposiciones. En el caso de un convenio o convención, la posibilidad de que los Estados partes hagan modificaciones al texto uniforme (lo que normalmente se denomina "reservas") está mucho más limitada; los convenios y convenciones de derecho mercantil en especial prohíben normalmente las reservas o permiten sólo algunas específicas. La flexibilidad inherente a la legislación modelo es particularmente conveniente en los casos en que es probable que los Estados deseen hacer varias modificaciones al texto uniforme antes de incorporarlo a su derecho interno. En particular, cabe esperar algunas modificaciones cuando el texto uniforme está estrechamente relacionado con el sistema procesal y judicial nacional. No obstante, ello supone también que el grado de armonización y certeza que se logra mediante la legislación modelo es probablemente inferior al de un convenio o convención. Sin embargo, esta desventaja relativa de la legislación modelo puede compensarse con el hecho de que el número de Estados promulgantes de la legislación modelo será probablemente superior al número de Estados que se adhieren a un convenio o convención. Para lograr un grado satisfactorio de armonización y certeza se recomienda que los Estados hagan el menor número posible de modificaciones al incorporar la nueva Ley Modelo a su derecho interno. En general, al promulgar la nueva Ley Modelo (o la Ley Modelo de la CNUDMI sobre Comercio Electrónico), es aconsejable ajustarse lo más posible al texto uniforme a fin de que el derecho interno sea lo más transparente y familiar posible para los extranjeros que recurran a él.

28. Cabe señalar que algunos países estiman que las cuestiones jurídicas relacionadas con la utilización de la firma electrónica han quedado resueltas con la Ley Modelo de CNUDMI sobre Comercio Electrónico y no tienen previsto adoptar ninguna otra normativa sobre la firma electrónica hasta que las prácticas del mercado en esta nueva esfera estén mejor asentadas. Sin embargo, los Estados que incorporen a su derecho interno la nueva Ley Modelo junto con la Ley Modelo de la CNUDMI sobre Comercio Electrónico pueden esperar otros beneficios. Para los países en los que las autoridades gubernamentales y legislativas están preparando leyes sobre cuestiones relacionadas con las firmas electrónicas, incluido el establecimiento de infraestructuras de clave pública (ICP), la Ley Modelo ofrece la orientación de un instrumento internacional que se preparó teniendo presentes las cuestiones y la terminología relacionadas con las ICP. Para todos los países, la Ley Modelo ofrece un conjunto de normas básicas que pueden aplicarse independientemente del modelo de ICP, ya que prevén la interacción de tres funciones distintas que pueden intervenir en cualquier tipo de firma electrónica (es decir, crear, certificar y confiar en una firma electrónica). Esas tres funciones deben abordarse prescindiendo de si son de hecho desempeñadas por tres entidades separadas o si dos de esas funciones lo son por la misma persona (por ejemplo, cuando desempeña la función de certificación una parte que confía en la firma). La Ley Modelo presenta, en consecuencia, un terreno común para los sistemas de ICP que confían en entidades de certificación independientes y sistemas de firma

electrónica en los que no participa ese tercero independiente en el proceso de la firma electrónica. En todos los casos, la nueva Ley Modelo aporta una mayor certidumbre en lo que respecta a la eficacia jurídica de las firmas electrónicas, sin limitar la posibilidad de recurrir al criterio flexible consagrado en el artículo 7 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico (véanse *infra*, los párrs. 67 y 70 a 75).

III. Observaciones generales sobre las firmas electrónicas[8]

A. Funciones de las firmas

29. El artículo 7 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico se basa en el reconocimiento de las funciones que cumple una firma manuscrita en papel. Durante la preparación de la Ley Modelo de la CNUDMI sobre Comercio Electrónico, el Grupo de Trabajo examinó las siguientes funciones tradicionales de las firmas manuscritas: identificar a una persona, proporcionar certidumbre en cuanto a su participación personal en el acto de la firma; y vincular a esa persona con el contenido de un documento. Se señaló además que una firma podía cumplir diversas funciones, según cuál fuera la naturaleza del documento firmado. Por ejemplo, una firma podía constituir un testimonio de la intención de una parte de considerarse vinculada por el contenido de un contrato firmado, de la intención de una persona de respaldar la autoría de un texto (manifestando así su consciencia de que del acto de la firma podrían derivarse consecuencias jurídicas), de la intención de una persona de asociarse al contenido de un documento escrito por otra persona, y del hecho de que una persona estuviera en un lugar determinado en un momento determinado. En los párrafos 67 y 70 a 75 de la presente Guía se sigue examinando la relación de la Ley Modelo con el artículo 7 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico.

30. En un entorno electrónico, el original de un mensaje no se puede distinguir de una copia, no lleva una firma manuscrita y no figura en papel. Las posibilidades de fraude son considerables debido a la facilidad con que se pueden interceptar y alterar datos en forma electrónica sin posibilidad de detección y a la velocidad con que se procesan operaciones múltiples. La finalidad de las diversas técnicas que ya están disponibles en el mercado o que se están desarrollando es ofrecer medios técnicos para que algunas o todas las funciones identificadas como características de las firmas manuscritas se puedan cumplir en un entorno electrónico. Estas técnicas se pueden denominar, en general, "firmas electrónicas".

B. Firmas numéricas y otras firmas electrónicas

31. Al examinar la conveniencia y viabilidad de preparar la nueva Ley Modelo y de definir el ámbito de un régimen uniforme, la CNUDMI ha examinado varias técnicas de firmas electrónicas ya disponibles o en desarrollo. La finalidad común de dichas técnicas es proporcionar equivalentes funcionales de las 1) firmas manuscritas y 2) de otros tipos de mecanismos de autenticación empleados en soporte de papel (por ejemplo, sellos o timbres). Las mismas técnicas pueden desempeñar en el ámbito del comercio electrónico otras funciones derivadas de las

funciones de la firma pero que no correspondan a un equivalente estricto en soporte de papel.

32. Como ya se ha indicado (véanse los párrafos 21 y 28), los órganos ejecutivos y legislativos de muchos países que están preparando legislación sobre cuestiones relacionadas con las firmas electrónicas, incluido el establecimiento de infraestructuras de clave pública (ICP), u otros proyectos sobre cuestiones estrechamente relacionadas, esperan recibir orientación de la CNUDMI (véase A/CN.9/457, párr. 16). En cuanto a la decisión adoptada por la CNUDMI de centrarse en cuestiones y terminología relativas a las ICP, debería señalarse que la relación existente entre tres tipos distintos de partes (a saber, firmantes, prestadores de servicios de certificación y partes que confían en el certificado) corresponde a un modelo posible de ICP, pero que ya se utilizan corrientemente en el mercado otros modelos (por ejemplo, sin la participación de ninguna entidad certificadora independiente). Una de las principales ventajas de centrarse en las cuestiones de ICP es facilitar la elaboración de una Ley Modelo por remisión a tres funciones (o papeles) con respecto a las firmas electrónicas, a saber, la función del firmante (emisor o suscriptor de la clave), la función de certificación y la función de confianza. Estas tres funciones son comunes a todos los modelos de ICP y deberían tratarse en cualquier caso independientemente de que las desempeñen tres organismos independientes o de que la misma persona desempeñe dos de dichas funciones (por ejemplo, si el prestador de los servicios de certificación es también tercero que confía en el certificado). Centrarse en las funciones que se llevan a cabo en un entorno de ICP y no hacerlo en un modelo concreto facilita también el desarrollo de una norma de neutralidad respecto de los medios técnicos utilizables en la medida en que en la tecnología de firmas electrónicas que no sean de ICP se prestan funciones análogas.

1. Firmas electrónicas basadas en técnicas distintas de la criptografía de clave pública

33. Además de las Afirmas numéricas@ basadas en la criptografía de clave pública, hay otros diversos dispositivos, también incluidos en el concepto más amplio de mecanismos de Afirma electrónica@ que ya se están utilizando o que se prevé utilizar en el futuro con miras a cumplir una o más de las funciones de las firmas manuscritas mencionadas anteriormente. Por ejemplo, ciertas técnicas se basarían en la autenticación mediante un dispositivo biométrico basado en las firmas manuscritas. Con este dispositivo el firmante firmaría de forma manual utilizando un lápiz especial en una pantalla de computadora o en un bloc numérico. La firma manuscrita sería luego analizada por la computadora y almacenada como un conjunto de valores numéricos que se podrían agregar a un mensaje de datos y que el receptor podría recuperar en pantalla para autenticar la firma. Este sistema de autenticación exigiría el análisis previo de muestras de firmas manuscritas y su almacenamiento utilizando el dispositivo biométrico. Otras técnicas entrañan el uso de números de identificación personal (NIP), versiones digitalizadas de firmas manuscritas y otros métodos, como la selección de un signo afirmativo en la pantalla electrónica mediante el ratón.

34. La CNUDMI ha tratado de elaborar una legislación uniforme que pueda facilitar el empleo tanto de las firmas numéricas como de otras formas de firmas

electrónicas. A ese fin, la CNUDMI ha tratado de abordar las cuestiones jurídicas de las firmas electrónicas a un nivel intermedio entre la gran generalidad de la Ley Modelo de la CNUDMI sobre Comercio Electrónico y la especificidad que podría requerirse al abordar una técnica de firma determinada. En cualquier caso, y siguiendo el criterio de neutralidad respecto de los medios técnicos de la Ley Modelo de la CNUDMI sobre Comercio Electrónico, no debe interpretarse que la Ley Modelo desalienta el empleo de cualquier método de firma electrónica ya existente o que pueda aplicarse en el futuro.

2. Firmas numéricas basadas en la criptografía de clave pública[9]

35. Ante el creciente empleo de técnicas de firma numérica en diversos países, la siguiente introducción puede ayudar a los que están preparando legislación sobre las firmas electrónicas.

a) Terminología y conceptos técnicos

i) Criptografía

36. Las firmas numéricas se crean y verifican utilizando la criptografía, la rama de las matemáticas aplicadas que se ocupa de transformar mensajes en formas aparentemente ininteligibles y devolverlas a su forma original. Las firmas numéricas utilizan lo que se denomina “criptografía de clave pública”, que con frecuencia se basa en el empleo de funciones algorítmicas para generar dos “claves” diferentes pero matemáticamente relacionadas entre sí (por ejemplo, grandes números producidos utilizando una serie de fórmulas matemáticas aplicadas a números primos). Una de esas claves se utiliza para crear una firma numérica o transformar datos en una forma aparentemente ininteligible, y la otra para verificar una firma numérica o devolver el mensaje a su forma original. El equipo y los programas informáticos que utilizan dos de esas claves se suelen denominar en conjunto “criptosistemas” o, más concretamente, “criptosistemas asimétricos” cuando se basan en el empleo de algoritmos asimétricos.

37. Si bien el empleo de la criptografía es una de las características principales de las firmas numéricas, el mero hecho de que una firma numérica se utilice para autenticar un mensaje que contiene información en forma numérica, no debe confundirse con el uso más general de la criptografía con fines de confidencialidad. El cifrado con fines de confidencialidad es un método utilizado para codificar una comunicación electrónica de modo que sólo el originador y el destinatario del mensaje puedan leerlo. En algunos países, el empleo de la criptografía con fines de confidencialidad está limitado por ley por razones de orden público que pueden incluir consideraciones de defensa nacional. Ahora bien, el empleo de la criptografía con fines de autenticación para crear una firma numérica, no implica necesariamente el empleo del cifrado para dar carácter confidencial a la información durante el proceso de comunicación, dado que la firma numérica codificada puede sencillamente añadirse a un mensaje no codificado.

ii) Claves públicas y privadas

38. Las claves complementarias utilizadas para las firmas numéricas se denominan "clave privada", que se utiliza sólo por el firmante para crear la firma numérica, y "clave pública", que de ordinario conocen más personas y se utiliza para que el tercero que actúa confiando en el certificado pueda verificar la firma numérica. El usuario de una clave privada debe mantenerla en secreto. Hay que señalar que el usuario individual no necesita conocer la clave privada. Esa clave privada probablemente se mantendrá en una tarjeta inteligente, o se podrá acceder a ella mediante un número de identificación personal o, en una situación ideal, mediante un dispositivo de identificación biométrica, por ejemplo, mediante el reconocimiento de una huella digital. Si es necesario que muchas personas verifiquen firmas numéricas del firmante, la clave pública debe estar a disposición o en poder de todas ellas, por ejemplo publicándola en una base de datos de acceso electrónico o en cualquier otro directorio público de fácil acceso. Si bien las claves del par están matemáticamente relacionadas entre sí, el diseño y la ejecución en forma segura de un criptosistema asimétrico hace virtualmente imposible que las personas que conocen la clave pública puedan deducir de ella la clave privada. Los algoritmos más comunes para la codificación mediante el empleo de claves públicas y privadas se basan en una característica importante de los grandes números primos: una vez que se multiplican entre sí para obtener un nuevo número, constituye una tarea larga y difícil determinar cuáles fueron los dos números primos que crearon ese nuevo número mayor[10]. De esa forma, aunque muchas personas puedan conocer la clave pública de un firmante determinado y utilizarla para verificar las firmas de éste, no podrán descubrir la clave privada del firmante y utilizarla para falsificar firmas numéricas.

39. Cabe señalar, sin embargo, que el concepto de criptografía de clave pública no implica necesariamente el empleo de los algoritmos mencionados anteriormente basados en números primos. En la actualidad se están utilizando o desarrollando otras técnicas matemáticas, como los criptosistemas de curvas elípticas, que se suelen describir como sistemas que ofrecen un alto grado de seguridad mediante el empleo de longitudes de clave notablemente reducidas.

iii) La función control

40. Además de la creación de pares de claves, se utiliza otro proceso fundamental, generalmente conocido con el nombre de "función control", tanto para crear como para verificar una firma numérica. La función control es un proceso matemático, basado en un algoritmo que crea una representación numérica o forma comprimida del mensaje, a menudo conocida con el nombre de "compendio de mensaje" o "huella digital" del mensaje, en forma de un "valor control" o "resultado control" de una longitud estándar que suele ser mucho menor que la del mensaje, pero que es no obstante esencialmente única con respecto al mismo. Todo cambio en el mensaje produce invariablemente un resultado control diferente cuando se utiliza la misma función control. En el caso de una función control segura, a veces denominada "función control unidireccional", es virtualmente imposible deducir el mensaje original aun cuando se conozca su valor control. Por tanto las funciones control hacen posible que el programa de creación de firmas numéricas funcione con cantidades más pequeñas y predecibles de datos, proporcionando no obstante una

consistente correlación testimonial con respecto al contenido original del mensaje, y dando garantías efectivas de que el mensaje no ha sido modificado desde que se firmó en forma numérica.

iv) La firma numérica

41. Para firmar un documento o cualquier otro material de información, el firmante delimita primero en forma precisa el espacio de lo que se ha de firmar. Seguidamente, mediante la función control del programa informático del firmante se obtiene un resultado control único, a todos los fines prácticos, de la información que se firme. El programa del firmante transforma luego el resultado control en una firma numérica utilizando la clave privada del firmante. La firma numérica resultante es, por lo tanto, exclusiva de la información firmada y de la clave privada utilizada para crearla.

