NATIONS
UNIES

A

Assemblée générale

Distr. LIMITÉE
A/CN.9/WG.IV/WP.76
25 mai 1998

FRANÇAIS
Original: ANGLAIS

COMMISSION DES NATIONS UNIES
POUR LE DROIT COMMERCIAL INTERNATIONAL
Groupe de travail sur le commerce électronique
Trente-troisième session
New York, 29 juin-10 juillet 1998

PROJET DE RÈGLES UNIFORMES SUR LES SIGNATURES ÉLECTRONIQUES

Note du Secrétariat

TABLE DES MATIÈRES

	Paragraphes	Page
INTRODUCTION	1-8	3
I. OBSERVATIONS GÉNÉRALES	9-11	4
II. PROJET DE DISPOSITIONS SUR LES SIGNATURES NUMÉRIQUES, LES AUTRES SIGNATURES ÉLECTRONIQUES, LES AUTORITÉS DE CERTIFICATION ET LES QUESTIONS JURIDIQUES CONNEXES	12-50	5
CHAPITRE PREMIER. CHAMP D'APPLICATION ET DISPOSITIONS GÉNÉRALES	12-15	5
CHAPITRE II. SIGNATURES ÉLECTRONIQUES	16-38	6
Section I. Signatures électroniques en général	16-22	6
Article premier. Définitions	16-20	6
Article 2. Effet de la signature électronique	21	9
Section II. Signatures électroniques [renforcées] [sécurisées]	22-30	10
Article 3. Présomption de signature	22-23	10
Article 4. Présomption d'attribution	24	10
Article 5. Présomption d'intégrité	25-26	11
Article 6. Prédétermination de la signature électronique [renforcée] [sécurisée]	27	11

V.98-53825

TABLE DES MATIÈRES (suite)

	Paragraphes	Page
Article 7. Responsabilité pour une signature électronique [renforcée] [sécurisée]	28-30	12
Section III. Signatures numériques accompagnées de certificats	31-38	13
Article 8. Teneur d'un certificat [renforcé][sécurisé]	31	13
Article 9. Effet des signatures numériques accompagnées de certificats	32-38	14
CHAPITRE III. AUTORITÉS DE CERTIFICATION ET QUESTIONS CONNEXES	39-47	16
Article 10. Garanties données au moment de l'émission d'un certificat	39	16
Article 11. Responsabilité contractuelle	40	17
Article 12. Responsabilité de l'autorité de certification envers les parties se fiant au certificat	41	18
Remarque générale concernant les projets d'articles 13 à 16	42	18
Article 13. Annulation d'un certificat	43	19
Article 14. Suspension d'un certificat	44	20
Article 15. Registre des certificats	45-46	20
Article 16. Relations entre les parties se fiant aux certificats et l'autorité de certification	47	21
CHAPITRE IV. SIGNATURES ÉLECTRONIQUES ÉTRANGÈRES	48-50	22
Article 17. Fourniture de services par des autorités de certification étrangères	48	22
Article 18 Approbation des certificats étrangers par les autorités de certification nationales	49	23
Article 19. Reconnaissance de certificats étrangers	50	24

INTRODUCTION

1. À sa vingt-neuvième session (1996), la Commission a décidé d'inscrire à son ordre du jour les questions des signatures numériques et des autorités de certification. Le Groupe de travail sur le commerce électronique a été prié d'examiner l'opportunité et la faisabilité de l'établissement de règles uniformes sur ces questions. Il a été convenu que, dans le cadre des travaux de sa trente et unième session, le Groupe de travail pourrait élaborer un projet de règles sur certains de leurs aspects. Il a été prié de fournir à la Commission des éléments d'information suffisants pour permettre à cette dernière de se prononcer en toute connaissance de cause sur le champ d'application des règles uniformes à élaborer. S'agissant de donner un mandat plus précis au Groupe de travail, il a été convenu que les règles uniformes devraient porter sur des questions telles que le fondement juridique des opérations de certification, y compris les nouvelles techniques d'authentification et de certification numériques; l'applicabilité de la certification; la répartition des risques et des responsabilités entre utilisateurs, prestataires et tiers dans le contexte de l'utilisation de techniques de certification; les questions spécifiques à la certification sous l'angle de l'utilisation de registres; et l'incorporation par référence[1].

2. À sa trentième session (1997), la Commission était saisie du rapport du Groupe de travail sur les travaux de sa trente et unième session (A/CN.9/437). S'agissant de l'opportunité et de la faisabilité de l'élaboration de règles uniformes sur les questions des signatures numériques et des autorités de certification, le Groupe de travail a indiqué à la Commission qu'il était parvenu à un consensus quant à l'importance et à la nécessité de travailler à l'harmonisation du droit dans ce domaine. Bien que n'ayant pas pris de décision ferme sur la forme et la teneur de ces travaux, il était parvenu à la conclusion préliminaire qu'il était possible d'entreprendre l'élaboration d'un projet de règles uniformes tout au moins sur les questions concernant les signatures numériques et les autorités de certification, et éventuellement sur des questions connexes. Le Groupe de travail a rappelé que, outre les signatures numériques et les autorités de certification, les travaux dans le domaine du commerce électronique devaient peut-être concerner aussi les questions touchant des techniques autres que la cryptographie à clef publique, les questions générales concernant les fonctions exercées par les tiers fournisseurs de services et les contrats électroniques (A/CN.9/437, par. 156 et 157). S'agissant de la question de l'incorporation par référence, le Groupe de travail a conclu qu'il n'y avait pas besoin de nouvelle étude du Secrétariat, car les problèmes fondamentaux étaient bien connus, et il était clair que de nombreux aspects du conflit de formulaires et des contrats d'adhésion devraient être réglés par les lois nationales applicables en raison, par exemple, de la protection du consommateur et d'autres considérations d'ordre public. Le Groupe de travail a donc été d'avis que cette question devrait être la première des questions de fond inscrites à l'ordre du jour de sa prochaine session (A/CN.9/437, par. 155).

