Naciones Unidas A/CN.9/WG.IV/WP.86

Asamblea General

Distr. limitada
18 de agosto de 2000
Español
Original: inglés

Comisión de las Naciones Unidas para el Derecho Mercantil Internacional
Grupo de Trabajo sobre Comercio Electrónico
37º período de sesiones
Viena, 18 a 29 de septiembre de 2000

Firmas electrónicas

Proyecto de guía para la incorporación al derecho interno del Régimen Uniforme 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 36º a la preparación del proyecto de Régimen Uniforme de la CNUDMI para las firmas electrónicas (en adelante denominado "Régimen Uniforme"). En los documentos A/CN.9/437, 446, 454, 457, 465 y 467 figuran los informes correspondientes a dichos períodos de sesiones. Al preparar el Régimen Uniforme, el Grupo de Trabajo observó que sería útil ofrecer, en un comentario, más información sobre dicho Régimen. Siguiendo el criterio adoptado en la preparación de la Ley Modelo de la CNUDMI sobre Comercio Electrónico, recibió apoyo general la sugerencia de acompañar el proyecto de Régimen Uniforme de una guía para ayudar a los Estados a incorporarlo a su derecho interno y aplicarlo. La Guía, gran parte de la cual se extraería de los *trabajos preparatorios* del Régimen Uniforme, también sería útil para otros usuarios del Régimen Uniforme.

2. En su 32º período de sesiones, el Grupo de Trabajo examinó la cuestión de las firmas electrónicas tomando como base la nota elaborada por la Secretaría (A/CN.9/WG.IV/WP.84). Tras el debate, el Grupo de Trabajo aprobó el contenido de los proyectos de artículo 1 y 3 a 11 del Régimen Uniforme y los remitió a un grupo de redacción para asegurar la coherencia entre las disposiciones del Régimen Uniforme. Se pidió a la Secretaría que preparase un proyecto de guía para la incorporación al derecho interno de las disposiciones aprobadas. El Grupo de

Trabajo recomendó que, con sujeción a la aprobación de la Comisión, el Grupo examinara en un próximo período de sesiones[3] los proyectos de artículo 2 y 13 del Régimen Uniforme.

3. En su 33º período de sesiones (junio y julio de 2000), la Comisión tomó nota de que el Grupo de Trabajo había aprobado, en su 36º período de sesiones, el texto de los proyectos de artículo 1 y 3 a 11 del Régimen Uniforme. Se dijo que aún quedaban algunas cuestiones por aclarar como consecuencia de la decisión que había adoptado el Grupo de Trabajo de eliminar el concepto de firma electrónica refrendada del Régimen Uniforme. Se manifestó la inquietud de que pudiera ser necesario revisar el resto de las disposiciones del proyecto, dependiendo de las decisiones que adoptase el Grupo de Trabajo con respecto a los proyectos de artículo 2 y 13, para evitar que se creara una situación en la que la norma fijada por el Régimen Uniforme se aplicara de igual manera 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 fuera conllevar consecuencias jurídicas importantes.

4. Tras el debate, la Comisión manifestó su reconocimiento por la labor realizada por el Grupo de Trabajo y por los progresos alcanzados en la preparación del Régimen Uniforme. Se instó al Grupo de Trabajo a que finalizara la labor relativa al Régimen Uniforme en su 37º período de sesiones y a que examinara el proyecto de guía para la incorporación al derecho interno que prepararía la Secretaría[4].

5. En el anexo a la presente nota figuran la Primera parte y el Capítulo I de la Segunda parte del proyecto de guía preparado por la Secretaría. El Capítulo II de la Segunda parte se recoge en el documento A/C.N.9/WG.IV/WP.86/Add.1.