42. Normalmente, la firma numérica (es decir, el resultado control con firma numérica del mensaje) se adjunta al mensaje y se almacena o transmite junto con éste. Ahora bien, puede también ser enviado o almacenado como un conjunto de datos independiente, siempre que mantenga una vinculación fiable con el mensaje correspondiente. Dado que una firma numérica es exclusiva de un mensaje, resulta inútil si se la desvincula de éste permanentemente.

v) Verificación de la firma numérica

43. La verificación de la firma numérica es el proceso de comprobar esa firma por remisión al mensaje original y a una clave pública dada, determinando de esa forma si la firma numérica fue creada para ese mismo mensaje utilizando la clave privada que corresponde a la clave pública remitida. La verificación de una firma numérica se logra calculando un nuevo resultado control del mensaje original mediante la misma función control utilizada para crear la firma numérica. Seguidamente, utilizando la clave pública y el nuevo resultado control, el verificador comprueba si la firma numérica fue creada utilizando la clave privada correspondiente y si el nuevo resultado control calculado corresponde al resultado control original que fue transformado en la firma numérica durante el proceso de la firma.

44. El programa de verificación confirmará la firma numérica como “verificada”: 1) si se utilizó la clave privada del firmante para firmar numéricamente el mensaje, lo que ocurre si se utilizó la clave pública del firmante para verificar la firma, dado que esta clave pública sólo verificará una firma numérica creada con la clave privada del firmante; y 2) si el mensaje no fue modificado, lo que ocurre si el resultado control calculado por el verificador es idéntico al resultado control extraído de la firma numérica durante el proceso de verificación.

b) Infraestructura de clave pública (ICP) y prestadores de servicios de certificación

45. Para verificar una firma numérica, el verificador debe tener acceso a la clave pública del firmante y tener la seguridad de que corresponde a la clave privada de éste. Ahora bien, un par de claves pública y privada no tiene ninguna vinculación

intrínseca con ninguna persona; es simplemente un par de números. Se necesita un mecanismo adicional para vincular en forma fiable a una persona o entidad determinada al par de claves. Para que la codificación de la clave pública pueda cumplir su función específica, es necesario disponer de un medio de enviar claves a una gran diversidad de personas, muchas de las cuales no son conocidas del remitente y con las que no ha desarrollado ninguna relación de confianza. A tal efecto, las partes interesadas deben tener un alto grado de confianza en las claves pública y privada que se emitan.

46. El nivel de confianza requerido puede existir entre partes que confíen unas en otras, que se hayan tratado durante algún tiempo, que se comuniquen mediante sistemas cerrados, que operen dentro de un grupo cerrado, o que puedan regir sus operaciones en base a un contrato, por ejemplo, en un acuerdo de asociación comercial. En una transacción en la que participen sólo dos partes, cada una puede sencillamente comunicar (por un canal relativamente seguro, como un servicio de mensajería o el teléfono, que conlleva el reconocimiento de la voz) la clave pública del par de claves que cada parte utilizará. Ahora bien, este nivel de confianza puede no existir entre partes que no realicen transacciones con frecuencia, que se comuniquen a través de sistemas abiertos (por ejemplo, Internet), que no formen parte de un grupo cerrado o que no tengan acuerdos de asociación comercial u otros acuerdos que rijan sus relaciones.

47. Además, dado que la codificación de clave pública es una tecnología altamente matemática, todos los usuarios deben tener confianza en las aptitudes, los conocimientos y los dispositivos de seguridad de las partes que emitan las claves pública y privada[11].

48. Un firmante potencial podría hacer una declaración pública indicando que las firmas verificables por una clave pública determinada deben ser consideradas como procedentes de ese firmante. Ahora bien, puede que otras partes no estén dispuestas a aceptar la declaración, especialmente si no hay ningún contrato previo que establezca con certeza el efecto jurídico de esa declaración publicada. La parte que se base en esa declaración publicada sin ningún respaldo en un sistema abierto corre un gran riesgo de confiar inadvertidamente en un impostor, o de tener que impugnar con buen éxito la negativa falsa de una firma numérica (cuestión a menudo mencionada en el contexto del “repudio negativo” de firmas numéricas) si la operación resulta desfavorable para el supuesto firmante.

49. Una de las soluciones a estos problemas es el empleo de uno o más terceros de confianza para vincular a un firmante identificado o el nombre del firmante a una clave pública determinada. El tercero en quien se confía se conoce en general, en la mayoría de las normas y directrices técnicas, como “entidad certificadora”, “prestador de servicios de certificación” o “proveedor de servicios de certificación” (en la Ley Modelo, se ha elegido el término de “prestador de servicios de certificación”). En unos cuantos países, esas entidades certificadoras están siendo organizadas en forma jerárquica en lo que suele denominarse una infraestructura de clave pública (ICP).

i) Infraestructura de clave pública (ICP)

50. El establecimiento de una infraestructura de clave pública (ICP) es una forma de ofrecer confianza en que: 1) la clave pública del usuario no ha sido alterada y corresponde de hecho a la clave privada del mismo usuario; 2) se han utilizado buenas técnicas de codificación; 3) se puede confiar en las entidades que emiten las claves criptográficas en cuanto a la retención o al restablecimiento de las claves pública y privada que se puedan utilizar para efectuar una codificación de confidencialidad en los casos en que esté autorizado el empleo de esta técnica; 4) los sistemas de codificación diferentes son intercambiables. Para poder ofrecer el grado de confianza descrito más arriba, una ICP puede ofrecer diversos servicios, incluidos los siguientes: 1) gestión de las claves criptográficas utilizadas para las firmas numéricas; 2) certificación de que una clave pública corresponde a una clave privada; 3) provisión de claves a usuarios finales; 4) establecimiento de los privilegios que tendrán los diversos usuarios de un sistema; 5) publicación de una guía segura de certificados o claves públicas; 6) administración de contraseñas personales (por ejemplo, tarjetas inteligentes) que permitan identificar al usuario con información de identificación personal singular o que permitan generar y almacenar claves privadas individuales; 7) comprobación de la identificación de los usuarios finales y prestación de servicios a éstos; 8) prestación de servicios de repudio negativo; 9) prestación de servicios de marcado cronológico; 10) gestión de las claves de codificación utilizadas con fines de confidencialidad en los casos en que esté autorizado el empleo de esa técnica.

51. Una infraestructura de clave pública (ICP) se suele basar en diversos niveles jerárquicos de autoridad. Por ejemplo, los modelos considerados en ciertos países para el establecimiento de una posible ICP entrañan referencias a los siguientes niveles: 1) una “entidad principal” única que certificaría la tecnología y las prácticas a todas las partes autorizadas a emitir certificados o pares de claves criptográficas en relación con el empleo de dichos pares de claves, y llevaría un registro de las entidades de certificación subordinadas[12]; 2) diversas entidades de certificación, situadas bajo la autoridad “principal” que certificarían que la clave pública de un usuario corresponde en realidad a la clave privada del mismo usuario (es decir que no ha sido alterada); y 3) diversas entidades locales de registro, situadas bajo las autoridades de certificación, que reciban de los usuarios peticiones de pares de claves criptográficas o de certificados relativos al empleo de esos pares de claves, y que exijan pruebas de identidad a los posibles usuarios y las verifiquen. En ciertos países, se prevé que los notarios podrían actuar como entidades locales de registro o prestar apoyo a dichas entidades.

52. Las cuestiones de la ICP quizá no se presten fácilmente a la armonización a nivel internacional. La organización de una ICP puede comprender diversas cuestiones técnicas, así como cuestiones de orden público que es preferible dejar al arbitrio de cada Estado[13]. A este respecto, quizá sea necesario que cada Estado que contemple el establecimiento de una ICP adopte decisiones, por ejemplo, respecto de: 1) la forma y el número de niveles de entidades que se incluirán en una ICP; 2) si sólo las entidades certificadoras pertenecientes a la ICP podrán emitir pares de claves criptográficas o si éstos podrían ser emitidos también por los propios usuarios; 3) si las entidades certificadoras de la validez de los pares de claves criptográficas deben ser entidades públicas o si también las entidades privadas podrían actuar como entidades certificadoras; 4) si el proceso de autorizar a una

entidad determinada para actuar como entidad certificadora debería adoptar la forma de una autorización expresa, o "licencia", por parte del Estado, o si se deberían utilizar otros métodos para controlar la calidad de las operaciones de las entidades certificadoras permitiendo que éstas actúen sin una autorización específica; 5) el grado en el que el empleo de la criptografía se debe autorizar para fines de confidencialidad; y 6) si las autoridades gubernamentales deben retener el acceso a la información codificada mediante un mecanismo de "custodia de claves" o de otro tipo. La Ley Modelo no aborda estas cuestiones.

ii) Prestadores de servicios de certificación

53. Para vincular un par de claves a un posible firmante, el prestador de servicios de certificación (o entidad certificadora) emite un certificado, un registro electrónico que indica una clave pública junto con el nombre del suscriptor del certificado como "sujeto" del certificado, y puede confirmar que el firmante potencial que figura en el certificado posee la clave privada correspondiente. La función principal del certificado es vincular una clave pública con un titular determinado. El "receptor" del certificado que desee confiar en una firma numérica creada por el tenedor que figura en el certificado puede utilizar la clave pública indicada en ese certificado para verificar si la firma numérica fue creada con la clave privada correspondiente. Si dicha verificación es positiva, se obtiene la garantía de que la firma numérica fue creada por el tenedor de la clave pública que figura en el certificado, y que el mensaje correspondiente no ha sido modificado desde que fue firmado en forma numérica.

54. Para asegurar la autenticidad del certificado con respecto tanto a su contenido como a su fuente, la entidad certificadora lo firma en forma numérica. La firma numérica de la entidad certificadora que figura en el certificado se puede verificar utilizando la clave pública de esta última que está recogida en otro certificado de otra entidad certificadora (que puede ser de un nivel jerárquico superior aunque no tiene que serlo necesariamente), y ese otro certificado puede ser a su vez autenticado utilizando la clave pública incluida en un tercer certificado, y así sucesivamente hasta que la persona que confíe en la firma numérica tenga seguridad suficiente de su autenticidad. En todos los casos, la entidad que emita el certificado deberá firmarlo en forma numérica durante el período de validez del otro certificado utilizado para verificar la firma numérica de la entidad certificadora.

55. La firma numérica correspondiente a un mensaje, ya sea creada por el tenedor de un par de claves para autenticar un mensaje o por una entidad certificadora para autenticar su certificado, deberá contener por lo general un sello cronológico fiable para que el verificador pueda determinar con certeza si la firma numérica fue creada durante el "período de validez" indicado en el certificado, que es una condición para poder verificar una firma numérica.

56. Para que una clave pública y su correspondencia con un tenedor específico se pueda utilizar fácilmente en una verificación, el certificado debe publicarse en un repositorio o difundirse por otros medios. Normalmente, los repositorios son bases de datos electrónicas de certificados y de otro tipo de información a los que se puede acceder y que pueden utilizarse para verificar firmas numéricas.

57. Una vez emitido, puede que un certificado no sea fiable, por ejemplo si el titular falsifica su identidad ante la entidad certificadora. En otros casos, un certificado puede ser suficientemente fiable cuando se emite pero dejar de serlo posteriormente. Si la clave privada ha quedado "en entredicho", por ejemplo si el tenedor de la clave ha perdido el control de ésta, el certificado puede dejar de ser fiable y la entidad certificadora (a petición del titular o aún sin el consentimiento de éste, según las circunstancias), puede suspender (interrumpir temporalmente el período de validez) o revocar (invalidar de forma permanente) el certificado. Inmediatamente después de suspender o revocar un certificado, la entidad debe, por lo general, hacer pública la revocación o suspensión o notificar este hecho a las personas que soliciten información o de que se tenga conocimiento de que han recibido una firma numérica verificable por remisión al certificado que carezca de fiabilidad.

58. Las entidades certificadoras podrán ser entidades públicas o privadas. En algunos países, por razones de orden público, se prevé que sólo las entidades públicas estén autorizadas para actuar como entidades certificadoras. En otros países, se considera que los servicios de certificación deben quedar abiertos a la competencia del sector privado. Independientemente de que las entidades certificadoras sean públicas o privadas y de que deban obtener una autorización, normalmente existe más de una entidad certificadora en la ICP. Plantea especial inquietud la relación entre las diversas entidades certificadoras. Las entidades certificadoras de una ICP pueden establecerse en una estructura jerárquica, en la que algunas de ellas sólo certifican a otras entidades certificadoras, que son las que prestan los servicios directamente a los usuarios. En dicha estructura, las entidades certificadoras están subordinadas a otras entidades certificadoras. En otras posibles estructuras, algunas entidades certificadoras pueden actuar en plano de igualdad con otras entidades certificadoras. En una ICP de gran envergadura, probablemente habría tanto entidades certificadoras subordinadas como superiores. En cualquier caso, si no existe una ICP internacional, pueden surgir una serie de problemas con respecto al reconocimiento de certificados por parte de entidades certificadoras de países extranjeros. El reconocimiento de certificados extranjeros se realiza generalmente mediante un método denominado "certificación cruzada". En tales casos es necesario que entidades certificadoras sustancialmente equivalentes (o entidades certificadoras dispuestas a asumir ciertos riesgos con respecto a los certificados emitidos por otras entidades certificadoras) reconozcan mutuamente los servicios prestados, de forma que los respectivos usuarios puedan comunicarse entre ellos de manera más eficaz y con mayor confianza en la fiabilidad de los certificados que se emitan.

59. Con respecto a la certificación cruzada o a las cadenas de certificados, cuando entran en juego diversas políticas de seguridad se pueden plantear problemas jurídicos, por ejemplo, respecto de la identificación del autor del error que causó una pérdida y de la fuente en que se basó el usuario. Cabe señalar que las normas jurídicas cuya aprobación se está considerando en ciertos países disponen que, cuando los niveles de seguridad y las políticas se pongan en conocimiento de los usuarios y no haya negligencia por parte de las entidades certificadoras, no habrá responsabilidad.

60. Puede que corresponda a la entidad certificadora, o a la entidad principal asegurar que los requisitos de sus políticas se cumplen de forma permanente. Si bien la selección de las entidades certificadoras puede basarse en diversos factores, incluida la solidez de la clave pública utilizada y la identidad del usuario, el grado de fiabilidad de la entidad certificadora puede depender también de la forma en que aplique las normas para emitir certificados y de la fiabilidad de la evaluación que realice de los datos que reciba de los usuarios que solicitan certificados. Es de especial importancia el régimen de responsabilidad que se aplique a la entidad certificadora con respecto al cumplimiento, en todo momento, de la política y los requisitos de seguridad de la entidad principal o de la entidad certificadora superior, o de cualquier otro requisito aplicable.