3. La Commission a pris note avec satisfaction des travaux déjà effectués par le Groupe de travail à sa trente et unième session, a approuvé ses conclusions et lui a confié l'élaboration de règles uniformes sur les questions juridiques relatives aux signatures numériques et aux autorités de certification (dénommées ci-après "les Règles uniformes").

4. S'agissant du champ d'application et de la forme exacts de ces règles uniformes, il a été généralement convenu qu'aucune décision ne pouvait être prise à un stade aussi précoce. On a estimé qu'il était justifié que le Groupe de travail axe son attention sur les questions relatives aux signatures numériques étant donné le rôle apparemment prédominant joué par la cryptographie à clef publique dans la nouvelle pratique du commerce électronique mais les règles uniformes devraient être compatibles avec l'approche techniquement neutre adoptée dans la Loi type de la CNUDCI sur le commerce électronique. Ainsi, les règles uniformes ne devraient pas décourager l'utilisation d'autres techniques d'authentification. En outre, s'agissant de la cryptographie à clef publique, il pourrait être nécessaire de prendre en considération, dans ces règles uniformes, divers niveaux de sécurité et de reconnaître les divers effets juridiques et niveaux de responsabilité correspondant aux différents types de services fournis dans le contexte des signatures numériques. S'agissant des autorités de certification, la Commission a certes reconnu la valeur des normes issues du marché mais il a été largement considéré que le

Groupe de travail pourrait utilement envisager l'établissement d'un ensemble minimum de normes que les autorités de certification devraient respecter, en particulier dans les cas de certification internationale[2].

5. Le Groupe de travail a entamé l'élaboration des règles uniformes à sa trente-deuxième session sur la base d'une note établie par le secrétariat (A/CN.9/WG.IV/WP.73). Le secrétariat a été prié d'élaborer, à partir des délibérations et conclusions du Groupe de travail, un ensemble de dispositions révisées, en y incluant des variantes possibles, aux fins d'examen par le Groupe à une future session (pour le rapport sur les travaux de cette session, voir le document A/CN.9/446). En ce qui concerne l'incorporation par référence, le Groupe de travail a adopté le texte d'un projet de disposition, a décidé de le présenter à la Commission pour examen et éventuellement pour incorporation en tant que nouvel article 5 *bis* de la Loi type de la CNUDCI sur le commerce électronique et a prié le secrétariat d'établir une note explicative à ajouter au Guide pour l'incorporation de la Loi type (A/CN.9/446, par. 24).

6. La présente note contient un projet révisé de dispositions élaboré à la suite des délibérations et des décisions du Groupe de travail et à la suite des délibérations et des décisions de la Commission à sa trentième session, dont il est rendu compte ci-dessus. Le projet de dispositions est fondé, en particulier, sur le principe adopté par le Groupe de travail selon lequel ses travaux dans le domaine des signatures numériques prendraient la forme de projets de dispositions juridiques (A/CN.9/437, par. 27). Il tient également compte de la décision prise par le Groupe de travail à sa trente et unième session selon laquelle les éventuelles règles uniformes concernant les signatures numériques devraient s'inspirer de l'article 7 de la Loi type de la CNUDCI sur le commerce électronique (dénommée ci-après "la Loi type") et être considérées comme définissant la manière dont une méthode fiable pourrait servir à "identifier une personne" et "signifier qu'une personne approuve" l'information contenue dans un message de données. De façon plus générale, en attendant une décision finale sur la relation entre la Loi type, les règles uniformes et d'éventuelles règles sur l'incorporation par référence (voir A/CN.9/437, par. 151 à 155), le projet de dispositions doit être conforme aux principes énoncés et à la terminologie employée dans la Loi type (A/CN.9/437, par. 26).

7. Pour établir la présente note, le Secrétariat a bénéficié de l'aide d'un groupe d'experts dont certains avaient été invités par lui et d'autres désignés par les pays et les organisations internationales intéressés.

8. En application des instructions concernant un contrôle et une limitation plus rigoureux des documents de l'Organisation des Nations Unies, les remarques qui suivent chacun des projets de disposition sont aussi brèves que possible. Des explications plus détaillées seront données oralement lors de la session.

I. OBSERVATIONS GÉNÉRALES

9. Les Règles uniformes ont pour objectif, comme le montre le projet de dispositions figurant dans la deuxième partie de la présente note, de faciliter un développement de l'utilisation des signatures numériques dans les transactions commerciales internationales. S'inspirant des nombreux instruments législatifs déjà en vigueur ou en cours d'élaboration dans un certain nombre de pays, ce projet de dispositions vise à prévenir une discordance des règles juridiques applicables au commerce électronique en offrant un ensemble de normes sur lesquelles se fonder pour reconnaître les effets juridiques des signatures numériques et autres signatures électroniques, avec l'aide éventuelle des autorités de certification, pour lesquels un certain nombre de règles de base sont aussi prévues.