Anexo

RÉGIMEN UNIFORME 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

RÉGIMEN UNIFORME DE LA CNUDMI PARA LAS FIRMAS ELECTRÓNICAS (2001)

Preámbulo *Página*

Artículo 1. Ámbito de aplicación 6
Artículo 3. Igualdad de tratamiento de las tecnologías para la firma 6
Artículo 4. Interpretación 6
Artículo 5. Modificación mediante acuerdo 7
Artículo 6. Cumplimiento del requisito de firma 7
Artículo 7. Cumplimiento de lo dispuesto en el artículo 6 8
Artículo 8. Proceder del firmante 8
Artículo 9. Proceder del proveedor de servicios de certificación 8
Artículo 10. Fiabilidad 9
Artículo 11. Proceder del tercero que actúa confiando en el certificado 10

Segunda parte

GUIA PARA LA INCORPORACIÓN AL DERECHO INTERNO DEL RÉGIMEN UNIFORME DE LA CNUDMI PARA LAS FIRMAS ELECTRÓNICAS (2001)

Párrafos *Página*

Finalidad de la presente guía 1-2 11

Capítulo I. Introducción al Régimen Uniforme 3-84 11

I. Finalidad y origen del Régimen Uniforme 3-24 11

A. Finalidad 3-5 11

B. Antecedentes 6-11 12

C. Historia 12-24 14

II. El Régimen Uniforme como instrumento de armonización de leyes 25-26 17

III. Observaciones generales sobre las firmas electrónicas 27-61 18

A. Funciones de las firmas 27-28 18

B. Firmas numéricas y otras firmas electrónicas 29-61 19

1. Firmas electrónicas basadas en técnicas distintas de la criptografía de clave pública 31-33 19

2. Firmas numéricas basadas en la criptografía de clave pública 34-61 20

a) Terminología y conceptos técnicos 35-43 20

i) Criptografía 35-36 20

ii) Claves públicas y privadas 37-38 21

		Párrafos	*Página*
	iii) La función control	39	21
	iv) La firma numérica	40-41	22
	v) Verificación de la firma numérica	42-43	22
	b) Infraestructura de clave pública (ICP) y proveedores de servicios de certificación	44-60	23
	i) Infraestructura de clave pública	49-51	24
	ii) Proveedor de servicios de certificación	52-50	25
	c) Sinopsis del proceso de la firma numérica	61	27
IV.	Principales características del Régimen Uniforme	62-81	28
	A. Naturaleza legislativa del Régimen Uniforme	62-63	28
	B. Relación con la Ley Modelo de la CNUDMI sobre comercio electrónico	64-67	29
	1. El Régimen Uniforme como instrumento jurídico independiente	64	29
	2. Plena coherencia entre el Régimen Uniforme y la Ley Modelo	65-66	29
	3. Relación con el artículo 7 de la Ley Modelo	67	29
	C. Régimen “marco” que se complementará con reglamentaciones técnicas y contratos	68-69	30
	D. Mayor seguridad de las consecuencias jurídicas de las firmas electrónicas	70-75	30
	E. Normas de conducta básicas para las partes interesadas	76-80	32
	F. Marco de neutralidad respecto de los medios técnicos utilizables	81	33
V.	Asistencia de la Secretaría de la CNUDMI	82-84	34
	A. Asistencia para la redacción de legislación	82-83	34
	B. Información relativa a la interpretación de la legislación basada en el Régimen Uniforme	84	34
Capítulo II. Observaciones artículo por artículo (véase A/CN.9/WG.IV/WP.86/Add.1)		1	3
Artículo 1.	Ámbito de aplicación	2-6	3
Artículo 3.	Igualdad de tratamiento de las tecnologías para la firma	7	5
Artículo 4.	Interpretación	8-10	6
Artículo 5.	Modificación mediante acuerdo	11-14	7
Artículo 6.	Cumplimiento del requisito de firma	15-28	8
Artículo 7.	Cumplimiento de lo dispuesto en el artículo 6	29-33	13
Artículo 8.	Proceder del firmante	34-38	15
Artículo 9.	Proceder del proveedor de servicios de certificación	39-42	17
Artículo 10.	Fiabilidad	43	19
Artículo 11.	Proceder del tercero que actúa confiando en el certificado	44-47	20