61. Al preparar la Ley Modelo, se examinaron los siguientes elementos como posibles factores a tener en cuenta para determinar el grado de fiabilidad de una entidad certificadora: 1) independencia (es decir, ausencia de un interés financiero o de otro tipo en las transacciones subyacentes); 2) recursos y capacidad financieros para asumir la responsabilidad por el riesgo de pérdida; 3) experiencia en tecnologías de clave pública y familiaridad con procedimientos de seguridad apropiados; 4) longevidad (las entidades certificadoras pueden tener que presentar pruebas de certificaciones o claves de codificación muchos años después de que se hayan concluido las operaciones subyacentes, por ejemplo con motivo de un juicio o de una reivindicación); 5) aprobación del equipo y los programas informáticos; 6) mantenimiento de un registro de auditoría y realización de auditorías por una entidad independiente; 7) existencia de un plan para casos de emergencia (por ejemplo, “programas de recuperación en casos de desastre” o depósitos de claves); 8) selección y gestión del personal; 9) disposiciones para proteger su propia clave privada; 10) seguridad interna; 11) disposiciones para suspender las operaciones, incluida la notificación a los usuarios; 12) garantías y representaciones (otorgadas o excluidas); 13) limitación de la responsabilidad; 14) seguros; 15) capacidad para intercambiar datos con otras entidades certificadoras; y 16) procedimientos de revocación (en caso de que la clave criptográfica se haya perdido o haya quedado en entredicho).

c) Sinopsis del proceso de la firma numérica

62. El empleo de las firmas numéricas abarca por lo general los siguientes procesos, realizados por el firmante o por el receptor del mensaje firmado en forma numérica:

1) El usuario genera o recibe un par de claves criptográficas único;

2) El remitente prepara el mensaje (por ejemplo, en forma de mensaje de correo electrónico) en una computadora;

3) El remitente prepara un “compendio del mensaje”, utilizando un algoritmo de control seguro. En la creación de la firma numérica se utiliza un resultado control derivado del mensaje firmado y de una clave privada determinada, que es exclusivo de éstos. Para que el resultado control sea seguro, debe haber sólo una posibilidad mínima de que la misma firma numérica se pueda crear mediante la combinación de cualquier otro mensaje o clave privada;

4) El remitente codifica el compendio del mensaje utilizando la clave privada. La clave privada se aplica al texto del compendio del mensaje utilizando un algoritmo matemático. La firma numérica es el compendio del mensaje codificado;

5) El remitente normalmente adjunta o acompaña su firma numérica al mensaje;

6) El remitente envía la firma numérica y el mensaje (codificado o no) al receptor en forma electrónica;

7) El receptor utiliza la clave pública del remitente para verificar la firma numérica de éste. Esta verificación con la clave pública del remitente prueba que el mensaje proviene exclusivamente del remitente;

8) El receptor también crea un "compendio del mensaje" utilizando el mismo algoritmo de control seguro;

9) El receptor compara los dos compendios de mensajes. Si son iguales, el receptor sabe que el mensaje no ha sido modificado después de la firma. Aun cuando sólo se haya modificado una parte ínfima del mensaje después de que haya sido firmado en forma numérica, el compendio del mensaje creado por el receptor será diferente al compendio del mensaje creado por el remitente;

10) El receptor obtiene un certificado de la entidad certificadora (o por conducto del iniciador del mensaje), que confirma la firma numérica del remitente del mensaje. La entidad certificadora es, por lo general, un tercero de confianza que administra la certificación en el sistema de firmas numéricas. El certificado contiene la clave pública y el nombre del remitente (y posiblemente otra información), y lleva la firma numérica de la entidad certificadora.

IV. Principales características de la Ley Modelo

A. Naturaleza legislativa de la Ley Modelo

63. La nueva Ley Modelo fue preparada partiendo del supuesto de que debería derivarse directamente del artículo 7 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico y considerarse como una forma de proporcionar información detallada sobre el concepto del "método fiable para identificar" a una persona y "para indicar que esa persona aprueba" la información que figura en el mensaje de datos (véase A/CN.9/WG.IV/WP.71, párr. 49).

64. Se planteó la cuestión de la forma que debería adoptar el instrumento y se señaló la importancia de tener en cuenta la relación de la forma con el contenido. Se sugirieron diferentes criterios con respecto a la forma que debería adoptar, como los de régimen contractual, disposiciones legislativas, o directrices para que los Estados estudiasen la promulgación de legislación sobre las firmas electrónicas. Se adoptó como hipótesis de trabajo que las disposiciones que se prepararan serían normas jurídicas con un comentario, y no meras directrices (véase A/CN.9/437, párr. 27; A/CN.9/446, párr. 25; y A/CN.9/457, párrs. 51 y 72). El texto se adoptó finalmente en forma de ley modelo (A/CN.9/483, párrs. 137 y 138).

B. Relación con la Ley Modelo de la CNUDMI sobre Comercio Electrónico

1. La Ley Modelo como instrumento jurídico independiente

65. Las nuevas disposiciones podrían haberse integrado en una versión ampliada de la Ley Modelo de la CNUDMI sobre Comercio Electrónico, por ejemplo como una nueva tercera parte de esta última. Con el fin de señalar claramente que cabría promulgar la Ley Modelo tanto en forma de norma independiente como en forma de texto adicional a la Ley Modelo de la CNUDMI sobre Comercio Electrónico, se decidió finalmente que la nueva Ley Modelo adquiriese la forma de un instrumento jurídico independiente (véase A/CN.9/465, párr. 37). Esta decisión se deriva principalmente del hecho de que, cuando se estaba concluyendo la Ley Modelo, la Ley Modelo de la CNUDMI sobre Comercio Electrónico ya se había aplicado de manera satisfactoria en una serie de países y otros estaban estudiando su aprobación. La preparación de una versión ampliada de la Ley Modelo de la CNUDMI sobre Comercio Electrónico podría haber puesto en peligro el éxito de la versión original al sugerir que era necesario mejorar ese texto mediante una actualización. Además, la preparación de una nueva versión de la Ley Modelo de la CNUDMI sobre Comercio Electrónico podría haber dado lugar a confusiones en los países que la habían aprobado recientemente.

2. Plena coherencia entre la Ley Modelo y la Ley Modelo de la CNUDMI sobre Comercio Electrónico

66. Al redactar la nueva Ley Modelo, se hizo todo lo posible por asegurar su coherencia con el contenido y la terminología de la Ley Modelo de la CNUDMI sobre Comercio Electrónico (A/CN.9/465, párr. 37). En el nuevo instrumento se han reproducido las disposiciones generales de la Ley Modelo de la CNUDMI sobre Comercio Electrónico, es decir los artículos 1 (Ámbito de aplicación), 2 a), c) y e) (Definiciones de “mensaje de datos”, “iniciador” y “destinatario”), 3 (Interpretación), 4 (Modificación mediante acuerdo) y 7 (Firma) de la Ley Modelo de la CNUDMI sobre Comercio Electrónico.

67. Al basarse en la Ley Modelo de la CNUDMI sobre Comercio Electrónico, la nueva Ley Modelo 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 de la voluntad contractual de las partes (A/CN.9/WG.IV/WP.84, párr. 16). 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 disposiciones contractuales modelo o 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).

3. Relación con el artículo 7 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico

68. Al preparar la nueva Ley Modelo, se expresó la opinión de que la referencia al artículo 7 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico en el texto del artículo 6 de la nueva Ley Modelo debía interpretarse en el sentido de que limitaba el alcance de ésta a los supuestos en que se utilizara una firma electrónica para cumplir con el requisito legal imperativo de que ciertos documentos han de ser firmados para ser *válidos*. Según ese criterio, dado que la ley de la mayoría de las naciones imponía muy pocos requisitos de esta índole con respecto a los documentos utilizados en operaciones comerciales, el alcance de la nueva Ley Modelo sería muy limitado. En respuesta a este argumento, se convino en general en que esa interpretación del artículo 6 (y del artículo 7 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico) era incompatible 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 de la CNUDMI sobre Comercio Electrónico al derecho interno, conforme a 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". De hecho, el ámbito tanto del artículo 7 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico como del artículo 6 de la Ley Modelo es particularmente amplio, ya que la mayoría de los documentos utilizados en el contexto de operaciones comerciales probablemente tendrá que ajustarse, en la práctica, a los requisitos legales impuestos para la prueba por escrito (A/CN.9/465, párr. 67).

C. Régimen "marco" que se complementará con reglamentaciones técnicas y contratos

69. Como complemento a la Ley Modelo de la CNUDMI sobre Comercio Electrónico, la finalidad de la nueva Ley Modelo es ofrecer principios fundamentales que faciliten el empleo de las firmas electrónicas. Sin embargo, en tanto que "marco", la Ley Modelo no establece en sí misma todas las normas y reglamentaciones que puedan ser necesarias (además de las disposiciones contractuales existentes entre los usuarios) para aplicar dichas técnicas en un Estado promulgante. Además, como se señala en la presente Guía, la finalidad de la Ley Modelo no es abarcar todos los aspectos del empleo de firmas electrónicas. Por ello, los Estados promulgantes tal vez deseen emitir reglamentaciones que cubran los detalles procedimentales relativos a los procedimientos autorizados por la Ley Modelo y tengan en cuenta circunstancias específicas, posiblemente cambiantes, existentes en el Estado promulgante, sin poner en entredicho los objetivos de la Ley Modelo. Se recomienda que, en caso de que se decida promulgar dicha reglamentación, los Estados promulgantes presten especial atención a la necesidad de mantener la flexibilidad del funcionamiento de los sistemas de creación de firmas electrónicas por parte de los usuarios de éstas.

70. Cabe señalar que las técnicas de creación de firmas electrónicas que se recogen en la Ley Modelo, además de plantear cuestiones de procedimiento que tal vez sea necesario abordar al aplicar reglamentaciones técnicas, pueden plantear ciertas cuestiones jurídicas cuya respuesta no vendrá dada necesariamente en la Ley Modelo, sino en otros instrumentos jurídicos. Estos instrumentos jurídicos pueden

ser, por ejemplo, la legislación administrativa, contractual, penal y procesal aplicable, a la que no se hace referencia en la Ley Modelo.

D. Mayor seguridad de las consecuencias jurídicas de las firmas electrónicas

71. Una de las características principales de la nueva Ley Modelo es la de aumentar la seguridad del funcionamiento de los criterios de flexibilidad que se establecen en el artículo 7 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico para el reconocimiento de una firma electrónica como equivalente funcional a una firma manuscrita. El artículo 7 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico dice 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 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 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 en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que no exista una firma.
>
> 3) Lo dispuesto en el presente artículo no será aplicable a: [...]."

72. El artículo 7 se basa en el reconocimiento de las funciones que se atribuyen a una firma en las comunicaciones consignadas sobre papel. En la preparación de la Ley Modelo de la CNUDMI sobre Comercio Electrónico se tomaron en consideración las siguientes funciones de la firma: identificar a una persona; dar certeza a la participación personal de esa persona en el acto de firmar; y asociar a esa persona con el contenido de un documento. Se observó que una firma podía desempeñar además diversas otras funciones, según la naturaleza del documento firmado. Por ejemplo, podía demostrar la intención de una parte contractual de obligarse por el contenido del contrato firmado; la intención de una persona de reivindicar la autoría de un texto; la intención de una persona de asociarse con el contenido de un documento escrito por otra; y el hecho de que esa persona hubiera estado en un lugar determinado, en un momento dado.

73. Para evitar que se niegue validez jurídica a un mensaje que deba autenticarse por el mero hecho de que no esté autenticado en la forma característica de los documentos consignados sobre papel, el artículo 7 adopta un criterio general. El artículo define las condiciones generales que, de cumplirse, autenticarían un mensaje de datos con suficiente credibilidad para satisfacer los requisitos de firma que actualmente obstaculizan el comercio electrónico. El artículo 7 se centra en las dos funciones básicas de la firma: la identificación del autor y la confirmación de que el autor aprueba el contenido del documento. En el apartado a) del párrafo 1) se enuncia el principio de que, en las comunicaciones electrónicas, esas dos funciones jurídicas básicas de la firma se cumplen al utilizarse un método que identifique al

iniciador de un mensaje de datos y confirme que el iniciador aprueba la información en él consignada.

74. El apartado b) del párrafo 1) establece un criterio flexible respecto del grado de seguridad que se ha de alcanzar con la utilización del método de identificación mencionado en el apartado a). El método seleccionado conforme al apartado a) del párrafo 1) deberá ser tan fiable como sea apropiado para los fines para los que se consignó o comunicó el mensaje de datos, a la luz de las circunstancias del caso, así como del acuerdo entre el iniciador y el destinatario del mensaje.

75. Para determinar si el método seleccionado con arreglo al párrafo 1) es apropiado, pueden tenerse en cuenta, entre otros, los siguientes factores jurídicos, técnicos y comerciales: 1) la perfección técnica del equipo utilizado por cada una de las partes; 2) la naturaleza de su actividad comercial; 3) la frecuencia de sus relaciones comerciales; 4) el tipo y la magnitud de la operación; 5) la función de los requisitos de firma con arreglo a la norma legal o reglamentaria aplicable; 6) la capacidad de los sistemas de comunicación; 7) la observancia de los procedimientos de autenticación establecidos por intermediarios; 8) la gama de procedimientos de autenticación que ofrecen los intermediarios; 9) la observancia de los usos y prácticas comerciales; 10) la existencia de mecanismos de aseguramiento contra el riesgo de mensajes no autorizados; 11) la importancia y el valor de la información contenida en el mensaje de datos; 12) la disponibilidad de otros métodos de identificación y el costo de su aplicación; 13) el grado de aceptación o no aceptación del método de identificación en el sector o la esfera pertinente, tanto en el momento en el que se acordó el método como en el que se comunicó el mensaje de datos; y 14) cualquier otro factor pertinente (Guía para la incorporación al derecho interno de la Ley Modelo de la CNUDMI sobre Comercio Electrónico, párrs. 53 y 56 a 58).

76. Partiendo de los flexibles criterios que figuran en el apartado b) del párrafo 1) del artículo 7 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico, los artículos 6 y 7 de la nueva Ley Modelo establecen un mecanismo mediante el cual las firmas electrónicas que reúnan criterios objetivos de fiabilidad técnica puedan beneficiarse de una pronta determinación de su eficacia jurídica. El efecto de la Ley Modelo es reconocer dos categorías de firmas electrónicas. La primera y más amplia de las categorías es la que se describe en el artículo 7 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico. Se trata de cualquier “método” que pueda emplearse para cumplir el requisito jurídico de una firma manuscrita. La eficacia jurídica de dicho “método” como equivalente a una firma manuscrita depende de la demostración de su “fiabilidad” con respecto a alguien que constate los hechos. La segunda y más limitada de las categorías es la que se crea en la Ley Modelo. Consiste en métodos de firma electrónica que pueden ser reconocidos por una entidad pública, una entidad privada acreditada o por las mismas partes, conforme a los criterios de fiabilidad técnica establecidos en la Ley Modelo. La ventaja de este reconocimiento es que aporta seguridad a los usuarios de dichas técnicas de creación de firmas electrónicas (a veces denominada firmas electrónicas “refrendadas”, “garantizadas” o “calificadas”) antes de que empleen realmente la técnica de creación de la firma electrónica.