10. Axées sur les aspects de droit privé des transactions commerciales, les Règles uniformes ne tentent pas de régler toutes les questions pouvant surgir dans le cadre d'une utilisation accrue des signatures électroniques. En particulier, elles ne traitent pas des aspects relatifs à l'ordre public, au droit administratif, au droit de la

consommation ou au droit pénal que les législateurs nationaux peuvent être appelés à prendre en considération lorsqu'ils établissent un cadre juridique général pour les signatures électroniques.

11. S'inspirant de la Loi type, les Règles uniformes visent à faire ressortir en particulier le principe de la neutralité quant aux techniques employées, se fondent sur une approche ne désavantageant pas les équivalents fonctionnels des concepts et pratiques traditionnels fondés sur le papier et font une large place à l'autonomie des parties. Elles devraient constituer à la fois des normes minimales dans un environnement "ouvert" (c'est-à-dire où les parties communiquent par des moyens électroniques sans convention préalable) et des règles par défaut dans un environnement "fermé" (c'est-à-dire où les parties sont liées par des règles et procédures contractuelles préexistantes qu'elles doivent suivre lorsqu'elles communiquent par des moyens électroniques).

II. PROJET DE DISPOSITIONS SUR LES SIGNATURES NUMÉRIQUES, LES AUTRES SIGNATURES ÉLECTRONIQUES, LES AUTORITÉS DE CERTIFICATION ET LES QUESTIONS JURIDIQUES CONNEXES

CHAPITRE PREMIER. CHAMP D'APPLICATION ET DISPOSITIONS GÉNÉRALES

12. Lorsqu'il étudiera le projet de dispositions qu'il est proposé d'inclure dans les Règles uniformes, le Groupe de travail souhaitera peut-être examiner, de manière plus générale, la relation entre ces Règles uniformes et la Loi type. Il voudra peut-être, en particulier, formuler des propositions à la Commission sur la question de savoir si des règles uniformes relatives aux signatures numériques devraient constituer un instrument juridique à part entière où si elles devraient être incorporées dans une version élargie de la Loi type, comme troisième partie, par exemple.

13. Si les Règles uniformes sont conçues comme un instrument séparé, il est proposé qu'elles comprennent des dispositions s'inspirant des articles premier (Champ d'application), 2 a), c) et e) (Définition des termes "message de données", "expéditeur" et "destinataire"), 3 (Interprétation), 7 (Signature) et 13 (Attribution des messages de données) de ladite Loi. Ces articles ne sont pas reproduits dans la présente note, mais on observera que, pour ses travaux, le secrétariat est parti du principe que de telles dispositions feraient partie des Règles uniformes. En ce qui concerne le champ d'application de ces Règles, il faut se rappeler que, compte tenu de l'article premier de la Loi type, les transactions dans lesquelles interviennent des consommateurs, sans être l'élément principal des Règles uniformes, ne seraient pas exclues de leur champ d'application sauf si la loi applicable à ce type de transactions dans l'État adoptant était incompatible avec les Règles uniformes.

14. En ce qui concerne l'autonomie des parties, la simple référence à l'article 4 (Dérogation conventionnelle) de la Loi type, peut ne pas constituer à elle seule une solution satisfaisante, étant donné que cet article établit une distinction entre les dispositions de la Loi type auxquelles il peut être librement dérogé par contrat et celles qui doivent être considérées comme des règles de droit, sauf si la loi applicable en dehors de la Loi type autorise une telle dérogation conventionnelle. En ce qui concerne les signatures électroniques, il est nécessaire, étant donné l'importance pratique des réseaux "fermés", de prévoir une large reconnaissance de l'autonomie des parties. Toutefois, il pourrait aussi être nécessaire de tenir compte des restrictions à la liberté contractuelle liées à l'ordre public, y compris les lois protégeant les consommateurs contre des contrats d'adhésion excessifs. Le Groupe de travail pourrait ainsi souhaiter inclure dans les Règles uniformes une disposition s'inspirant de l'article 4-1 de la Loi type, à savoir que, sauf disposition contraire des Règles uniformes ou d'une autre loi applicable, les signatures électroniques et les certificats qui ont été émis, reçus ou sur lesquels une partie s'est fondée conformément aux procédures convenues entre les parties à une transaction produisent les effets indiqués dans la convention. En outre, le Groupe de travail pourrait envisager d'établir une règle d'interprétation en vertu de laquelle il faudrait, lorsque l'on détermine si un certificat, une signature électronique ou un message de données vérifié par référence

à un certificat est suffisamment fiable pour un objet particulier, tenir compte de toutes les conventions pertinentes liant les parties, toute conduite à laquelle se sont conformées ces dernières et tout usage commercial pertinent.

15. En plus des dispositions susmentionnées, le Groupe de travail souhaitera peut-être examiner la question de savoir si un préambule aux Règles uniformes serait susceptible d'en préciser l'objectif, à savoir promouvoir l'utilisation efficace des communications numériques par la mise en place d'une structure de sécurité et l'affirmation de l'égalité entre les signatures manuscrites et les signatures numériques s'agissant de leur effet juridique.