Primera parte

RÉGIMEN UNIFORME DE LA CNUDMI PARA LAS FIRMAS ELECTRÓNICAS (2001)

Proyectos de artículo 1 y 3 a 11 del Régimen Uniforme de la CNUDMI para las Firmas Electrónicas

(aprobados por el Grupo de Trabajo de la CNUDMI sobre Comercio Electrónico en su 36º período de sesiones, celebrado del 14 al 25 de febrero de 2000 en Nueva York)

Artículo 1. Ámbito de aplicación

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

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

> AEl presente Régimen será aplicable en todos los casos en que se utilicen firmas electrónicas, excepto en las situaciones siguientes [Y]"

**El término Acomercial@ 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 transacciones siguientes: toda transacción 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 3. Igualdad de tratamiento de las tecnologías para la firma

Ninguna de las presentes disposiciones, 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 del presente Régimen 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 el presente Régimen y que no estén expresamente resueltas en él serán dirimidas de conformidad con los principios generales en que él se inspira.

Artículo 5. Modificación mediante acuerdo

Las partes podrán hacer excepciones al presente Régimen o modificar sus efectos mediante acuerdo, salvo que ese acuerdo no sea válido o eficaz en el derecho del Estado promulgante [o a menos que en el presente Régimen se disponga otra cosa].

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) El medio de creación de la firma electrónica, en el contexto en que es utilizado, corresponde al firmante y a nadie más;

b) El medio de creación de la firma electrónica estaba, al momento de la firma, bajo el control del firmante y de nadie más;

c) Es posible detectar cualquier alteración a 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) Alegue 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 precedente 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.

Artículo 8. Proceder del firmante

1) Cada firmante deberá:

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

b) 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 si:

i) Sabe que el dispositivo de creación de firma ha dejado de ser seguro; o

ii) Las circunstancias de que tiene conocimiento dan lugar a un riesgo considerable de que el dispositivo de creación de firma haya dejado de ser seguro;

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 proveedor de servicios de certificación

1) El proveedor 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 materiales 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 al tercero que ha de actuar confiando en el certificado determinar en éste:

i) La identidad del proveedor de servicios de certificación;

ii) Que la persona nombrada en el certificado tenía bajo su control el dispositivo de creación de firma al momento de ésta;

iii) Que el dispositivo de creación de firma estaba en funcionamiento en la fecha en que se emitió el certificado o antes de ella;

d) Proporcionar medios de acceso relativamente fácil que, según proceda, permitan al tercero que ha de actuar confiando en el certificado determinar, en 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 el dispositivo de creación de firma o el certificado;

iii) Si el dispositivo de creación de firma está en funcionamiento y no ha dejado de ser seguro;

iv) Cualquier limitación en cuanto al ámbito o el alcance de la responsabilidad indicada por el proveedor de los servicios de certificación;

v) Si existe un medio para que el firmante dé aviso de que un dispositivo de creación de firma ha dejado de ser seguro;

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

e) Proporcionar un medio para que el firmante avise que un dispositivo de creación de firma ha dejado de ser seguro y 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 proveedor de servicios de certificación incurrirá en responsabilidad por el incumplimiento de los requisitos enunciados en el párrafo 1).

[Artículo 10. Fiabilidad

Para determinar si los sistemas, procedimientos o recursos humanos son fiables, y en qué medida lo son, se tendrán 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, las solicitudes de certificados y la conservación de registros;

d) La disponibilidad de información para el firmante nombrado en el certificado y para los terceros que puedan actuar confiando en éste;

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

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

g) Cualesquiera otros factores pertinentes.]

Artículo 11. Proceder del tercero que actúa confiando en el certificado

Serán de cargo del tercero que actúe confiando 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 está 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.