E. Normas de conducta básicas para las partes interesadas

77. La Ley Modelo no aborda en detalle las cuestiones de la responsabilidad que pueda corresponder a cada una de las partes interesadas en el funcionamiento de los sistemas de creación de firmas electrónicas. Esas cuestiones quedan al margen de la Ley Modelo y se dejan al derecho aplicable. No obstante, en la Ley Modelo se fijan criterios para evaluar la conducta de las partes, a saber, el firmante, el tercero que confía en el certificado y el prestador de servicios de certificación.

78. En cuanto al firmante, la Ley Modelo desarrolla el principio básico de que debe actuar con diligencia razonable con respecto a su dispositivo de creación de firma electrónica. Se espera que el firmante actúe con diligencia razonable para evitar la utilización no autorizada de ese dispositivo de creación de la firma. Cuando el firmante sepa o deba saber que el dispositivo de creación de la firma ha dejado de ser seguro deberá dar aviso sin dilación indebida a cualquier persona que, según pueda razonablemente prever, haya de considerar fiable la firma electrónica o prestar servicios que la refrenden. Cuando se emplee un certificado para refrendar la firma electrónica, se espera que el firmante actúe con diligencia razonable para cerciorarse de que todas las declaraciones que haya hecho sean exactas y cabales.

79. Se espera que el tercero que confía en el certificado tome medidas razonables para verificar la fiabilidad de la firma electrónica. Cuando la firma electrónica esté refrendada por un certificado, el tercero que confía en el certificado deberá tomar medidas razonables para verificar la validez, suspensión o revocación del certificado, y tener en cuenta cualquier limitación que lo afecte.

80. La obligación general del prestador de servicios de certificación es utilizar, al prestar sus servicios, sistemas, procedimientos y recursos humanos fiables y actuar de conformidad con las declaraciones que haga respecto de sus normas y prácticas. Además, se espera que actúe con diligencia razonable para cerciorarse de que todas las declaraciones materiales que haya hecho en relación con el certificado sean exactas y cabales. En el certificado, el prestador deberá proporcionar información fundamental que permita al tercero que haya de confiar en el certificado determinar la identidad del prestador de servicios de certificación. También deberá permitir determinar: 1) que la persona nombrada en el certificado tenía bajo su control el dispositivo de creación de la firma al momento de ésta; y 2) que el dispositivo era válido en la fecha en que se emitió el certificado o antes de ella. Con respecto al tercero que ha de confiar, el prestador de servicios de certificación deberá aportar también información relativa a: 1) el método utilizado para identificar al firmante; 2) cualquier limitación en los fines o el valor respecto de los cuales pueda utilizarse el dispositivo de creación de la firma o el certificado; 3) las condiciones de funcionamiento del dispositivo de creación de la firma; 4) cualquier limitación en cuanto al ámbito o el alcance de la responsabilidad del prestador de los servicios de certificación; 5) si existe un medio para que el firmante dé aviso de que un dispositivo de creación de firma ha quedado en entredicho; y 6) si se ofrece un servicio de revocación oportuna del certificado.

81. En la Ley Modelo figura una lista abierta de factores indicativos para determinar la fiabilidad de los sistemas, procedimientos y recursos humanos utilizados por el prestador de servicios de certificación.

F. Marco de neutralidad respecto de los medios técnicos utilizables

82. Ante la evolución de las innovaciones tecnológicas, la Ley Modelo establece el reconocimiento jurídico de las firmas electrónicas independientemente de la tecnología utilizada (a saber, firmas electrónicas basadas en la criptografía asimétrica; la biometría; la utilización de números de identificación personal (NIP); versiones digitalizadas de firmas manuscritas; y otros métodos, como la selección de un signo afirmativo en la pantalla electrónica mediante el ratón).

V. Asistencia de la Secretaría de la CNUDMI

A. Asistencia para la redacción de legislación

83. En el marco de sus actividades de formación y asistencia, la Secretaría de la CNUDMI presta asistencia a los Estados mediante consultas técnicas para la preparación de legislación basada en la Ley Modelo de la CNUDMI para las Firmas Electrónicas. Esta misma asistencia se prestará a los gobiernos que estudien la promulgación de legislación basada en otras leyes modelo de la CNUDMI (es decir la Ley Modelo de la CNUDMI sobre Arbitraje Comercial Internacional, la Ley Modelo de la CNUDMI sobre Transferencias Internacionales de Crédito, la Ley Modelo de la CNUDMI sobre la Contratación Pública de Bienes, Obras y Servicios, la Ley Modelo de la CNUDMI sobre Comercio Electrónico y la Ley Modelo de la CNUDMI sobre la Insolvencia Transfronteriza) o la adhesión a uno de los convenios y convenciones de derecho mercantil internacional preparados por la CNUDMI.

84. Puede pedirse a la Secretaría, cuya dirección se indica a continuación, más información acerca de la Ley Modelo, así como sobre otras leyes modelo y convenios y convenciones preparados por la CNUDMI:

Subdivisión de Derecho Mercantil Internacional, Oficina de Asuntos Jurídicos
Naciones Unidas
Centro Internacional de Viena
Apartado postal 500
A-1400, Viena, Austria

Teléfono:	(+43-1) 26060-4060 ó 4061
Fax:	(+43-1) 26060-5813
Correo electrónico:	uncitral@uncitral.org
Dirección de Internet:	http://www.uncitral.org

B. Información relativa a la interpretación de la legislación basada en la Ley Modelo

85. La Secretaría agradecerá cualquier observación relativa a la Ley Modelo y a la Guía, así como que se le informe sobre la promulgación de legislación basada en la Ley Modelo. Una vez promulgada, la Ley Modelo se incluirá en el sistema de información acerca de jurisprudencia de los tribunales sobre textos de la CNUDMI (CLOUT), que se emplea para recopilar y difundir información sobre jurisprudencia

relativa a los convenios, convenciones y leyes modelo emanados de la labor de la CNUDMI. El objetivo del sistema es promover la difusión internacional de los textos legislativos elaborados por la CNUDMI y facilitar la interpretación y aplicación uniformes de éstos. La Secretaría publica, en los seis idiomas oficiales de las Naciones Unidas, resúmenes de las decisiones, y facilita las decisiones que sirvieron de base para la preparación de dichos resúmenes a contrarreembolso de los gastos de reproducción. El sistema se explica en una guía del usuario que puede obtenerse de la Secretaría en soporte de papel (A/CN.9/SER.C/GUIDE/1) y en la página de Internet de la CNUDMI antes mencionada.

Capítulo II. Observaciones artículo por artículo

Título

"*Ley Modelo*"

86. A lo largo de su preparación, el instrumento se ha concebido como un suplemento de la Ley Modelo de la CNUDMI sobre Comercio Electrónico y debería tratarse en pie de igualdad con el instrumento que lo precedió y compartir con él la misma naturaleza jurídica.

Artículo 1. Ámbito de aplicación

La presente ley será aplicable en todos los casos en 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 de la presente Ley:

"La presente Ley será aplicable en todos los casos en que se utilicen firmas electrónicas, excepto en las situaciones siguientes: [...]."

** El término "comercial" deberá ser interpretado en forma lata de manera que abarque las cuestiones que dimanen de toda relación de índole comercial, sea o no contractual. Las relaciones de índole comercial comprenden, sin que esta lista sea taxativa, las operaciones siguientes: toda operación comercial de suministro o intercambio de bienes o servicios; acuerdos de distribución; representación o mandato comercial; facturaje ("factoring"); arrendamiento con opción de compra ("leasing"); construcción de obras; consultoría; ingeniería; concesión de licencias; inversiones; financiación; banca; seguros; acuerdos o concesiones de explotación; empresas conjuntas y otras formas de cooperación industrial o comercial; transporte de mercancías o de pasajeros por vía aérea, marítima y férrea, o por carretera.

Observaciones generales

87. La finalidad del artículo 1 es delimitar el ámbito de aplicación de la Ley Modelo. En la Ley Modelo se ha tratado en principio de abarcar todas las situaciones de hecho en que se utilizan firmas electrónicas, independientemente del tipo de firma electrónica o de técnica de autenticación que se aplique. Durante la preparación de la Ley Modelo se estimó que si se excluía alguna forma o algún medio merced a una limitación del ámbito de aplicación de la Ley Modelo podían surgir dificultades prácticas que irían en contra de la finalidad de ofrecer unas

disposiciones neutrales con respecto a los medios. Sin embargo, en la preparación de la Ley Modelo se ha prestado especial atención a las “firmas numéricas”, es decir, a las firmas electrónicas obtenidas mediante la aplicación de una criptografía de doble clave, que, en opinión del Grupo de Trabajo de la CNUDMI sobre Comercio Electrónico, era una tecnología considerablemente difundida. La Ley Modelo se centra en la utilización de tecnología moderna y, salvo cuando dispone expresamente otra cosa, no pretende alterar el régimen tradicional aplicable a las firmas manuscritas.

*Nota de pie de página ***

88. Se consideró que en la Ley Modelo debía indicarse que se centraba en los tipos de situaciones que se daban en el ámbito comercial y que se había preparado en función del contexto de las relaciones comerciales y financieras. Por esta razón, el artículo 1 hace referencia a las “actividades comerciales” y en la nota de pie de página ** se especifica lo que se entiende por tales actividades. Esas indicaciones, que pueden ser particularmente útiles para los países que no disponen de un cuerpo de normas diferenciadas de derecho mercantil, se han calcado, por razones de coherencia, de la nota referente al artículo 1 de la Ley Modelo de la CNUDMI sobre Arbitraje Comercial Internacional (también reproducida como nota de pie de página **** referente al artículo 1 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico). En ciertos países, la utilización de notas de pie de página en textos legales no se consideraría una práctica legislativa aceptable. Sería pues conveniente que las autoridades nacionales que incorporaran la Ley Modelo al derecho interno se plantearan la posible inclusión del texto de las notas de pie de página en el texto propiamente dicho.

*Nota de pie de página **

89. La Ley Modelo es aplicable a todos los tipos de mensajes de datos a los que se adjunta una firma electrónica con valor jurídico, y nada de lo dispuesto en la Ley Modelo debería impedir al Estado ampliar el alcance de la Ley Modelo para abarcar también la utilización de las firmas electrónicas fuera del ámbito comercial. Por ejemplo, si bien la Ley Modelo no se centra en las relaciones entre usuarios de firmas electrónicas y autoridades públicas, sus disposiciones no se han concebido con la finalidad de que no sean aplicables a tales relaciones. La nota de pie de página * prevé otros posibles enunciados a los que puedan recurrir los Estados que consideren apropiado ampliar el ámbito de aplicación de la Ley Modelo más allá del ámbito comercial.

Protección del consumidor

90. Algunos países tienen leyes especiales de protección del consumidor que pueden regular ciertos aspectos de la utilización de sistemas de información. Con respecto a esa legislación de protección del consumidor, al igual que en la elaboración de anteriores instrumentos de la CNUDMI (por ejemplo, la Ley Modelo de la CNUDMI sobre Transferencias Internacionales de Crédito y la Ley Modelo de la CNUDMI sobre Comercio Electrónico), se consideró que debía indicarse que la

Ley Modelo se había redactado sin prestar especial atención a las cuestiones que podrían plantearse en el contexto de la protección del consumidor. Al mismo tiempo, se estimó que no había motivo para que las situaciones que afectaban a los consumidores fueran excluidas del ámbito de aplicación de la Ley Modelo mediante una disposición general, particularmente porque las disposiciones de la Ley Modelo podían juzgarse muy beneficiosas para la protección del consumidor, según el tipo de legislación de cada Estado. Así pues, el artículo 1 reconoce que la legislación de protección del consumidor puede estar por encima de las disposiciones de la Ley Modelo. En caso de que los legisladores llegaran a conclusiones distintas sobre el eventual efecto beneficioso que podía tener la Ley Modelo en las transacciones del consumidor en un determinado país, podían plantear la posibilidad de excluir a los consumidores del ámbito de aplicación del instrumento legislativo mediante el cual se incorporara la Ley Modelo al derecho interno. La determinación de las personas físicas y jurídicas que deban considerarse "consumidores" se deja en manos del derecho aplicable al margen de la Ley Modelo.

La utilización de firmas electrónicas en operaciones internacionales y nacionales

91. Se recomienda que se dé al Régimen Uniforme la aplicación más amplia posible. Debe actuarse con suma prudencia al excluir la aplicación de la Ley Modelo limitando su alcance a los usos internacionales de firmas electrónicas, ya que puede considerarse que tal limitación impide cumplir plenamente los objetivos de la Ley Modelo. Además, la diversidad de procedimientos que ofrece la Ley Modelo para limitar la utilización de firmas electrónicas en caso necesario (por ejemplo, por razones de orden público) puede hacer menos necesario limitar el alcance de la Ley Modelo. La certeza jurídica que debe aportar la Ley Modelo es necesaria para el comercio tanto nacional como internacional, y la superposición de dos regímenes que regularan la utilización de las firmas electrónicas podría suponer un grave obstáculo para la aplicación de esas técnicas.

Referencias a documentos de la CNUDMI

A/CN.9/467, párrs. 22 a 24;

A/CN.9/WG.IV/WP.84, párr. 22;

A/CN.9/465, párrs. 36 a 42;

A/CN.9/WG.IV/WP.82, párr. 21;

A/CN.9/457, párrs. 53 a 64.

Artículo 2. Definiciones

Para los fines de la presente Ley:

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 que puedan ser utilizados para identificar al firmante 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 “certificado” se entenderá todo mensaje de datos u otro registro que confirme el vínculo entre un firmante y los datos de creación de la firma;

c) Por “mensaje de datos” se entenderá la información generada, enviada, recibida o archivada 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;

d) Por “firmante” se entenderá la persona que posee los datos de creación de la firma y que actúa en nombre propio o de la persona a la que representa;

e) Por “prestador de servicios de certificación” se entenderá la persona que expide certificados y puede prestar otros servicios relacionados con las firmas electrónicas;

f) Por “parte que confía” se entenderá la persona que pueda actuar sobre la base de un certificado o de una firma electrónica.

Definición de “firma electrónica”

La firma electrónica como equivalente funcional de la firma manuscrita

92. La noción de “firma electrónica” aspira a abarcar todos los usos tradicionales de una firma manuscrita con consecuencias jurídicas, siendo la identificación del firmante y la intención de firmar sólo el mínimo común denominador de los diversos criterios relativos a la “firma” que se hallan en los diversos ordenamientos jurídicos. Esas funciones de la firma manuscrita ya se examinaron en el contexto de la preparación del artículo 7 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico. En consecuencia, definir una firma electrónica como capaz de indicar la aprobación de la información equivale primordialmente a establecer un requisito técnico previo para el reconocimiento de una determinada tecnología apta para crear el equivalente de una firma manuscrita. La definición no deja de lado el hecho de que las tecnologías comúnmente denominadas “firmas electrónicas” podrían utilizarse para otros fines que crear una firma jurídicamente pertinente. La definición se limita a ilustrar que la Ley Modelo se centra en el uso de firmas electrónicas como equivalentes funcionales de las manuscritas (véase el documento (A/CN.9/483, párr. 62).