CHAPITRE II. SIGNATURES ÉLECTRONIQUES

Section I. Signatures électroniques en général

Article premier. Définitions

Aux fins des présentes Règles:

a) Le terme "signature électronique" désigne des données sous forme électronique contenues dans un message de données, ou jointes ou logiquement associées audit message et [pouvant être] utilisées pour [identifier le signataire du message et indiquer qu'il approuve l'information qui y est contenue] [satisfaire aux conditions énoncées au paragraphe 1 a) de l'article 7 de la Loi type de la CNUDCI sur le commerce électronique];

b) Le terme "signature électronique [renforcée] [sécurisée]" désigne une signature électronique qui [est créée et] [dès lors qu'elle a été apposée] peut être vérifiée par l'application d'une procédure de sécurité ou d'une combinaison de procédures de sécurité qui garantit que cette signature électronique:

i) est particulière au signataire [aux fins pour lesquelles] [dans le contexte où] elle est utilisée;

ii) peut être utilisée pour identifier objectivement le signataire du message de données;

iii) a été créée et apposée au message de données par le signataire ou à l'aide d'un moyen dont seul le signataire a le contrôle; [et]

[iv) a été créée et est liée au message de données auquel elle se rapporte d'une manière telle que tout changement apporté audit message apparaîtrait].

c) Variante A

Le terme "signature numérique" désigne une signature électronique créée par transformation d'un message de données à l'aide d'une fonction d'abrégement du message et par cryptage de cette transformation à l'aide d'un système de cryptographie asymétrique utilisant la clef privée du signataire, de manière à ce que toute personne en possession du message de données initial non transformé, de la transformation cryptée et de la clef publique correspondante du signataire puisse déterminer [avec exactitude]:

i) si la transformation a été opérée à l'aide de la clef privée du signataire correspondant à sa clef publique; et

ii) si le message de données initial a été altéré après la transformation.

Variante B

Le terme "signature numérique" désigne une transformation cryptographique (à l'aide d'une technique cryptographique asymétrique) de la représentation numérique d'un message de données, de telle sorte que toute personne en possession du message de données et de la clef publique appropriée puisse déterminer:

i) que la transformation a été opérée à l'aide de la clef privée correspondant à la clef publique appropriée; et

ii) que le message de données n'a pas été altéré après la transformation cryptographique.

d) Le terme "autorité de certification" désigne toute personne ou entité qui, dans le cours de ses affaires, émet des certificats [d'identification] concernant des clefs cryptographiques utilisées pour créer des signatures numériques. [Cette définition s'entend sous réserve de toute loi applicable exigeant qu'une autorité de certification soit agrée ou accréditée ou qu'elle fonctionne d'une manière spécifiée dans ladite loi.]

e) Le terme "certificat" [d'identification] désigne un message de données ou un autre enregistrement émis par une autorité de certification et supposé confirmer l'identité [ou une autre caractéristique importante] d'une personne ou d'une entité détenant une paire de clefs particulière.

f) Le terme "certificat [renforcé] [sécurisé]" désigne un certificat [d'identification] émis pour étayer des signatures électroniques [renforcées] [sécurisées].

g) Le terme "déclaration relative aux pratiques d'authentification" désigne une déclaration publiée par une autorité de certification, qui indique les pratiques suivies par cette autorité pour émettre et traiter de toute autre manière les certificats.

h) Le terme "signataire" désigne la personne par laquelle, ou au nom de laquelle, [une signature électronique est utilisée] [des données sont utilisées comme signature électronique].

Références

A/CN.9/446, par. 27 à 46 (projet d'article premier), 62 à 70 (projet d'article 4), 113 à 131 (projet d'article 8), 132 et 133 (projet d'article 9);
A/CN.9/WG.IV/WP.73, par. 16 à 27, 37 et 38, 50 à 57 et 58 à 60;
A/CN.9/437, par. 29 à 50 et 90 à 113 (projets d'articles A, B et C); et
A/CN.9/WG.IV/WP.71, par. 52 à 60.

Remarques

Définitions des termes "signature électronique" et "signature électronique [renforcée] [sécurisée]"

16. Conformément à la décision prise par le Groupe de travail à sa trente-deuxième session (A/CN.9/446, par. 30), la définition du terme "signature électronique" renvoie à l'article 7 de la Loi type. Il sera peut-être nécessaire de reprendre entièrement les dispositions du paragraphe 1 a) de l'article 7 de cette loi, en fonction de la décision qui sera prise en ce qui concerne la relation entre les Règles uniformes et la Loi type.

17. La distinction entre la notion générale de "signature électronique" et une catégorie plus restreinte (appelée provisoirement signature électronique "renforcée" ou "sécurisée") a été maintenue afin de bien montrer les différences, sur le plan juridique, de ces deux types de procédure. D'un côté, une large gamme de techniques

d'authentification non précisées (dénommées "signatures électroniques") pourraient être reconnues juridiquement comme constituant une signature ayant un sens juridique, à condition de satisfaire au critère de fiabilité énoncé au paragraphe 1b) de l'article 7 de la Loi type, ce qui devrait être établi après l'utilisation de la signature électronique et qui nécessiterait normalement l'intervention d'un juge, d'un arbitre ou d'un autre juge des faits. D'un autre côté, un certain nombre de techniques d'authentification, déterminées par le biais de procédures administratives devant être définies par chacun des États adoptants ou par convention expresse entre les parties, seraient reconnues par avance comme équivalents fonctionnels de signatures manuscrites.

Définition du terme "signature numérique"

18. La catégorie des "signatures numériques" n'est pas définie comme une sous-catégorie des signatures électroniques "renforcées". En effet, si dans la plupart des cas ce sont des techniques "numériques" (avec ou sans recours à des autorités de certification) qui seraient utilisées pour obtenir les effets juridiques envisagés pour la catégorie des signatures électroniques plus "sécurisées", de telles techniques pourraient aussi être employées dans un contexte moins spécifique. La définition du terme "signature numérique" vise donc à faire ressortir l'approche techniquement neutre adoptée dans les Règles uniformes.