Segunda parte

GUÍA PARA LA INCORPORACIÓN AL DERECHO INTERNO DEL RÉGIMEN UNIFORME DE LA CNUDMI PARA LAS FIRMAS ELECTRÓNICAS (2001)

Finalidad de la presente guía

1. Al preparar y aprobar el Régimen Uniforme de la CNUDMI para las Firmas Electrónicas (también denominado en la presente publicación "Régimen Uniforme"), la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) tuvo presente que el Régimen Uniforme 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 el Régimen Uniforme. La Comisión fue además consciente de la probabilidad de que el Régimen Uniforme fuera aplicado por algunos Estados poco familiarizados con las técnicas de comunicación reguladas en el Régimen Uniforme. La presente Guía, que en gran parte está inspirada en los *trabajos preparatorios*, del Régimen Unifome 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 del Régimen Uniforme que tal vez conviniera modificar en razón de alguna circunstancia nacional particular. En la preparación del Régimen Uniforme se partió del supuesto de que el proyecto de Régimen Uniforme iría acompañado de una Guía. Por ejemplo, se decidió que ciertas cuestiones no serían resueltas en el texto del Régimen Uniforme sino en la guía que había de orientar a los Estados en la incorporación del Régimen Uniforme a su derecho interno. En la información presentada en la Guía se explica cómo las disposiciones incluidas en el Régimen Uniforme enuncian los rasgos mínimos esenciales de toda norma legal destinada a lograr los objetivos del Régimen Uniforme.

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

Capítulo I. Introducción al Régimen Uniforme

I. FINALIDAD Y ORIGEN DEL RÉGIMEN UNIFORME

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 (también denominada en la presente publicación "Ley Modelo") con respecto al cumplimiento de la función de la firma en el ámbito electrónico, la finalidad del Régimen Uniforme es ayudar a los Estados a establecer un marco legislativo moderno, armonizado y equitativo para abordar de manera más eficaz las cuestiones de las firmas electrónicas. Como complemento modesto pero importante a la Ley Modelo, el Régimen Uniforme ofrece normas prácticas para comprobar la fiabilidad técnica de las firmas electrónicas. Además, el Régimen Uniforme ofrece un vínculo entre dicha fiabilidad técnica y la eficacia jurídica que cabe esperar de una determinada firma electrónica. El Régimen Uniforme supone una contribución importante a la Ley Modelo 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, el Régimen Uniforme 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 proveedores de servicios) en el Régimen Uniforme puede ayudar a configurar prácticas comerciales más armoniosas en el ciberespacio.

5. Los objetivos del Régimen Uniforme, 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 el Régimen Uniforme (y la Ley Modelo) para todo supuesto en que las partes opten por emplear medios electrónicos de comunicación, un Estado creará un entorno jurídico neutro para todo medio técnicamente viable de comunicación comercial.

B. Antecedentes

6. El Régimen Uniforme 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 dirigidos 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 concreto (y probablemente el 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 para facilitar el creciente empleo de los medios de comunicación modernos. La finalidad de la Ley Modelo 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 “originales”, “manuscritos” o “firmados”. Con respecto a los conceptos de documentos “originales”, “manuscritos” o “firmados”, la Ley Modelo adoptó un enfoque de equivalencia funcional.

9. Cuando se estaba preparando la Ley Modelo, unos cuantos países habían adoptado reglas especiales para regular determinados aspectos del comercio electrónico. No obstante, se hacía sentir la ausencia de un régimen 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 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. Además, la Ley Modelo puede resultar un valioso instrumento, en el ámbito internacional, para interpretar ciertos convenios y otros instrumentos internacionales existentes que impongan de hecho algunos obstáculos 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 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 normas uniformes sobre los temas mencionados. Se convino en que las normas uniformes que había que preparar se refirieran 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 de certificación mediante el uso de registros y la incorporación por remisión[5].