Otros usos posibles de la firma electrónica

93. Debe trazarse una distinción entre la noción jurídica de “firma” y la noción técnica de “firma electrónica”, término especializado que comprende algunas prácticas que no intervienen necesariamente en la producción de firmas jurídicamente pertinentes. En la preparación de la Ley Modelo, se estimó que había que señalar a la atención de los usuarios el riesgo de confusión que podría resultar del uso del mismo instrumento técnico para la producción de una firma

jurídicamente pertinente y para otras funciones de autenticación o identificación (ibíd.).

Definición de "certificado"

Necesidad de una definición

94. La palabra "certificado" utilizada en el contexto de ciertos tipos de firma electrónica y definida en la Ley Modelo poco difiere de su significado general de documento mediante el cual una persona confirma ciertos hechos. No obstante, dado que en todos los ordenamientos jurídicos existe la noción general de "certificado", ni siquiera en todos los idiomas, se juzgó útil incluir una definición en el contexto de la Ley Modelo (ibíd., párr. 65).

Finalidad del certificado

95. La finalidad del certificado es reconocer, mostrar o confirmar un vínculo entre los datos de creación de la firma y el firmante. Ese vínculo nace cuando se generan los datos de creación de la firma (ibíd., párr. 67).

"*Datos de creación de la firma*"

96. La expresión "datos de creación de la firma" tiene por fin designar las claves secretas, los códigos u otros elementos que, en el proceso de crear una firma electrónica, se utilizan para obtener un vínculo seguro entre la firma electrónica resultante y la persona del firmante. Por ejemplo, en el contexto de las firmas numéricas fundadas en una criptografía asimétrica, el elemento nuclear operativo que podría describirse como "vinculado exclusivamente al firmante" es el par de claves criptográficas. En el contexto de las firmas electrónicas basadas en dispositivos biométricos, el elemento decisivo sería el indicador biométrico, como una huella dactilar o los datos de barrido de la retina. La definición abarca únicamente los elementos nucleares que deben mantenerse bajo reserva para garantizar la calidad del proceso de firma, con exclusión de todo otro elemento que, aunque pueda contribuir al proceso de firma, cupiera divulgar sin poner en peligro la fiabilidad de la firma electrónica resultante. Por ejemplo, en el caso de las firmas numéricas, si bien tanto la clave pública como la privada están vinculadas a la persona del firmante, sólo la clave privada tiene que entrar en la definición, ya que únicamente la clave privada debe mantenerse bajo reserva y es de la esencia de la clave pública que pueda hacerse accesible al público (A/CN.9/483, párr. 71). Entre los elementos que no ha de abarcar la definición, el texto firmado electrónicamente, aunque desempeña también un importante papel en el proceso de creación de la firma (mediante una función control o de otra manera) no debe evidentemente quedar sujeto a la misma confidencialidad que la información que identifica al firmante (ibíd., párrs. 72 y 76). El artículo 6 expresa la idea de que los datos de creación de la firma deben estar vinculados al firmante y a ninguna otra persona (ibíd., párr. 75).

Definición de "mensaje de datos"

97. La definición de "mensaje de datos" está tomada del artículo 2 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico como noción amplia que comprende todos los mensajes generados en el contexto del comercio electrónico, incluido el basado en la red (ibíd., párr. 69). La noción de "mensaje de datos" no se limita a la comunicación sino que pretende abarcar asimismo los registros generados informáticamente no destinados a la comunicación. Por lo tanto, la noción de "mensaje" comprende la de "registro".

98. La referencia a "medios similares" tiene por objeto reflejar el hecho de que la Ley Modelo no fue pensada únicamente para su aplicación en el contexto de las técnicas de comunicación existentes sino también para dar cabida a las novedades técnicas previsibles. El fin de la definición de "mensaje de datos" es comprender todos los tipos de mensajes generados, almacenados o comunicados básicamente sin papel. Con esta finalidad, se quiere que todos los medios de comunicación y almacenamiento de información que quepa utilizar para desempeñar funciones paralelas a las realizadas con los medios enumerados en la definición queden cubiertos mediante la referencia a "medios similares", si bien, por ejemplo, los medios de comunicación "electrónicos" y "ópticos" puedan no ser, en sentido estricto, similares. Para los fines de la Ley Modelo, la palabra "similares" connota "funcionalmente equivalentes".

99. La definición de "mensaje de datos" tiene además por fin su aplicación en el caso de revocación o modificación. Se presume que un mensaje de datos tiene un contenido fijo de información que puede, empero, ser revocado o modificado por otro mensaje de datos (Guía para la incorporación al derecho interno de la Ley Modelo de la CNUDMI sobre Comercio Electrónico, párrs. 30 a 32).

Definición de "firmante"

"una persona"

100. De forma coherente con el criterio adoptado en la Ley Modelo de la CNUDMI sobre Comercio Electrónico toda referencia en la nueva Ley Modelo a una "persona" debe entenderse que abarca todos los tipos de personas o entidades, físicas, colectivas o personas jurídicas de otra índole (A/CN.9/483, párr. 86).

"en nombre de la persona a la que representa"

101. La analogía con las firmas manuscritas puede no siempre ser adecuada para aprovechar las posibilidades que ofrece la tecnología moderna. En un entorno basado en el papel, por ejemplo, las personas jurídicas no pueden ser estrictamente hablando firmantes de los documentos redactados en su nombre, porque sólo las personas físicas pueden producir firmas manuscritas auténticas. Pero cabe concebir que las firmas electrónicas sean atribuibles a sociedades u otras personas jurídicas (incluidas las autoridades gubernamentales y otras de carácter público), y pueden darse situaciones en que la identidad de la persona que genera realmente la firma, cuando se requiere un acto humano, no sea importante a los efectos para los que se creó la firma (ibíd., párr. 85).

102. Sin embargo, conforme a la Ley Modelo la noción de "firmante" no puede separarse de la persona o entidad que genera realmente la firma electrónica, dado que varias obligaciones concretas del firmante conforme a la Ley Modelo están lógicamente vinculadas con el control efectivo de los datos de creación de la firma. No obstante, para cubrir las situaciones en que el firmante actuaría en representación de otra persona, se ha conservado en la definición de "firmante" la frase "o en nombre de la persona a la que representa". La medida en que una persona pueda quedar obligada por una firma electrónica generada "en nombre propio" es asunto que debe decidirse de acuerdo con la ley que rige, según corresponda, la relación jurídica entre el firmante y la persona en cuyo nombre se genera la firma electrónica, por un aparte, y por otra, la parte que confía en ella. Esa materia, así como otras pertenecientes a la operación subyacente, incluidas cuestiones de mandato y otras relativas a quién es responsable en último término del incumplimiento por el signatario de sus obligaciones conforme al artículo 8 (si el firmante o la persona por él representada) queda fuera del ámbito de la Ley Modelo (ibíd., párrs. 86 y 87).

Definición de "prestador de servicios de certificación"

103. Como mínimo, el prestador de servicios de certificación definido para los fines de la Ley Modelo tendría que prestar servicios de certificación, posiblemente junto con otros servicios (ibíd., párr. 100).

104. No se ha establecido ninguna distinción en la Ley Modelo entre las situaciones en que un prestador de servicios de certificación se dedica a prestarlos como actividad principal o como negocio auxiliar, con carácter habitual u ocasional, directamente o mediante un subcontratista. La definición comprende todas las entidades que prestan servicios de certificación en el ámbito material de la Ley Modelo, es decir, "en el contexto de actividades comerciales". Con todo, vista esa limitación en el ámbito de aplicación de la Ley Modelo, las entidades que expidieran certificados con fines internos y no con fines comerciales no estarían comprendidas en la categoría de "prestadores de servicios de certificación" definida en el artículo 2 (ibíd., párrs. 94 a 99).

Definición de "parte que confía"

105. La definición de "parte que confía" tiene por fin asegurar la simetría en la definición de las diversas partes que intervienen en el funcionamiento de sistemas de firma electrónica conforme a la Ley Modelo (ibíd., párr. 107). Para los fines de esa definición, "actuar" debe interpretarse con amplitud de modo que abarque no sólo un acto positivo sino también una omisión (ibíd., párr. 108).

Referencias a documentos de la CNUDMI

A/CN.9/483, párrs. 59 a 109;
A/CN.9/WG.IV/WP.84, párrs. 23 a 36;
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 artículos A, B y C); y

A/CN.9/WG.IV/WP.71, párrs. 52-60.

Artículo 3. Igualdad de tratamiento de las tecnologías para la firma

Ninguna de las disposiciones de la presente Ley, con la excepción del artículo 5, será aplicada de modo que excluya, restrinja o prive de efecto jurídico cualquier método para crear una firma electrónica que cumpla los requisitos enunciados en el párrafo 1) del artículo 6 o que cumpla de otro modo los requisitos del derecho aplicable.

Neutralidad respecto de la tecnología

106. En el artículo 3 se enuncia el principio fundamental de que ningún método de firma electrónica puede ser objeto de discriminación, es decir, que debe darse a todas las tecnologías la misma oportunidad de satisfacer los requisitos del artículo 6. En consecuencia, no debe haber diferencias de tratamiento entre los mensajes firmados electrónicamente y los documentos de papel con firmas manuscritas, ni entre diversos tipos de mensajes firmados electrónicamente, siempre y cuando cumplan los requisitos básicos enunciados en el párrafo 1) del artículo 6 de la Ley Modelo o cualquier otro requisito enunciado en el derecho aplicable. Esos requisitos podrían, por ejemplo, prescribir el uso de una técnica de firma especialmente concebida en ciertas situaciones especificadas o podrían fijar una pauta superior o inferior a la establecida en el artículo 7 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico (y en el artículo 6 de la Ley Modelo). El principio fundamental de la no discriminación se ha concebido con la finalidad de tener una aplicación general. Sin embargo, cabe señalar que ese principio no tiene que afectar a la autonomía de la voluntad contractual de las partes reconocida en el artículo 5. Por consiguiente, las partes pueden seguir acordando entre ellas, siempre que lo permita la ley, la exclusión de ciertas técnicas de firma electrónica. Al disponer que la presente Ley no se aplicará "de modo que excluya, restrinja o prive de efecto jurídico cualquier método para crear una firma electrónica", el artículo 3 indica meramente que la forma en que se aplica una determinada firma electrónica no puede invocarse como única razón para denegar eficacia jurídica a esa firma. Sin embargo, no debe interpretarse erróneamente el artículo 3 considerando que establece la validez jurídica de una determinada técnica de firma o de una determinada información firmada por medios electrónicos.

Referencias a documentos de la CNUDMI

A/CN.9/467, párrs. 25 a 32;
A/CN.9/WG.IV/WP.84, párr. 37;
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.

Artículo 4. Interpretación

1) En la interpretación de la presente Ley habrán de tenerse en cuenta su origen internacional y la necesidad de promover la uniformidad en su aplicación y la observancia de la buena fe.

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

F*uente*

107. El artículo 4 se inspira en el artículo 7 de la Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías y su texto es reproducción del artículo 3 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico. El artículo tiene la finalidad de dar orientación a los tribunales arbitrales y ordinarios y a otras autoridades administrativas nacionales o locales en la interpretación de la Ley Modelo. Con el artículo 4 se pretende lograr que, una vez incorporado a la legislación de los países, el texto uniforme se interprete menos por referencia exclusiva a los conceptos de derecho nacional.

Párrafo 1)

108. La finalidad del párrafo 1) es advertir a la persona que deba aplicar la Ley Modelo de que las disposiciones de éste (o las disposiciones del instrumento por el que se dé aplicación a la Ley Modelo), aunque estén incorporadas a la legislación nacional y sean por tanto derecho nacional, deben interpretarse teniendo en cuenta su origen internacional, a fin de asegurar la uniformidad en la interpretación de la Ley Modelo en todos los países promulgantes.

Párrafo 2)

109. Entre los principios generales en que se basa la Ley Modelo, cabe hacer la siguiente relación no exhaustiva de objetivos: 1) facilitar el comercio electrónico entre los países y en los países; 2) validar las operaciones concertadas mediante nuevas tecnologías de información; 3) promover y alentar de forma neutral respecto de la tecnología la aplicación de nuevas tecnologías de información en general y de las firmas electrónicas en particular; 4) promover la uniformidad del derecho; y 5) apoyar la práctica comercial. Si bien el objetivo general de la Ley Modelo es facilitar la utilización de las firmas electrónicas, no debería interpretarse en modo alguno en el sentido de que impone su utilización.

Referencias a documentos de la CNUDMI

A/CN.9/467, párrs. 33 a 35;
A/CN.9/WG.IV/WP.84, párr. 38;
A/CN.9/465, párrs. 49 y 50;
A/CN.9/WG.IV/WP.82, párr. 35.

Artículo 5. Modificación mediante acuerdo

Las partes podrán hacer excepciones a la presente Ley o modificar sus efectos mediante acuerdo, salvo que ese acuerdo no sea válido o eficaz conforme al derecho aplicable.

Remisión al derecho aplicable

110. La decisión de emprender la preparación de la Ley Modelo se adoptó ante la evidencia de que, en la práctica, las soluciones de las dificultades jurídicas que plantea la utilización de los medios modernos de comunicación suelen buscarse en los contratos. Por consiguiente, la Ley Modelo se ha concebido con la finalidad de apoyar el principio de la autonomía de la voluntad de las partes. Sin embargo, el derecho aplicable puede limitar la aplicación de ese principio. No debe interpretarse el artículo 5 en el sentido de que permita a las partes apartarse de las reglas imperativas, como por ejemplo las reglas adoptadas por razones de orden público. Tampoco debería interpretarse el artículo 5 en el sentido de que aliente a los Estados a establecer una legislación imperativa que limite el efecto de la autonomía de la voluntad de las partes con respecto a las firmas electrónicas o que invite a los Estados a restringir esa autonomía para acordar entre ellas las soluciones de las cuestiones de los requisitos de forma que rijan sus comunicaciones.

111. El principio de la autonomía de la voluntad de las partes es ampliamente aplicable con respecto a las disposiciones de la Ley Modelo, ya que ésta no contiene ninguna disposición imperativa. Ese principio rige también en el contexto del párrafo 1) del artículo 13. En consecuencia, si bien los tribunales del Estado promulgante o las entidades encargadas de aplicar la Ley Modelo no deben negar ni anular los efectos jurídicos de un certificado extranjero únicamente en función del lugar en que se ha expedido, el párrafo 1) del artículo 13 no limita la libertad de las partes en una operación comercial para convenir la utilización de certificados procedentes de un determinado lugar (A/CN.9/483, párr. 112).

Acuerdo explícito o implícito

112. Con respecto a la forma en que se expresa el principio de la autonomía de la voluntad de las partes en el artículo 5, durante la preparación de la Ley Modelo se reconoció en general que la modificación mediante acuerdo podía ser explícita o implícita. El texto del artículo 5 se ha ajustado al del artículo 6 de la Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías (A/CN.9/467, párr. 38).