Définition du terme "autorité de certification"

19. Les Règles uniformes ne contiennent aucune condition quant aux normes que les autorités de certification doivent respecter avant de pouvoir mener leur activité. La question avait été examinée par le Groupe de travail à des sessions antérieures et traitée également dans le projet d'article 19. S'il est jugé nécessaire de donner des indications aux États adoptants, soit dans le texte des Règles uniformes soit dans un guide, l'exemple suivant de disposition pourrait être pris en considération:

Les autorités de certification doivent:

a) être suffisamment fiables pour offrir des services de certification;

b) employer un personnel possédant les connaissances spécialisées, l'expérience et les qualifications nécessaires pour fournir les services offerts;

c) utiliser des systèmes fiables ainsi que du matériel et des logiciels généralement reconnus correspondant au type de service et au niveau de sécurité offerts;

d) posséder des ressources financières suffisantes pour pouvoir se conformer aux [présentes Règles];

e) conserver toutes les informations pertinentes enregistrées concernant un certificat [renforcé] [sécurisé] pendant une période appropriée, en particulier pour être en mesure de fournir des preuves de la certification dans une instance. Ce type d'enregistrement peut être fait par des moyens électroniques;

f) publier toutes les informations pertinentes concernant le recours adéquat et sûr aux services de certification et établir des procédures pour apaiser les griefs et régler les litiges; et

g) publier, en ce qui concerne les services offerts au public, toutes les informations pertinentes concernant les procédures appliquées et les pratiques suivies, les clauses des contrats, en particulier les obligations contractées en matière de responsabilité, ainsi que les procédures appliquées pour apaiser les griefs et régler les litiges; les publications sont dûment et facilement accessibles.

Définitions des termes "certificat [d'identification]" et "certificat [renforcé] [sécurisé]"

20. Les définitions figurant aux alinéas e) et f) sont fondées sur la suggestion faite à la trente-deuxième session du Groupe de travail, selon laquelle il conviendrait de distinguer les cas où les signatures numériques sont utilisées aux fins d'opérations commerciales internationales avec l'intention de signer (c'est-à-dire d'identifier le signataire et de rattacher le signataire à l'information signée) et les autres utilisations de ces signatures (par exemple pour déterminer les pouvoirs d'une personne ("certificat de pouvoirs") (voir A/CN.9/446, par. 72). Si les dispositions figurant au chapitre III des Règles uniformes traitent en grande partie des techniques de signature numérique comme moyen d'établir une équivalence prédéterminée avec les signatures manuscrites, le Groupe de travail pourrait néanmoins souhaiter examiner dans quelle mesure ces techniques devraient être traitées dans d'autres contextes. Si les Règles uniformes sont axées sur les signatures numériques en tant qu'équivalents des signatures manuscrites, il n'est peut-être pas nécessaire d'établir une distinction entre les "certificats", les "certificats d'identification" et les "certificats [renforcés] [sécurisés]". On se rappellera que toute utilisation de signatures numériques offrant un niveau de sécurité plus faible pourrait être également traitée dans les dispositions générales du projet d'article 2.

Article 2. Effet de la signature électronique

1. Pour ce qui est d'un message de données authentifié à l'aide d'une signature électronique [autre qu'une signature électronique sécurisée], cette signature satisfait à toute exigence légale concernant une signature si sa fiabilité est suffisante au regard de l'objet pour lequel elle a été utilisée, compte tenu de toutes les circonstances, y compris tout accord en la matière.

2. Le paragraphe 1 s'applique, que l'exigence légale qui y est visée ait la forme d'une obligation ou que la loi prévoie simplement certaines conséquences s'il n'y a pas de signature.

3. Sauf disposition contraire énoncée expressément dans [les présentes Règles], les signatures électroniques qui ne sont pas des signatures électroniques [renforcées] [sécurisées] ne sont pas soumises à la réglementation aux normes ou aux procédures d'octroi de licences établies par ... *[les organes ou autorités indiqués par l'État dans l'article]* ou aux présomptions créées par les articles 4, 5 et 6.

4. Les dispositions du présent article ne s'appliquent pas dans les situations suivantes: [...]

Référence

A/CN.9/446, par. 27 à 46 (projet d'article premier).

Remarques

21. Le projet d'article 2 a pour objet de traiter les effets juridiques des signatures électroniques qui ne satisfont pas aux exigences définies pour la reconnaissance de leur caractère "renforcé" ou "sécurisé". Conformément au mandat donné par la Commission et compte tenu des vues exprimées à la trente-deuxième session du Groupe de travail (voir A/CN.9/446, par. 4 et 45), le projet d'article a pour objectif d'assurer la neutralité des Règles uniformes quant aux techniques utilisées, de bien préciser que l'utilisation de techniques d'authentification offrant une faible sécurité n'est pas interdite et de prévoir une reconnaissance appropriée de l'autonomie des parties, sans autoriser ces dernières à déroger aux règles de droit impératives relatives aux signatures. Les paragraphes 1, 2 et 4 reprennent simplement les dispositions de l'article 7 de la Loi type. Le paragraphe 3 a pour but d'établir une distinction entre les effets juridiques des signatures électroniques en général, et les techniques d'authentification "renforcées" ou "sécurisées".