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 normas uniformes 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 que se examinaran las cuestiones siguientes en el ámbito del comercio electrónico: alternativas técnicas a la criptografía de clave pública; cuestiones generales relacionadas con los terceros que eran proveedores de servicios; y la contratación electrónica (A/CN.9/437, párrs. 156 y 157). 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 en lo relativo a los diversos medios técnicos disponibles. Por ello, el Régimen Uniforme no debería desalentar el recurso a otras técnicas de autenticación. Además, al ocuparse de la criptografía de clave pública, tal vez fuera preciso que el Régimen Uniforme acomodara diversos grados de seguridad y reconociera diversos efectos jurídicos y grados de responsabilidad según cuales fueran los servicios prestados en el contexto de las firmas numéricas. Respecto de las entidades certificadoras, si bien la Comisión reconoció el valor de las normas de fiabilidad o seguridad fijadas por el mercado, predominó el parecer de que el Grupo de Trabajo podría considerar el establecimiento de un 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[6].

15. El Grupo de Trabajo empezó a preparar el Régimen Uniforme 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 claras 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 el 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[7].

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 sus períodos de sesiones 33º (junio y julio de 1998) y 34º (febrero de 1999) (A/CN.9/454 y 457). La Comisión expresó su agradecimiento por los esfuerzos desplegados por el Grupo de Trabajo con miras a preparar el proyecto de régimen uniforme para las firmas electrónicas. Si bien en general se convino en que durante esos períodos de sesiones se habían logrado

progresos considerables en la comprensión de las cuestiones jurídicas relativas a las firmas electrónicas, también se estimó que el Grupo de Trabajo había afrontado dificultades para formar un consenso con respecto a la política legislativa en que debía basarse el Régimen Uniforme.

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. Si bien se requería cierto grado de reglamentación con respecto a algunos usos de las firmas electrónicas que rebasaban el ámbito del derecho comercial, el Grupo de Trabajo no debía desempeñar ninguna función de reglamentación.

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 actúan confiando en el certificado) correspondía a un posible modelo de IPC, otros modelos eran concebibles, por ejemplo, cuando no participara una entidad certificadora independiente. Una de las principales ventajas que podrían obtenerse si se centrara la atención en las cuestiones relativas a las ICP era facilitar la estructuración del Régimen Uniforme mediante la referencia a tres funciones (o papeles) con respecto a los pares de claves, a saber, la función del emisor (o suscriptor) de la clave, la función de certificación y la función de confianza. Se convino en general en que esas tres funciones eran comunes a todos los modelos de ICP. Se convino también en que las tres funciones debían abordarse sin perjuicio de que las desempeñasen tres entidades distintas o que dos de esas funciones las desempeñase la misma persona (por ejemplo, cuando la entidad certificadora fuese asimismo tercero que actúa confiando 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 de una norma plenamente neutral respecto de los medios técnicos utilizados en una etapa ulterior (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[8].

23. El Grupo de Trabajo continuó con su labor en sus períodos de sesiones 35 (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 artículo 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 artículo 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 proyecto de régimen uniforme y examinara el proyecto de guía para su incorporación al derecho interno que prepararía la Secretaría[9]. *[Nota de la Secretaría: la presente sección en la que figura la historia del régimen uniforme tendrá que completarse, y posiblemente se hará más concisa, una vez que la Comisión lleve a cabo el examen final y apruebe el Régimen Uniforme]*.

II. EL RÉGIMEN UNIFORME COMO INSTRUMENTO DE ARMONIZACIÓN DE LEYES

25. Al igual que la Ley Modelo, el Régimen Uniforme 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 del Régimen Uniforme (o de cualquier otra Ley Modelo elaborada por la CNUDMI).

26. 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 el Régimen Uniforme a su derecho interno. En general, al promulgar un régimen uniforme (o una Ley Modelo), es aconsejable ajustarse lo más posible al texto uniforme a fin de que el derecho interno sea lo más transparente posible para los extranjeros que recurran a él.

III. OBSERVACIONES GENERALES SOBRE LAS FIRMAS ELECTRÓNICAS[10]

A. Funciones de las firmas

27. 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, el Grupo de Trabajo examinó la 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 cual 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 del Régimen Uniforme con el artículo 7 de la Ley Modelo.

28. 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 transacciones 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

29. Al examinar la conveniencia y viabilidad de preparar un régimen uniforme y de definir el ámbito de dicho régimen, 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.