Acuerdo bilateral o multilateral

113. El artículo 5 tiene la finalidad de ser aplicable no sólo en el contexto de las relaciones entre iniciadores y destinatarios de mensajes de datos sino también en el marco de las relaciones con intervención de intermediarios. Así pues, las disposiciones de la Ley Modelo podrían modificarse mediante acuerdos bilaterales o multilaterales entre las partes o mediante reglas de un sistema convenido por las partes. Normalmente, el derecho aplicable limitaría la autonomía de la voluntad de las partes a los derechos y obligaciones dimanantes para las partes, a fin de evitar repercusiones en cuanto a los derechos y obligaciones de terceros.

Referencias a documentos de la CNUDMI

A/CN.9/467, párrs. 36 a 43;

A/CN.9/WG.IV/WP.84, párrs. 39 y 40;

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.

Artículo 6. Cumplimiento del requisito de firma

1) Cuando la ley exija la firma de una persona, ese requisito quedará cumplido en relación con un mensaje de datos si se utiliza una firma electrónica que, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo aplicable, sea tan fiable como resulte apropiada a los fines para los cuales se generó o comunicó ese mensaje.

2) El párrafo 1) será aplicable tanto si el requisito a que se refiere está expresado en la forma de una obligación como si la ley simplemente prevé consecuencias para el caso de que no haya firma.

3) La firma electrónica se considerará fiable a los efectos del cumplimiento del requisito a que se refiere el párrafo 1) si:

a) los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante;

b) los datos de creación de la firma electrónica estaban, en el momento de la firma, bajo el control exclusivo del firmante;

c) es posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma; y

d) cuando uno de los objetivos del requisito legal de firma consista en dar seguridades en cuanto a la integridad de la información a que corresponde, es posible detectar cualquier alteración de esa información hecha después del momento de la firma.

4) Lo dispuesto en el párrafo 3) se entenderá sin perjuicio de la posibilidad de que cualquier persona:

a) demuestre de cualquier otra manera, a los efectos de cumplir el requisito a que se refiere el párrafo 1), la fiabilidad de una firma electrónica; o

b) aduzca pruebas de que una firma electrónica no es fiable.

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

Importancia del artículo 6

114. El artículo 6 es una de las disposiciones clave de la Ley Modelo. El artículo 6 sigue la pauta del artículo 7 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico y tiene por objeto dar orientación sobre el modo en que puede satisfacerse el criterio de fiabilidad del inciso b) del párrafo 1) del artículo 7. En la interpretación del artículo 6 debería tenerse presente que el propósito de esa disposición es asegurar que la utilización de una firma electrónica fidedigna tenga las mismas consecuencias jurídicas que pudiera tener una firma manuscrita.

Párrafos 1), 2) y 5)

115. Los párrafos 1), 2) y 5) del artículo 6 introducen disposiciones extraídas de los párrafos 1) b), 2) y 3), respectivamente, del artículo 7 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico. La definición de "firma electrónica" que figura en el artículo 2 a) ya se inspira en el artículo 7 1) a) de la Ley Modelo de la CNUDMI sobre Comercio Electrónico.

Conceptos de "identidad" e "identificación"

116. El Grupo de Trabajo convino en que, a efectos de definición de la "firma electrónica" en la Ley Modelo, el concepto de "identificación" podría ser más que la mera identificación del firmante por su nombre. El concepto de identidad o identificación sirve para diferenciar al firmante de toda otra persona recurriendo a su nombre o a otros datos, que pueden ser otras características notables como la posición o la autoridad de esa persona, ya sea en combinación con un nombre o sin ninguna indicación de nombre. Sobre esa base, no es necesario distinguir entre la identidad y otras características notables de la persona ni limitar la Ley Modelo a las situaciones en que sólo se utilizan certificados de identidad en que se menciona el nombre del tenedor del dispositivo de creación de la firma (A/CN.9/467, párrs. 56 a 58).

Variación del efecto de la Ley Modelo en función de la fiabilidad técnica

117. Durante la preparación de la Ley Modelo, se expresó la opinión de que (mediante una referencia al concepto de "firma electrónica refrendada" o mediante una mención directa de los criterios para verificar la fiabilidad técnica de una determinada técnica de firma) se debería dar al artículo 6 el doble objetivo de establecer: 1) que la aplicación de las técnicas de firmas electrónicas reconocidas como fiables tendría efectos jurídicos; y 2) inversamente, que no se producirían tales efectos jurídicos al utilizarse técnicas de menor fiabilidad. No obstante, se estimó en general que convendría hacer una distinción más sutil entre las diversas técnicas posibles de firma electrónica, ya que debería evitarse que la Ley Modelo

discriminara algún tipo de firma electrónica, por más que en determinadas circunstancias alguna de ellas pudiera parecer poco compleja o segura. Por consiguiente, toda técnica de firma electrónica aplicada con el propósito de firmar un mensaje de datos en el sentido del artículo 7 1) a) de la Ley Modelo de la CNUDMI sobre Comercio Electrónico podía producir efectos jurídicos, siempre y cuando fuera suficientemente fiable habida cuenta de todas las circunstancias, incluidos los eventuales acuerdos entre las partes. Sin embargo, en virtud del artículo 7 de la Ley Modelo, la determinación de lo que constituye un método fiable de firma habida cuenta de las circunstancias sólo puede ser efectuada por un tribunal u otro investigador de hechos que intervenga *a posteriori*, posiblemente mucho tiempo después de que se haya utilizado la firma electrónica. En cambio, la Ley Modelo debe crear en principio un beneficio para ciertas técnicas consideradas particularmente fiables independientemente de las circunstancias en que se utilicen. Esta es la finalidad del párrafo 3), que debe crear la certeza (ya sea mediante una presunción o una regla de fondo), en el momento de utilizarse la técnica de firma electrónica o con anterioridad a ese momento (*a priori*), de que la utilización de una técnica reconocida producirá efectos jurídicos equivalentes a los que surtiría una firma manuscrita. Así pues, el párrafo 3) es una disposición esencial para que la nueva Ley Modelo cumpla su objetivo de ofrecer una certeza mayor que la que ya brinda la Ley Modelo de la CNUDMI sobre Comercio Electrónico en cuanto al efecto jurídico que cabe esperar de la utilización de tipos de firmas electrónicas particularmente fiables (véase A/CN.9/465, párr. 64).

Presunción o regla sustantiva

118. A fin de crear certeza sobre el efecto jurídico resultante de la utilización de lo que pueda o no llamarse una "firma electrónica refrendada" en virtud del artículo 2, el párrafo 3) establece expresamente los efectos jurídicos que se derivarían de la conjunción de ciertas características técnicas de una firma electrónica. En cuanto a la forma en que se establecerían esos efectos jurídicos, los Estados promulgantes, a reserva de lo que dispusiera su legislación de procedimiento civil y comercial, deberían poder adoptar una presunción o proceder a fijar directamente un vínculo entre ciertas características técnicas y el efecto jurídico de una firma (véase A/CN.9/467, párrs. 61 y 62).

Intención del firmante

119. Queda pendiente la cuestión de si se produce algún efecto jurídico al utilizarse técnicas de firma electrónica cuando el firmante no tiene la clara intención de quedar jurídicamente vinculado por la aprobación de la información firmada por medios electrónicos. En tal circunstancia, no se cumple la segunda función descrita en el artículo 7 1) a) de la Ley Modelo de la CNUDMI sobre Comercio Electrónico, pues no existe intención de "indicar que [se] aprueba la información que figura en el mensaje de datos". El criterio adoptado en la Ley Modelo es que las consecuencias jurídicas de la utilización de una firma manuscrita deben reproducirse también en los mensajes electrónicos. Así pues, al adjuntar una firma (ya sea manuscrita o electrónica) a cierta información, cabe presumir que el firmante ha aprobado la vinculación de su identidad con esa información. La posibilidad de que esa vinculación produjera efectos jurídicos (contractuales o de otra índole) dependería de la naturaleza de la información consignada y de otras circunstancias que habría

que evaluar conforme al derecho aplicable al margen de la Ley Modelo. En ese contexto, no se pretende que la Ley Modelo interfiera en el derecho general de los contratos o de las obligaciones (véase A/CN.9/465, párr. 65).

Criterios de fiabilidad técnica

120. Los apartados a) a d) del párrafo 3) tienen la finalidad de expresar criterios objetivos de fiabilidad técnica de las firmas electrónicas. El apartado a) se centra en las características objetivas de los datos de creación de la firma, que debe "corresponder exclusivamente al firmante". Desde el punto de vista técnico, los datos de creación de la firma podrían corresponder exclusivamente al firmante sin ser por sí mismos "exclusivos". El vínculo entre los datos utilizados para la creación de la firma y el firmante constituye el elemento esencial (A/CN.9/467, párr. 63). Si bien ciertos datos de creación de la firma electrónica pueden ser compartidos por diversos usuarios, por ejemplo, en el caso de varios empleados que usan conjuntamente los datos de creación de la firma de una empresa, es preciso que los datos puedan identificar inequívocamente a un usuario en el contexto de cada firma electrónica.

Control exclusivo de los datos de la firma por el firmante

121. El apartado b) regula las circunstancias en que se utilizan los datos de creación de la firma. En el momento de su utilización, los datos deben estar bajo el control exclusivo del firmante. En relación con el concepto de control exclusivo por parte del firmante se plantea la cuestión de si éste conservaría la capacidad para autorizar a otra persona a utilizar en su nombre los datos de la firma. Esta situación podría plantearse en el contexto de una empresa que fuera titular de una firma pero que autorizara a varias personas a firmar en su nombre (A/CN.9/467, párr. 66). Otro ejemplo sería el de ciertas aplicaciones empresariales, por ejemplo, cuando los datos de la firma figuran en una red y pueden ser utilizados por diversas personas. En tal situación, cabe suponer que la red correspondería a una determinada entidad que sería titular de la firma y controlaría los datos de creación de la firma. Si no fuera así y los datos de la firma estuviesen a disposición de cualquier persona, no deberían quedar comprendidos en la Ley Modelo (A/CN.9/467, párr. 67). Cuando una clave única sea utilizada por más de una persona dentro de un sistema de “clave compartida” o de algún otro sistema de “secreto compartido”, toda referencia al “firmante” ha de entenderse como una referencia a esas personas en conjunto (A/CN.9/483, párr. 152).

Mandato

122. Los apartados a) y b) tienen el objetivo común de asegurar que los datos de la firma sólo puedan ser utilizados por una persona en un momento determinado, básicamente el momento en que se crea la firma, y no por otra persona. La cuestión del mandato o la autorización para utilizar los datos de la firma se aborda en la definición de "firmante" (A/CN.9/467, párr. 68).

Integridad

123. Los apartados c) y d) regulan las cuestiones de la integridad de la firma electrónica y la integridad de la información consignada en el mensaje firmado electrónicamente. Se habrían podido combinar las dos disposiciones para subrayar que, cuando se adjunta una firma a un documento, la integridad del documento y la integridad de la firma son dos conceptos que están tan estrechamente vinculados que no pueden concebirse por separado. Cuando se utiliza una firma para firmar un documento, la idea de la integridad del documento es inherente a la utilización de la firma. No obstante, se decidió que la Ley Modelo siguiera la distinción hecha en la Ley Modelo de la CNUDMI sobre Comercio Electrónico entre los artículos 7 y 8. Si bien algunas tecnologías aportan al mismo tiempo la autenticación (artículo 7 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico) y la integridad (artículo 8 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico), se trata de dos conceptos jurídicos diferenciados que deben tratarse como tales. Dado que una firma manuscrita no garantiza la integridad del documento al que se adjunta ni garantiza que puedan detectarse eventuales cambios introducidos en el documento, el criterio de la equivalencia funcional exige que esos conceptos no se regulen en una única disposición. La finalidad del apartado c) del párrafo 3) es enunciar el criterio que debe cumplirse para demostrar que un determinado método de firma electrónica es suficientemente fiable para satisfacer el requisito legal de la firma. Ese requisito legal podía satisfacerse sin tener que demostrar la integridad de todo el documento (véase A/CN.9/467, párrs. 72 a 80).

Equivalente funcional del documento original

124. El apartado d) se ha concebido principalmente para los países cuya normativa legal sobre las firmas manuscritas no permitía hacer una distinción entre la integridad de la firma y la integridad de la información consignada. En otros países, el apartado d) podría crear una firma que resultara más fiable que una firma manuscrita e ir así más allá del concepto de equivalente funcional de una firma. En cualquier circunstancia, el efecto del apartado d) sería la creación de un equivalente funcional a un documento original.

Firma electrónica de parte de un mensaje

125. En el apartado d) el vínculo necesario entre la firma y la información firmada se expresa evitando que ello implique que la firma electrónica sólo pueda ser aplicable al contenido íntegro de un mensaje de datos. De hecho, en muchos casos la información firmada constituye sólo una parte de la información consignada en el mensaje de datos. Por ejemplo, una firma electrónica puede referirse únicamente a la información adjuntada al mensaje a efectos de transmisión.

Modificación mediante acuerdo

126. El párrafo 3) no tiene la finalidad de limitar la aplicación del artículo 5 ni de ningún derecho aplicable que reconozca la libertad de las partes para estipular en cualquier acuerdo pertinente que considerarán que una determinada técnica de firma constituirá entre dichas partes un equivalente fiable a una firma manuscrita.

Referencias a documentos de la CNUDMI

A/CN.9/467, párrs. 44 a 87;
A/CN.9/WG.IV/WP.84, párrs. 41 a 47;
A/CN.9/465, párrs. 62 a 82;
A/CN.9/WG.4/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.

Artículo 7. Cumplimiento de lo dispuesto en el artículo 6

1) *[La persona, el órgano o la entidad, del sector público o privado, a que el Estado promulgante haya expresamente atribuido competencia]* podrá determinar qué firmas electrónicas cumplen lo dispuesto en el artículo 6.

2) La determinación que se haga con arreglo al párrafo 1) deberá ser compatible con las normas internacionales reconocidas.

3) Lo dispuesto en el presente artículo se entenderá sin perjuicio de la aplicación de las normas del derecho internacional privado.

Determinación previa de la condición jurídica de la firma electrónica

127. En el artículo 7 se describe la función desempeñada por el Estado promulgante al establecer o reconocer la entidad que puede validar el uso de firmas electrónicas o certificar su calidad. Al igual que el artículo 6, el artículo 7 se basa en la idea de que lo indispensable para facilitar el desarrollo del comercio electrónico es la certeza y la previsibilidad cuando las partes comerciales hagan uso de técnicas de firma electrónica, no cuando haya una controversia ante un tribunal. Cuando una determinada técnica de firma pueda satisfacer los requisitos de un alto nivel de fiabilidad y seguridad, debería existir un medio para evaluar los aspectos técnicos de la fiabilidad y la seguridad y para dar a la técnica de firma algún tipo de reconocimiento.