Section II. Signatures électroniques [renforcées] [sécurisées]

Article 3. Présomption de signature

1. Un message de données est présumé avoir été signé [si] [à partir du moment où] une signature électronique [renforcée] [sécurisée] y est apposée.

2. Les dispositions du présent article ne s'appliquent pas dans les situations suivantes: [...].

Références

A/CN.9/446, par. 47 et 48 (projet d'article 2) et 49 à 61 (projet d'article 3);
A/CN.9/WG.IV/WP.73, par. 28 à 36; et
A/CN.9/437, par. 43, 48 et 92.

Remarques

22. Le projet d'article créant la présomption qu'un message de données doit être considéré comme "signé" s'il est authentifié par une signature électronique sécurisée a été remanié à la suite d'une vue exprimée à la trente-deuxième session selon laquelle la relation entre la définition d'une signature électronique sécurisée et les présomptions découlant de l'utilisation d'une telle signature devait être précisée (voir A/CN.9/446, par. 34).

23. Les Règles uniformes ne contiennent aucune définition du terme "signature" ni aucune indication des effets juridiques précis d'une telle "signature". En vertu du projet d'article 3, l'effet juridique d'une signature doit être déterminé par référence au droit interne, en dehors des Règles uniformes.

Article 4. Présomption d'attribution

1. Une signature électronique [renforcée] est réputée être celle de la personne par qui, ou au nom de laquelle, elle est supposée avoir été utilisée,

Variante A sauf si le signataire supposé établit que la signature électronique [renforcée] [sécurisée] a été apposée sans autorisation.

Variante B à condition que la partie se fiant à la signature établisse que la procédure de sécurité ou la combinaison de procédures de sécurité appliqué pour vérifier la signature

a) était commercialement raisonnable eu égard aux circonstances;

b) qu'elle l'avait appliquée de manière fiable, et

c) qu'elle s'y était fiée de manière raisonnable et de bonne foi.

2. Les dispositions du présent article ne s'appliquent pas dans les situations suivantes: [...].

Références

A/CN.9/446, par. 49 à 61 (projet d'article 3);
A/CN.9/WG.IV/WP.73, par. 33 à 36;
A/CN.9/437, par. 118 à 124 (projet d'article E); et
A/CN.9/WG.IV/WP.71, par. 64 et 65.

Remarques

24. La variante A porte sur l'attribution d'une signature électronique par l'allocation de la charge de la preuve selon les conditions proposées à la trente-deuxième session du Groupe de travail (voir A/CN.9/446, par. 60). En vertu de la variante B, c'est à la partie se fiant à la signature d'assumer la charge de la preuve.

Article 5. Présomption d'intégrité

1. Si le signataire supposé a utilisé une procédure de sécurité capable de prouver [de manière fiable] qu'un message de données ou toute signature [électronique] [électronique [renforcée] [sécurisée]] y étant apposée n'a pas été modifié après l'application de la procédure de sécurité audit message de données ou à toute signature, il est présumé [sauf preuve contraire] que le message de données ou la signature n'a pas été modifié.

2. Les dispositions du présent article ne s'appliquent pas dans les situations suivantes: [...].

Références

A/CN.9/446, par. 47 et 48 (projet d'article 2);
A/CN.9/WG.IV/WP.73, par. 28 à 32; et
A/CN.9/437, par. 43, 48 et 92.

Remarques

25. Dans le précédent projet de Règles uniformes, il était indiqué que la vérification de l'intégrité du message de données constituait un élément de la définition d'une "signature électronique sécurisée". On a porté à l'attention du secrétariat le fait que la vérification de l'intégrité du message de données pouvait être effectuée par des procédures séparées. En outre, on peut concevoir que certaines techniques d'authentification permettent d'obtenir le niveau élevé de sécurité requis dans la définition des signatures électroniques "renforcées" sans qu'il soit nécessaire de vérifier l'intégrité du message de données.

26. Si le Groupe de travail le juge plus approprié, les dispositions des projets d'articles 3, 4 et 5 pourraient être reformulées de manière à établir des effets juridiques au lieu de présomptions.

Article 6. Prédétermination de la signature électronique [renforcée] [sécurisée]

1. Une procédure de sécurité ou une combinaison de procédures de sécurité satisfait aux exigences d'une signature électronique [renforcée] [sécurisée] si *[l'organe ou l'autorité indiqué par l'État adoptant comme compétent en la matière]* en décide ainsi...

2. Pour ce qui est de la relation entre la personne signant un message de données et toute personne se fiant au message signé, une procédure de sécurité ou une combinaison de procédures de sécurité est supposée satisfaire aux exigences d'une signature électronique [renforcée] [sécurisée] si les parties en conviennent expressément.

3. Les dispositions du paragraphe 2 ne s'applique pas dans les situations suivantes: [...].

Références

A/CN.9/446, par. 37 à 45 (projet d'article premier); et
A/CN.9/WG.IV/WP.73, par. 27.

Remarques

27. Contrairement aux "signatures électroniques" ne remplissant pas les conditions requises, qui sont traitées au projet d'article 2, les signatures électroniques [renforcées] [sécurisées] traitées au projet d'article 6 présentent l'avantage de donner aux parties commerciales, soit par application de la réglementation applicable, soit directement par contrat, l'assurance, avant même l'utilisation d'une technique de signature donnée, que cette technique produira des effets juridiques. Le Groupe de travail souhaitera peut-être examiner la question de savoir si les limites de l'autonomie des parties à cet égard doivent être traitées dans les Règles uniformes ou simplement dans le droit interne au titre du paragraphe 3. (Voir ci-dessus par. 4).