30. Como ya se ha indicado, 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 de 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, proveedores de servicios de certificación y terceros que actúan confiando en el certificado) corresponde a un modelo posible de ICP, pero que existen 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 un régimen uniforme 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 proveedor de los servicios de certificación es también tercero que actúa confiando 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

31. 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.

32. En la preparación del régimen uniforme, se facilitó poca información al Grupo de Trabajo sobre Comercio Electrónico de la CNUDMI acerca de las consecuencias técnicas y jurídicas del empleo de dispositivos de "firma" basados en técnicas distintas de la criptografía de clave pública. Ante la disponibilidad de suficiente información previa acerca de las consecuencias jurídicas de las firmas numéricas, y de la existencia de proyectos de legislación sobre este tema en varios países, el trabajo de la CNUDMI se centró en cuestiones relativas a las firmas numéricas basadas en la criptografía de clave pública.

33. No obstante, la CNUDMI ha tratado de elaborar un régimen uniforme que facilite 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 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, no debe interpretarse que el Régimen Uniforme 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[11]

34. 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

35. 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 primarios). 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 general "criptosistemas" o, más concretamente, "criptosistemas asimétricos" cuando se basan en el empleo de algoritmos asimétricos.

36. 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. La codificación 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 de la codificación 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

37. 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. Cabe 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 primarios: una vez que se multiplican entre sí para obtener un nuevo número, constituye una tarea larga y difícil determinar cuáles fueron los dos números primarios que crearon ese nuevo número mayor[12]. 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.

38. 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 primarios. 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

39. 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 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 fue firmado en forma numérica.

iv) La firma numérica

40. 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.

41. 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

42. 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.

43. 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 proveedores de servicios de certificación

44. 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.

45. 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.

46. 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[13].

47. 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 contrarrestar una negativa falsa de una firma numérica (cuestión su suele denominarse Arepudio negativo@) si la transacción resulta desfavorable para el supuesto firmante.

48. 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 el Régimen Uniforme, se ha elegido el término de “proveedor 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)

49. 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 un directorio seguro 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.

50. 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 incluyen 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[14]; 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, 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.

51. 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[15]. A este respecto, quizá sea necesario que cada Estado que contemple el establecimiento de una ICP adopte decisiones, por ejemplo, respecto de: 1) el formato 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 Alicencia@, 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 Acustodia de claves@ o de otro tipo. El Régimen Uniforme no aborda estas cuestiones.

ii) Proveedor de servicios de certificación

52. Para vincular un par de claves a un posible firmante, el proveedor 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 Asujeto@ 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 tenedor 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.

53. 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 operacional del otro certificado utilizado para verificar la firma numérica de la entidad certificadora.

54. 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 Aperíodo operacional@ indicado en el certificado, que es una condición para poder verificar una firma numérica.

55. 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 utilizar para verificar firmas numéricas.

56. Una vez emitido, puede que un certificado no sea fiable, por ejemplo si el tenedor 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 tenedor o aún sin el consentimiento de éste, según las circunstancias), puede suspender (interrumpir temporalmente el período operacional) 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 que se tenga conocimiento de que han recibido una firma numérica verificable por remisión al certificado que carezca de fiabilidad.

57. 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 privada 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 Acertificación 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.

58. 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.

59. 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.

60. Al preparar el Régimen Uniforme, 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 transacciones subyacentes, por ejemplo con motivo de un proceso legal o de una reclamación de propiedad); 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, Aprogramas de recuperación en casos de desastre@ o depósitos de claves); 8) selección y gestión del personal; 9) diposiciones 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

61. 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 Acompendio 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 DEL RÉGIMEN UNIFORME

A. Naturaleza legislativa del Régimen Uniforme

62. El Régimen Uniforme fue preparado partiendo del supuesto de que debería derivarse directamente del artículo 7 de la Ley Modelo y considerarse como una forma de proporcionar información detallada sobre el concepto del “método fiable para identificar@ a una persona y Apara indicar que esa persona aprueba@ la información que figura en el mensaje de datos (véase A/CN.9/WG.IV/WP.71, párr. 49).