Finalidad del artículo 7

128. La finalidad del artículo 7 es aclarar que el Estado promulgante puede designar un órgano o una autoridad confiriéndole la facultad para determinar qué tecnologías específicas pueden beneficiarse de las presunciones o de la regla de fondo que establece el artículo 6. El artículo 7 no es una disposición de habilitación que los Estados puedan o deban necesariamente promulgar en su forma actual. No obstante, tiene el propósito de transmitir el claro mensaje de que puede lograrse certeza y previsibilidad determinando qué técnicas de firma electrónica cumplen los criterios de fiabilidad del artículo 6, siempre y cuando tal determinación se efectúe de conformidad con las normas internacionales. No debe interpretarse el artículo 7 en el sentido de que prescribe efectos jurídicos imperativos para la utilización de ciertos tipos de técnicas de firma, o de que limita la utilización de tecnología a las técnicas que, según se haya determinado, satisfacen los requisitos de fiabilidad del

artículo 6. Por ejemplo, las partes deberían tener libertad para utilizar las técnicas que hayan convenido, aunque no se haya determinado que cumplen los requisitos del artículo 6. También deberían tener libertad para demostrar ante un tribunal ordinario o arbitral que el método de firma que han elegido satisface de hecho los requisitos del artículo 6, aun cuando no haya sido objeto de evaluación para determinar si es así.

Párrafo 1)

129. El párrafo 1) especifica que la entidad que pueda validar la utilización de firmas electrónicas o certificar su calidad no tiene por qué representar una autoridad estatal. No debe deducirse de ello que el párrafo 1) recomienda a los Estados el único medio para lograr el reconocimiento de tecnologías de firma, sino más bien que el párrafo indica las limitaciones aplicables si los Estados optan por ese criterio.

Párrafo 2)

130. Con respecto al párrafo 2), el concepto de "normas" no debe limitarse a las normas oficiales formuladas, por ejemplo, por la Organización Internacional de Normalización (ISO) o por la Internet Engineering Task Force (IETF), ni a otras normas técnicas. La palabra "normas" debe interpretarse en un sentido amplio, que abarque las prácticas industriales y los usos comerciales, los textos dimanantes de organizaciones internacionales como la Cámara de Comercio Internacional y la labor de la CNUDMI propiamente dicha (incluidas la presente Ley Modelo y también la Ley Modelo de la CNUDMI sobre Comercio Electrónico). La posible falta de normas pertinentes no debe impedir a las personas o autoridades competentes efectuar la determinación mencionada en el párrafo 1). En cuanto a las normas "reconocidas", convendría plantearse lo que constituye "reconocimiento" y de quién hay que obtenerlo (véase A/CN.9/465, párr. 94). Esa cuestión se examina además en relación con el artículo 12 (véase *infra*, párr. 154).

Párrafo 3)

131. El párrafo 3) tiene la finalidad de dejar bien claro que el objetivo del artículo 7 es no obstaculizar la vigencia de las normas de derecho internacional privado (véase A/CN.9/467, párr. 94). A falta de tal disposición, podría malinterpretarse el artículo 7 y suponer que alienta a los Estados promulgantes a discriminar las firmas electrónicas extranjeras por no cumplir las reglas enunciadas por la persona o autoridad pertinente conforme al párrafo 1).

Referencias a documentos de la CNUDMI

A/CN.9/467, párrs. 90 a 95;
A/CN.9/WG.IV/WP.84, párrs. 49 a 51;
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.

Artículo 8. Proceder del firmante

1) Cuando puedan utilizarse datos de creación de firmas para crear una firma con efectos jurídicos, cada firmante deberá:

a) actuar con diligencia razonable para evitar la utilización no autorizada de sus datos de creación de la firma;

b) dar aviso sin dilación indebida a cualquier persona que, según pueda razonablemente prever, pueda considerar fiable la firma electrónica o prestar servicios que la apoyen si:

i) sabe que los datos de creación de la firma han quedado en entredicho; o

ii) las circunstancias de que tiene conocimiento dan lugar a un riesgo considerable de que los datos de creación de la firma hayan quedado en entredicho;

c) cuando se emplee un certificado para refrendar la firma electrónica, actuar con diligencia razonable para cerciorarse de que todas las declaraciones que haya hecho en relación con su ciclo vital o que hayan de consignarse en él sean exactas y cabales.

2) El firmante incurrirá en responsabilidad por el incumplimiento de los requisitos enunciados en el párrafo 1).

Título

132. Inicialmente se había previsto que el artículo 8 (y los artículos 9 y 11) contuvieran reglas relativas a las obligaciones y responsabilidades de las diversas partes interesadas (el firmante, la parte que confía en la firma y el eventual prestador de servicios de certificación). No obstante, los rápidos cambios que afectaban a los aspectos técnicos y comerciales del comercio electrónico, junto con el papel que actualmente desempeñaba la autorreglamentación en el comercio electrónico de ciertos países, dificultaban el consenso sobre el contenido de esas reglas. Los artículos se han redactado de modo que representen un "código de conducta" mínimo para las diversas partes. Las consecuencias del incumplimiento de ese código de conducta se dejan en manos del derecho aplicable al margen de la Ley Modelo.

Párrafo 1)

133. Los apartados a) y b) se aplican en general a todas las firmas electrónicas, mientras que el apartado c) es sólo aplicable a las firmas electrónicas avaladas por un certificado. La obligación enunciada en el apartado a) del párrafo 1), en particular, de actuar con diligencia razonable para evitar la utilización no autorizada de un dispositivo de firma, constituye una obligación básica que suele figurar, por ejemplo, en los acuerdos relativos a la utilización de tarjetas de crédito. Conforme al criterio adoptado en el párrafo 1), esa obligación debería ser aplicable también a cualquier dispositivo de firma electrónica que pudiera utilizarse para expresar una intención jurídicamente significativa. Sin embargo, la disposición del artículo 5 relativa a la modificación mediante acuerdo permite modificar las normas

establecidas en el artículo 8 cuando se considere que son inapropiadas o que pueden tener consecuencias indeseadas.

134. El apartado b) del párrafo 1) se refiere a la noción de "persona que, según pueda razonablemente prever [el firmante], pueda considerar fiable la firma electrónica o prestar servicios que la apoyen". Según la tecnología utilizada, esa "parte que confía" puede ser no sólo una persona que trate de confiar en la firma sino también personas como los prestadores de servicios de certificación, los prestadores de servicios de revocación de certificados y otras personas interesadas.

135. El apartado c) del párrafo 1) es aplicable cuando se utiliza un certificado para avalar los datos de la firma. La expresión "ciclo vital del certificado" debe entenderse de forma amplia como el período que va desde la solicitud del certificado o desde la creación del certificado hasta su expiración o revocación.

Párrafo 2)

136. En el párrafo 2) no se especifican las consecuencias ni los límites de la responsabilidad, todo lo cual queda en manos del derecho nacional. No obstante, si bien las consecuencias de la responsabilidad se regirán por el derecho nacional, el párrafo 2) sirve para dar una clara señal a los Estados promulgantes de que el incumplimiento de las obligaciones enunciadas en el párrafo 1) debe acarrear responsabilidad. El párrafo 2) se basa en la conclusión a la que llegó el Grupo de Trabajo en su 35º período de sesiones de que puede ser difícil obtener un consenso sobre las consecuencias que pueden derivarse de la responsabilidad del titular de los datos de creación de la firma. Según el contexto en que se utilice la firma electrónica, esas consecuencias pueden abarcar, según el derecho aplicable, desde la posibilidad de que el titular de los datos quede vinculado por el contenido del mensaje hasta la obligación de pagar daños y perjuicios. En consecuencia, el párrafo 2) se limita a establecer el principio de que el titular de los datos de creación de la firma debe tenerse por responsable del incumplimiento de los requisitos del párrafo 1), y deja en manos del derecho aplicable en cada Estado promulgante, al margen de la Ley Modelo, la regulación de las consecuencias jurídicas que se deriven de tal responsabilidad (A/CN.9/465, párr. 108).

Referencias a documentos de la CNUDMI

A/CN.9/467, párrs. 96 a 104;
A/CN.9/WG.IV/WP.84, párrs. 52 y 53;
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.

Artículo 9. Proceder del prestador de servicios de certificación

1) Cuando un prestador de servicios de certificación preste servicios para apoyar una firma electrónica que pueda utilizarse como firma con efectos jurídicos, ese prestador de servicios de certificación deberá:

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

b) actuar con diligencia razonable para cerciorarse de que todas las declaraciones importantes que haya hecho en relación con el ciclo vital del certificado o que estén consignadas en él sean exactas y cabales;

c) proporcionar medios de acceso razonablemente fácil que permitan a la parte que confía en el certificado determinar mediante éste:

i) la identidad del prestador de servicios de certificación;

ii) que el firmante nombrado en el certificado tenía bajo su control los datos de creación de la firma en el momento en que se expidió el certificado;

iii) que los datos de creación de la firma eran válidos en la fecha en que se expidió el certificado o antes de ella;

d) proporcionar medios de acceso razonablemente fácil que, según proceda, permitan a la parte que confía en el certificado determinar mediante éste o de otra manera:

i) el método utilizado para identificar al firmante;

ii) cualquier limitación en los fines o el valor respecto de los cuales pueda utilizarse los datos de creación de la firma o el certificado;

iii) si los datos de creación de la firma son válidos y no están en entredicho;

iv) cualquier limitación en cuanto al ámbito o el alcance de la responsabilidad indicada por el prestador de servicios de certificación;

v) si existe un medio para que el firmante dé aviso de que los datos de creación de la firma están en entredicho, conforme a lo dispuesto en el apartado b) del párrafo 1) del artículo 8;

vi) si se ofrece un servicio de revocación oportuna del certificado;

e) cuando se ofrezcan servicios conforme al inciso v) del apartado d), proporcionar un medio para que el firmante dé aviso conforme al apartado b) del párrafo 1) del artículo 8 y, cuando se ofrezcan servicios conforme al inciso vi) del apartado d), cerciorarse de que exista un servicio de revocación oportuna del certificado;

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

2) El prestador de servicios de certificación incurrirá en responsabilidad por el incumplimiento de los requisitos enunciados en el párrafo 1).

Párrafo 1)

137. En el apartado a) se enuncia la regla fundamental de que el prestador de servicios de certificación debe atenerse a las declaraciones que haya hecho y a los compromisos que haya contraído, por ejemplo, en una declaración de prácticas de certificación o en cualquier otro tipo de declaración de principios. En el apartado b) se reproduce, en el contexto de las actividades del prestador de servicios de certificación, la norma de conducta enunciada en el artículo 8 1) c) con respecto al firmante.

138. En el apartado c) se define el contenido esencial y el efecto primordial de todo certificado con arreglo a la Ley Modelo. En el apartado d) se enumeran otros elementos que deben incluirse en el certificado o que deben estar disponibles o accesibles para la parte que confía en la firma, cuando sean de interés para un determinado certificado. El apartado e) no es aplicable a certificados como los de transacción, que son certificados para una vez, ni a los certificados de bajo costo o aplicaciones de bajo riesgo, que en ambos casos pueden no estar sujetos a revocación.

139. Podría pensarse que cabe razonablemente esperar que cualquier prestador de servicios de certificación, y no sólo los que expide certificados de “alto valor” cumplan los deberes y obligaciones previstos en el artículo 9. Sin embargo, los autores de la Ley Modelo se esmeraron en no requerir de un firmante ni de un prestador de servicios de certificación un grado de diligencia o fiabilidad que no estuviera en relación razonable con las finalidades para las que se utilizan las firmas electrónicas o el certificado correspondiente. La Ley Modelo propugna, pues, una solución que vincula las obligaciones expuestas en los artículos 8 y 9 a la producción de firmas electrónicas jurídicamente relevantes (A/CN.9/483, párr. 117). Al limitar el alcance del artículo 9 a la amplia gama de situaciones en las que se prestan servicios de certificación en apoyo de una firma electrónica que pueda ser utilizada con efectos jurídicos como firma, la Ley Modelo no se propone crear nuevos tipos de efectos jurídicos para las firmas (ibíd., párr. 119).

Párrafo 2)

140. El párrafo 2) refleja la regla básica de fiabilidad enunciada en el artículo 8 2) con respecto al firmante. El efecto de esa disposición es dejar en manos del derecho nacional la determinación de las consecuencias de la responsabilidad. A reserva de las reglas aplicables del derecho nacional, el párrafo 2) no está concebido para que se interprete como una regla de responsabilidad absoluta. No se preveía que el efecto del párrafo 2) sería excluir la posibilidad de que el prestador de servicios de certificación demostrara, por ejemplo, la ausencia de culpa o de negligencia.

141. En anteriores proyectos del artículo 9 figuraba un párrafo suplementario en que se regulaban las consecuencias de la responsabilidad enunciada en el párrafo 2). Durante la preparación de la Ley Modelo, se observó que los prestadores de

servicios de certificación desempeñaban funciones de intermediario que eran fundamentales para el comercio electrónico, y que la cuestión de la responsabilidad de esos profesionales no quedaría suficientemente reglamentada con la adopción de una única disposición del tenor del párrafo 2). Aunque el párrafo 2) enunciara un principio apropiado para su aplicación a los signatarios, tal vez no resultara suficiente para regular las actividades profesionales y comerciales abarcadas por el artículo 9. Un posible modo de paliar esa insuficiencia habría consistido en enumerar, en el texto de la Ley Modelo, los factores que debían tenerse en cuenta al evaluar las pérdidas resultantes del incumplimiento de los requisitos del párrafo 1) por parte del prestador de servicios de certificación. Finalmente, se decidió que en esta Guía figurara una lista no exhaustiva de factores indicativos. Al evaluarse las pérdidas, debían tenerse en cuenta, entre otras cosas, los siguientes factores: a) el costo de obtención del certificado; b) la naturaleza de la información que se certifique; c) la existencia de limitaciones de los fines para los que pueda utilizarse el certificado y el alcance de esas limitaciones; d) la existencia de declaraciones que limiten el alcance o la magnitud de la responsabilidad del prestador de servicios de certificación; y e) toda conducta de la parte que confía en la firma que contribuya a la responsabilidad.

Referencias a documentos de la CNUDMI

A/CN.9/483, párrs. 114 a 127;

A/CN.9/467, párrs. 105 a 129;

A/CN.9/WG.IV/WP.84, párrs. 54 a 60;

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.

Artículo 10. Fiabilidad

A los efectos del apartado f) del párrafo 1) del artículo 9, para determinar si los sistemas, procedimientos o recursos humanos utilizados por un prestador de servicios de certificación son fiables, y en qué medida lo son, podrán tenerse en cuenta los factores siguientes:

a) los recursos humanos y financieros, incluida la existencia de un activo;

b) la calidad de los sistemas de equipo y programas informáticos;

c) los procedimientos para la tramitación del certificado y las solicitudes de certificados, y la conservación de registros;

d) la disponibilidad de información para los firmantes nombrados en el certificado y para las partes que confían en éste;

e) la periodicidad y el alcance de la auditoría por un órgano independiente;

f) la existencia de una declaración del Estado, de un órgano de acreditación o del prestador de servicios de certificación respecto del cumplimiento o la existencia de los factores que anteceden; y

g) cualesquiera otros factores pertinentes.