Article 7. Responsabilité pour une signature électronique [renforcée] [sécurisée]

Variante A

Lorsque l'utilisation d'une signature électronique [renforcée] [sécurisée] n'a pas été autorisée et lorsque le signataire supposé n'a pas exercé un soin raisonnable pour en éviter une utilisation non autorisée et pour empêcher que le destinataire ne s'y fie, le signataire supposé est tenu responsable du préjudice causé [et doit verser des dommages-intérêts à la partie s'étant fiée à sa signature], sauf si la partie s'étant fiée à la signature savait ou aurait dû savoir qu'elle n'était pas celle du signataire supposé.

Variante B

Lorsque l'utilisation d'une signature électronique [renforcée] [sécurisée] n'a pas été autorisée et que le signataire supposé n'a pas exercé un soin raisonnable pour en éviter l'utilisation non autorisée et empêcher que le destinataire ne s'y fie, ladite signature est néanmoins considérée comme la sienne, sauf si la partie qui s'y est fiée savait ou aurait dû savoir qu'elle n'était pas celle du signataire supposé.

Référence

A/CN.9/446, par. 49 à 61 (projet d'article 3);
A/CN.9/WG.IV/WP.73, par. 33 à 36;
A/CN.9/437, par. 118 à 124 (projet d'article E); et
A/CN.9/WG.IV/WP.71, par. 64 et 65.

Remarques

28. À sa trente-deuxième session, le Groupe de travail a examiné la question de savoir si les Règles uniformes devaient traiter uniquement de l'attribution des signatures électroniques sécurisées (ou signatures numériques) ou si elles devaient également porter sur la responsabilité du signataire supposé envers les parties se fiant à sa signature. Il a été souligné que les Règles uniformes devraient, en établissant le lien entre la signature électronique et le signataire supposé, encourager également l'utilisation des signatures numériques en répartissant comme il convenait les responsabilités en cas de préjudice subi par une partie se fiant à la signature, lorsque le signataire supposé n'avait pas exercé un soin raisonnable et évité une utilisation non autorisée de sa signature (voir A/CN.9/446, par. 51).

29. Le Groupe de travail souhaitera peut-être examiner le lien entre les Règles uniformes et l'article 13 de la Loi type. Ce dernier traite de l'attribution du message de données alors que la question de l'attribution d'une signature électronique est traitée dans la définition de la "signature électronique [renforcée] [sécurisée]" et dans le projet d'article 4.

30. La variante A limite la responsabilité du signataire supposé à l'indemnisation de la partie s'étant fiée à sa signature pour le préjudice prouvé, ce qui peut être calculé sur une base contractuelle ou extracontractuelle, en fonction des circonstances. La variante B rend le signataire supposé responsable de la teneur du message de données.

Section III. Signatures numériques accompagnées de certificats

Article 8. Teneur d'un certificat [renforcé] [sécurisé]

Aux fins des présentes Règles, un certificat [renforcé] [sécurisé] remplit au minimum les fonctions suivantes:

a) il identifie l'autorité de certification qui l'émet;

b) il nomme ou identifie le [signataire] [sujet du certificat] ou un dispositif ou un agent électronique sous le contrôle [du signataire] [du sujet du certificat] [de cette personne];

c) il contient une clef publique correspondant à une clef privée dont [le signataire] [sujet du certificat] a le contrôle;

d) il spécifie sa période d'effet;

e) il est signé numériquement ou sécurisé d'une autre manière par l'autorité de certification qui l'émet;

[f) il spécifie, le cas échéant, les restrictions à l'utilisation de la clef publique;] [et]

[g) il identifie l'algorithme à appliquer].

Références

A/CN.9/446, par. 113 à 131 (projet d'article 8);
A/CN.9/WG.IV/WP.73, par. 50 à 57;
A/CN.9/437, par. 98 à 113 (projet d'article C); et
A/CN.9/WG.IV/WP.71, par. 18 à 45 et 59 et 60.

Remarques

31. À sa trente-deuxième session, le Groupe de travail n'a pas pris de décision quant à la question de savoir si, sur le plan rédactionnel, il faudrait employer dans les Règles uniformes les termes le "sujet du certificat" ou spécifier que le sujet doit être une "personne". Pour rendre les Règles uniformes plus lisibles, on a employé systématiquement le terme "signataire", le terme "sujet" ayant été maintenu également à des fins de comparaison. Les Règles uniformes pourraient certes contenir une référence à la notion de "personne", mais il faudrait alors remanier considérablement le texte pour éviter toute ambiguïté quant à la personne visée. Il est indiqué dans la définition du terme "signataire" au paragraphe h) du projet d'article premier que le signataire doit être une "personne".