63. Se planteó la cuestión de la forma que debería adoptar el proyecto de Régimen Uniforme 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).

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

1. El régimen uniforme como instrumento jurídico independiente

64. El Régimen Uniforme podría haberse integrado en una versión ampliada de la Ley Modelo, por ejemplo como una nueva tercera parte de la Ley Modelo. Si bien se señaló claramente que cabría promulgar el Régimen Uniforme tanto en forma de norma independiente como en forma de texto adicional a la Ley Modelo, se decidió finalmente que el Régimen Uniforme 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 el régimen uniforme, la Ley Modelo 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 podría haber puesto en peligro el éxito de la versión original al sugerir la necesidad de mejorar ese texto mediante una actualización. Además, la preparación de una nueva versión de la Ley Modelo podría haber dado lugar a confusiones en los países que la habían aprobado recientemente.

2. Plena coherencia entre el Régimen Uniforme y la Ley Modelo

65. Al redactar el Régimen Uniforme, se hizo todo lo posible para asegurar su coherencia con el contenido y la terminología de la Ley Modelo (A/CN.9/465, párr. 37). En el Régimen Uniforme se han reproducido las disposiciones generales de la Ley Modelo, es decir los artículos 1 (Ámbito de aplicación), 2 a), c) y d) (Definiciones de Amensaje de datos@, Ainiciador@ y Adestinatario@), 3 (Interpretación), 4 (Modificación mediante acuerdo) y 7 (Firma) de la Ley Modelo.

66. Al basarse en la Ley Modelo, el Régimen Uniforme trata de reflejar en particular: el principio de la neutralidad respecto de los medios técnicos utilizados; el criterio de la no discriminación de todo equivalente funcional de los conceptos y prácticas que tradicionalmente funcionan sobre soporte de papel; y una amplia confianza en la autonomía contractual de las partes (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 Aabierto@ (es decir, un entorno en el que las partes negocien por vía electrónica sin acuerdo previo) y como reglas de derecho supletorio en un entorno Acerrado@ (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

67. Al preparar el Régimen Uniforme, se expresó la opinión de que la referencia al artículo 7 de la Ley Modelo en el texto del artículo 6 del Régimen Uniforme debía interpretarse en el sentido de que limitaba el alcance del Régimen Uniforme 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 imponía muy pocos requisitos de esta índole con respecto a los documentos utilizados en operaciones comerciales, el alcance del Régimen Uniforme era muy limitado. En respuesta a este argumento, se convino en general en que esa interpretación del proyecto de artículo 6 (y del artículo 7 de la Ley Modelo) era incompatible con la interpretación de las palabras Ala ley@ adoptada por la Comisión en el párrafo 68 de la Guía para la incorporación de la Ley Modelo al derecho interno, conforme a la cual debía entenderse que "las palabras Ala 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 como del artículo 6 del Régimen Uniforme 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 Amarco@ que se complementará con reglamentaciones técnicas y contratos

68. Como complemento a la Ley Modelo de la CNUDMI sobre Comercio Electrónico, la finalidad del Régimen Uniforme es ofrecer principios fundamentales que faciliten el empleo de las firmas electrónicas. Sin embargo, en tanto que Amarco@, el Régimen Uniforme no establece en sí mismo 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 del Régimen Uniforme 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 el Régimen Uniforme y tengan en cuenta circunstancias específicas, posiblemente cambiantes, existentes en el Estado promulgante, sin poner en entredicho los objetivos del Régimen Uniforme. 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.

69. Cabe señalar que las técnicas de creación de firmas electrónicas que se recogen en el Régimen Uniforme, 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 el Régimen Uniforme, 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 el Régimen Uniforme.

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

70. Una de las características principales del Régimen Uniforme es la de aumentar la seguridad del funcionamiento de los criterios de flexibilidad que se establecen en

el artículo 7 de la Ley Modelo para el reconocimiento de una firma electrónica como equivalente funcional a una firma manuscrita.