Flexibilidad del concepto de "fiabilidad"

142. Inicialmente, el artículo 10 fue redactado como parte del artículo 9. Si bien posteriormente esa parte pasó a ser otro artículo, tiene ante todo la finalidad de ayudar a interpretar el concepto de "sistemas, procedimientos y recursos humanos fiables" en el artículo 9 1) f). El artículo 10 está redactado en forma de lista no exhaustiva de factores que deben tenerse en cuenta para determinar la fiabilidad. Esa lista tiene el objetivo de presentar un concepto flexible de la fiabilidad, que podría variar de contenido según lo que se esperara del certificado en el contexto en que se creara.

Referencias a documentos de la CNUDMI

A/CN.9/483, párrs. 128 a 133;
A/CN.9/467, párrs. 114 a 119.

Artículo 11. Proceder de la parte que confía en el certificado

Serán de cargo de la parte que confía en el certificado las consecuencias jurídicas que entrañe el hecho de que no haya tomado medidas razonables para:

a) verificar la fiabilidad de la firma electrónica; o

b) cuando la firma electrónica esté refrendada por un certificado:

i) verificar la validez, suspensión o revocación del certificado; y

ii) tener en cuenta cualquier limitación en relación con el certificado.

Criterio de la confianza razonable

143. El artículo 11 refleja la idea de que la parte que se proponga confiar en una firma electrónica debe tener presente la cuestión de si tal confianza es razonable habida cuenta de las circunstancias y hasta qué punto es razonable. El artículo no pretende abordar la cuestión de la validez de una firma electrónica, que ya se regula en el artículo 6 y no debe depender de la conducta de la parte que confía en la firma. La cuestión de la validez de una firma electrónica no debe vincularse a la cuestión de si es razonable que una parte confíe en una firma que no cumpla la norma enunciada en el artículo 6.

Cuestiones relativas al consumidor

144. Si bien el artículo 11 puede imponer una carga a las partes que confían en una firma, particularmente si esas partes son consumidores, conviene recordar que la Ley Modelo no tiene la finalidad de derogar ninguna norma que rija la protección del consumidor. Sin embargo, la Ley Modelo puede ser de utilidad al informar a todas las partes interesadas, incluidas las partes que confían en firmas, sobre la norma de la conducta razonable que debe observarse con respecto a las firmas electrónicas. Además, el establecimiento de una norma de conducta en virtud de la cual la parte que confía en una firma debe verificar la fiabilidad de la firma con los medios disponibles puede considerarse esencial para el desarrollo de todo sistema de infraestructuras de clave pública.

Concepto de "parte que confía en la firma"

145. En la Ley Modelo no se define el concepto de "parte que confía en la firma". Conforme a la práctica seguida en la industria, ese concepto pretende abarcar a cualquier parte que confíe en una firma electrónica. Por lo tanto, según las circunstancias, la "parte que confía en la firma" puede ser cualquier persona, independientemente de si tiene una relación contractual con el signatario o con el prestador de servicios de certificación. Cabe incluso la posibilidad de que el prestador de servicios de certificación o el propio firmante pase a ser una "parte que confía en una firma". Sin embargo, ese concepto amplio de "parte que confía en una firma" no debe implicar que el suscriptor de un certificado esté obligado a verificar la validez del certificado que obtenga del prestador de servicios de certificación.

Incumplimiento de los requisitos del artículo 11

146. Con respecto a las posibles consecuencias de que se imponga a la parte que confía en la firma la obligación general de verificar la validez de la firma electrónica o del certificado, se plantea la cuestión de lo que debe ocurrir si dicha parte incumple los requisitos del artículo 11. En tal caso, no debe impedirse que la parte haga valer la firma o el certificado si sus medidas razonables de verificación no hubieran permitido determinar la invalidez de la firma o del certificado. Tal vez convendría que la ley aplicable al margen de la Ley Modelo regulara esa situación.

Referencias a documentos de la CNUDMI

A/CN.9/467, párrs. 130 a 143;

A/CN.9/WG.IV/WP.84, párrs. 61 a 63;

A/CN.9/465, párrs. 109 a 122 (artículos 10 y 11 del proyecto);

A/CN.9/WG.IV/WP.82, párrs. 56 a 58 (artículos 10 y 11 del proyecto);

A/CN.9/457, párrs. 99 a 107;

A/CN.9/WG.IV/WP.80, párrs. 20 y 21.

Artículo 12. Reconocimiento de certificados y firmas electrónicas extranjeras

1) Al determinar si un certificado o una firma electrónica produce efectos jurídicos, o en qué medida los produce, no se tomará en consideración:

a) el lugar en que se haya expedido el certificado o en que se haya creado o utilizado la firma electrónica; ni

b) el lugar en que se encuentre el establecimiento del expedidor o firmante.

2) Todo certificado expedido fuera *[del Estado promulgante]* producirá los mismos efectos jurídicos en *[el Estado promulgante]* que todo certificado expedido en *[el Estado promulgante]* si presenta un grado de fiabilidad sustancialmente equivalente.

3) Toda firma electrónica creada o utilizada fuera *[del Estado promulgante]* producirá los mismos efectos jurídicos en *[el Estado promulgante]* que toda firma electrónica creada o utilizada en *[el Estado promulgante]* si presenta un grado de fiabilidad sustancialmente equivalente.

4) A efectos de determinar si un certificado o una firma electrónica presenta un grado de fiabilidad sustancialmente equivalente para los fines del párrafo 2) o del párrafo 3), se tomarán en consideración las normas internacionales reconocidas y cualquier otro factor pertinente.

5) Cuando, sin perjuicio de lo dispuesto en los párrafos 2), 3) y 4), 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, salvo que ese acuerdo no sea válido o eficaz conforme al derecho aplicable.

Norma general de no discriminación

147. El párrafo 1) tiene por fin reflejar el principio básico de que el lugar de origen no debe, en sí mismo, ser un factor que determine si los certificados o las firmas electrónicas extranjeros tienen que ser reconocidos como jurídicamente eficaces, y en qué medida. La determinación de si un certificado o una firma electrónica es jurídicamente eficaz, o en qué medida lo es, no debe depender del lugar en el que se expidió el certificado o la firma (véase el documento A/CN.9/483, párr. 27) sino de su fiabilidad técnica.

"Grado de fiabilidad sustancialmente equivalente"

148. La finalidad del párrafo 2) es dar un criterio general para el reconocimiento transfronterizo de certificados sin el cual los prestadores de servicios de certificación podrían verse enfrentados a la carga irracional de tener que obtener licencias en muchas jurisdicciones. A esos efectos, el párrafo 2) establece un umbral de equivalencia técnica de los certificados extranjeros basado en contrastar su fiabilidad con los requisitos de fiabilidad establecidos por el Estado promulgante, de

conformidad con la Ley Modelo (ibíd., párr. 31). Ese criterio ha de aplicarse prescindiendo de la naturaleza del sistema de certificación utilizado en la jurisdicción de donde emanó el certificado o la firma (ibíd., párr. 29).

Variación del grado de fiabilidad según las jurisdicciones

149. Con una remisión a la noción central de un "grado de fiabilidad sustancialmente equivalente", el párrafo 2) reconoce que puede haber diferencias apreciables entre los requisitos de cada una de las jurisdicciones. El requisito de la equivalencia, utilizado en el párrafo 2), no significa que el grado de fiabilidad de un certificado extranjero sea exactamente idéntico al de un certificado nacional (ibíd., párr. 32).

Variación del grado de fiabilidad dentro de una jurisdicción

150. Además, hay que observar que, en la práctica, los prestadores de servicios de certificación expiden certificados con diversos grados de fiabilidad, según los fines para los que los clientes piensan utilizar esos certificados. Según el grado de fiabilidad respectivo, no todos los certificados son merecedores de producir efectos jurídicos, en el plano interno o en el extranjero. En consecuencia, al aplicar la noción de equivalencia utilizada en el párrafo 2), hay que tener presente que la equivalencia que hay que comprobar es entre certificados del mismo tipo. No obstante, no se ha intentado en la Ley Modelo determinar una correspondencia entre certificados de tipos diferentes expedidos por distintos prestadores de servicios de certificación en diferentes jurisdicciones. La Ley Modelo se ha redactado dejando abierta la posibilidad de una jerarquía de diferentes tipos de certificado. En la práctica, un tribunal judicial o arbitral al que se acuda para decidir sobre los efectos jurídicos de un certificado extranjero examinará normalmente cada certificado atendiendo a criterios de fondo y tratará de casarlo con el grado correspondiente más cercano en el Estado promulgante (ibíd., párr. 33).

Trato igual de los certificados y otros tipos de firmas electrónicas

151. El párrafo 3) expone con respecto a las firmas electrónicas la misma norma enunciada en el párrafo 2) respecto de los certificados (ibíd., párr. 41).

Reconocimiento de ciertos efectos jurídicos al cumplimiento de las leyes de un país extranjero

152. Los párrafos 2) y 3) se ocupan exclusivamente de la comprobación transfronteriza de la fiabilidad que debe practicarse al evaluar la fiabilidad de un certificado o una firma electrónica extranjeros. Pero, en la preparación de la Ley Modelo, se tuvo presente que tal vez los Estados promulgantes desearían obviar la necesidad de contrastar la fiabilidad respecto de determinadas firmas o certificados cuando el Estado promulgante estuviera convencido de que el derecho de la jurisdicción donde se originó la firma o el certificado proporcionaba un grado eficiente de fiabilidad. En cuanto a las técnicas jurídicas mediante las cuales un Estado promulgante pudiera reconocer por adelantado la fiabilidad de los certificados y firmas que cumpliesen con la legislación de un país extranjero (por

ejemplo, una declaración unilateral o un tratado) la Ley Modelo no contiene ninguna sugerencia en concreto (ibíd., párrs. 39 y 42).

Factores que hay que considerar al evaluar la equivalencia sustancial de los certificados y las firmas extranjeros

153. En la preparación de la Ley Modelo, el párrafo 4) se formuló en un principio como un catálogo de los factores a tener en cuenta al determinar si un certificado o una firma electrónica ofrecían un grado sustancialmente equivalente de fiabilidad a los fines del párrafo 2) o el párrafo 3). Se estimó luego que la mayoría de estos factores ya estaban numerados en los artículos 6, 9 y 10. Reiterar de nuevo esos factores en el contexto del artículo 12 habría sido superfluo. Se juzgó que otra posibilidad, remitirse, en el párrafo 4), a las disposiciones apropiadas de la Ley Modelo donde se mencionaban los criterios pertinentes, posiblemente añadiendo otros criterios particularmente importantes para el reconocimiento transfronterizo, produciría una formulación sencillamente compleja (véase, en particular, el documento A/CN.9/483, párrs. 43 a 49). El párrafo 4) se convirtió finalmente en una referencia inconcreta a "cualquier otro factor pertinente", entre los cuales son particularmente importantes los enumerados en los artículos 6, 9 y 10 para la evaluación de los certificados y las firmas electrónicas nacionales. Además, el párrafo 4) extrae las consecuencias del hecho de que evaluar la equivalencia de los certificados extranjeros es cosa algo diferente de evaluar la fiabilidad de un prestador de servicios de certificación conforme a los artículos 9 y 10. Con ese fin, se ha añadido en el párrafo 4) una referencia a "las normas internacionales reconocidas".

Normas internacionales reconocidas

154. La noción de "norma internacional reconocida" debe interpretarse con amplitud para que abarque las normas internacionales técnicas y comerciales (por ejemplo, las dependientes del mercado) y las normas y reglas adoptadas por órganos gubernamentales o intergubernamentales (ibíd., párr. 49). "Normas internacionales reconocidas" pueden ser declaraciones de prácticas técnicas, jurídicas o comerciales aceptadas, desarrolladas por el sector público o el privado (o por ambos), que tengan carácter normativo o interpretativo, generalmente aceptadas para su aplicación internacional. Esas reglas pueden adoptar la forma de requisitos, recomendaciones, directrices, códigos de conducta o declaraciones de prácticas óptimas o de normas (ibíd., párrs. 101 a 104).

Reconocimiento de los acuerdos entre las partes interesadas

155. El párrafo 5) prevé el reconocimiento de los acuerdos entre las partes interesadas acerca del uso de ciertos tipos de firmas electrónicas o certificados como motivo suficiente para el reconocimiento transfronterizo (entre ambas partes) de las firmas o certificados acordados (ibíd., párr. 54). Hay que observar que, en armonía con el artículo 5, no ha de entenderse que el párrafo 5) se aparte de ninguna ley imperativa, en particular de un requisito obligatorio de firmas manuscritas que los Estados promulgantes tal vez deseen mantener en la ley aplicable (ibíd., párr. 113). El párrafo 5) es necesario para dar efecto a las estipulaciones contractuales conforme a las cuales las partes puedan convenir, entre ellas, en reconocer el uso de

ciertas firmas electrónicas o certificados (que quepa considerar extranjeros en alguno o todos los Estados en que las partes puedan tratar de obtener el reconocimiento jurídico de esas firmas o certificados), sin que esas firmas o esos certificados se sometan al criterio de la equivalencia sustancial expresado en los párrafos 2), 3) y 4). El párrafo 5) no afecta a la situación jurídica de terceros (ibíd., párr. 56).

Referencias a documentos de la CNUDMI

A/CN.9/483, párrs. 25 a 58 (artículo 12);
A/CN.9/WG.IV/WP.84, párrs. 61 a 68 (proyecto de artículo 13);
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.

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

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

[5] Ibíd., *quincuagésimo tercer período de sesiones, Suplemento Nº 17* (A/53/17), párrs. 207 a 211.

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

[7] Ibíd., *quincuagésimo quinto período de sesiones, Suplemento Nº 17* (A/55/17), párrs. 380 a 383.

[8] Esta sección está extraída del documento A/CN.9/WG.IV/WP.71, parte I.

[9] Muchos elementos de la descripción del funcionamiento del sistema de firmas numéricas que figura en la presente sección se basan en las Directrices sobre las firmas numéricas de la Asociación de Abogados de los Estados Unidos, págs. 8 a 17.

[10] Algunas de las normativas existentes, como las Directrices sobre las firmas númericas de la Asociación de Abogados de los Estados Unidos recogen el concepto de “inviabilidad computacional” para describir la previsión de la irreversibilidad del proceso, es decir, la esperanza de que sea imposible descifrar la clave privada secreta de un usuario a partir de la clave pública de éste. El concepto de “inviabilidad computacional” es un concepto relativo que

se basa en el valor de los datos protegidos, la estructura informática necesaria para protegerlos, el período de tiempo que debe durar la protección, y el costo y el tiempo necesarios para acceder a los datos, evaluando dichos factores en la actualidad y a la vista de futuros avances tecnológicos (Directrices sobre las firmas numéricas de la Asociación de Abogados de los Estados Unidos, pág. 9, nota 23).

[11] En los casos en que los mismos usuarios emitan claves criptográficas públicas y privadas, tal vez debieran determinar la fiabilidad a los certificadores de claves públicas.

[12] La cuestión de si un gobierno debe tener capacidad técnica para retener o recrear claves de confidencialidad privada podría abordarse a nivel de las entidades principales.

[13] No obstante, en el ámbito de la certificación cruzada, la necesidad de la interoperabilidad mundial exige que las ICP de distintos países puedan comunicarse entre ellas.