El artículo 7 de la Ley Modelo 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: [...]".

71. 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 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.

72. 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.

73. 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.

74. 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).

75. Partiendo de los flexibles criterios que figuran en el apartado b) del párrafo 1) del artículo 7 de la Ley Modelo, los artículos 6 y 7 del Régimen Uniforme 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 del Régimen Uniforme 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. Se trata de cualquier “método” que pueda emplearse para cumplir un 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 el Régimen Uniforme. 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 el Régimen Uniforme. 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

76. El Régimen Uniforme no aborda en detalle las cuestiones de la responsabilidad que puede corresponder a cada una de las partes interesadas en el funcionamiento de los sistemas de creación de firmas electrónicas. Esas cuestiones quedan al margen del Régimen Uniforme y se dejan al derecho aplicable. No obstante, en el Régimen Uniforme se fijan criterios para evaluar la conducta de las partes, a saber, el firmante, el tercero que actúa confiando en el certificado y el proveedor de servicios de certificación.

77. En cuanto al firmante, el Régimen Uniforme 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 su dispositivo de creación de firma. Cuando el firmante sepa o deba saber que el dispositivo de creación de 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.

78. Se espera que el tercero que actúa confiando 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 actúa confiando en el certificado deberá tomar medidas razonables para verificar la validez, suspensión o revocación del certificado, y tener en cuenta cualquier limitación en relación con el certificado.

79. La obligación general del proveedor 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 el proveedor de servicios de certificación 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 proveedor deberá proporcionar información fundamental que permita al tercero que haya de actuar confiando en el certificado determinar la identidad del proveedor 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 firma al momento de ésta; y 2) que el dispositivo de creación de firma estaba en funcionamiento en la fecha en que se emitió el certificado o antes de ella. Con respecto al tercero que ha de actuar confiando, el proveedor 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 firma o el certificado; 3) las condiciones de funcionamiento del dispositivo de creación de firma; 4) cualquier limitación en cuanto al ámbito o el alcance de la responsabilidad del proveedor 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 dejado de ser seguro; y 6) si se ofrece el servicio de revocación oportuna del certificado.

80. En le Régimen Uniforme figura una lista abierta de factores indicativos para determinar la fiabilidad de los sistemas, procedimientos y recursos humanos utilizados por el proveedor de servicios de certificación.

F. Marco de neutralidad respecto de los medios técnicos utilizables

81. Ante la evolución de las innovaciones tecnológicas, el Régimen Uniforme establece el reconocimiento jurídico de las firmas electrónicas independientemente de la tecnología utilizada (a saber, firmas electrónicas basadas en la criptografía asimétrica o en la biometría).

V. ASISTENCIA DE LA SECRETARÍA DE LA CNUDMI

A. Asistencia para la redacción de legislación

82. 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 el Régimen Uniforme de la CNUDMI para las firmas electrónicas. Esta misma asistencia se prestará a los gobiernos que estudien la promulgación de legislación basada en leyes modelo de la CNUDMI o la adhesión a uno de los convenios y convenciones de derecho mercantil internacional preparados por la CNUDMI.

83. Puede pedirse a la Secretaría, cuya dirección se indica a continuación, más información acerca del Régimen Uniforme, 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 el Régimen Uniforme

84. La secretaría agradecerá cualquier observación relativa al Régimen Uniforme y a la Guía, así como que se le informe sobre la promulgación de legislación basada en el Régimen Uniforme. Una vez promulgado, el Régimen Uniforme 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 contrareembolso 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.

[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] A/CN.9/467, párrs. 18 a 20.

[4] *Documentos Oficiales de la Asamblea General, quincuagésimo primer período de sesiones, Suplemento Nº 17* (A/55/17), párrs. 380 a 383.

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

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

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

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

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

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

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

[12] Algunas de las normativas existentes, como las Directrices sobre las firmas numéricas 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).

[13] 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.

[14] 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.

[15] 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.