Article 9. Effet des signatures numériques accompagnées de certificats

1. Pour ce qui est de la totalité ou de toute partie d'un message de données, où l'expéditeur est identifié par une signature numérique, ladite signature [est une signature électronique [renforcée] [sécurisée]] [satisfait aux conditions de l'article 7 de la Loi type de la CNUDCI sur le commerce électronique] si:

a) elle a été créée de manière sûre pendant la période d'effet d'un certificat valide et est vérifiée de manière sûre par référence à la clef publique indiquée dans le certificat; et

b) le certificat rattache une clef publique à l'identité [du signataire] [d'une personne] pour les raisons suivantes:

i) le certificat a été émis par une autorité de certification agréée par ... *[l'État adoptant indique l'organe ou l'autorité ayant pouvoir d'agréer les autorités de certification et de promulguer des règles concernant les fonctions des autorités de certification agréées]*; ou

ii) le certificat a été émis par une autorité de certification habilitée par un organe d'habilitation responsable appliquant des normes commercialement appropriées et internationalement reconnues concernant la fiabilité de la technologie, des pratiques et d'autres caractéristiques pertinentes de l'autorité de certification. Une liste non exclusive des organes ou normes conformes au présent paragraphe peut être publiée par ... *[l'État adoptant indique l'organe ou l'autorité ayant pouvoir d'émettre des normes reconnues concernant les fonctions des autorités de certification agréées]*; ou

iii) le certificat a été émis de toute autre manière conformément à des normes commercialement appropriées et internationalement reconnues [.] [; ou]

[iv) des preuves suffisantes font apparaître que le certificat rattache [avec précision] la clef publique à l'identité du [signataire] [sujet].]

[2. Lorsqu'un message de données est signé à l'aide d'une signature numérique [créée pendant la période d'effet d'un certificat] qui ne satisfait pas aux conditions énoncées au paragraphe 1), cette signature est considérée comme une signature électronique [renforcée] [sécurisée] s'il existe des preuves suffisantes montrant que [le certificat] rattache avec précision la clef publique à l'identité du [signataire] [sujet du certificat].]

3. Les dispositions de présent article ne s'appliquent pas dans les situations suivantes: [...].

Références

A/CN.9/446, par. 71 à 84 (projet d'article 5);
A/CN.9/WG.IV/WP.73, par. 39 à 44; et
A/CN.9/437, par. 43, 48 et 92.

Remarques

32. Le chapeau du paragraphe 1 tient compte de la décision prise par le Groupe de travail à sa trente-deuxième session (voir A/CN.9/446, par. 76).

33. Correctement appliquées, les signatures numériques devraient constituer des signatures électroniques sécurisées. Mais encore faut-il déterminer quand une signature numérique a été appliquée d'une manière qui

permette de la qualifier de sécurisée. Toutes les signatures numériques vérifiables par référence à un certificat ne sont pas sécurisées, en particulier lorsque l'on n'est pas certain que l'identification ou l'authentification du signataire ou de la clef publique soient exactes. Pour déterminer si une signature numérique est sécurisée, il est fondamental de savoir: 1) si l'autorité de certification a correctement identifié le signataire; 2) si l'autorité de certification a correctement authentifié la clef publique du signataire; 3) si la clef privée du signataire a été compromise; et 4) si le processus est fiable (par exemple, si l'algorithme de la clef publique et sa longueur sont appropriés).

34. Le paragraphe 1 énonce deux critères fondamentaux pour déterminer quand une signature numérique peut être considérée comme une signature électronique sécurisée. Selon le premier, la signature doit être créée pendant la période d'effet d'un certificat valide et être vérifiée par référence à la clef publique indiquée dans le certificat. La période d'effet d'un certificat commence normalement lors de son émission et se termine soit à son expiration, soit à son annulation ou à sa suspension, selon lequel de ces trois événements se produit en premier.

35. Selon le deuxième critère, il faut garantir que le certificat lui-même identifie avec précision une personne comme le signataire par rapport à une clef privée correspondant à la clef publique indiquée dans le certificat. Il est possible d'évaluer la fiabilité du certificat par référence à des normes, procédures et autres règles spécifiées par les autorités reconnues de l'État adoptant. Ces normes peuvent être établies par l'habilitation des autorités de certification par des tiers, par leur obtention volontaire d'une licence ou l'application obligatoire de règles établies par l'État adoptant.

36. Par ailleurs, au titre du paragraphe 2, si un tribunal ou un autre juge des faits met en évidence le fait que l'information donnée dans le certificat est effectivement véridique, la fiabilité dudit certificat est alors manifeste. À ce stade, toutefois, le juge des faits est tenu de déterminer au cas par cas si le certificat a été émis par une autorité de certification ayant correctement identifié le signataire et authentifié sa clef publique.

37. Conformément à "l'approche duale" adoptée par le Groupe de travail, le projet d'article 9 vise à donner autant de latitude que possible pour déterminer la fiabilité d'un certificat émis par une autorité de certification. Cette souplesse est particulièrement importante du fait que l'emploi des signatures numériques est encore récent et que les modèles pour cet emploi ainsi que pour la réglementation ne sont pas encore bien établis. Il importe donc de faciliter une utilisation accrue des signatures numériques dans le commerce électronique, tout en établissant les normes nécessaires pour déterminer par présomption la fiabilité d'un message signé numériquement.

38. Il est également important de noter que si l'une des options énoncées dans le projet d'article 9 comprend une détermination judiciaire de l'exactitude d'un certificat, l'autre option par contre présume cette exactitude si le certificat a été émis par l'autorité de certification agréée par l'État adoptant ou s'il répond de toute autre manière à certaines normes établies par ledit État. Dans ce dernier cas, il n'est pas nécessaire d'établir par des moyens judiciaires l'exactitude de la signature électronique pour que celle-ci soit considérée comme sécurisée. La deuxième option peut être utile pour les personnes ayant recours au commerce électronique, qui sauraient ainsi, avant de prendre des mesures sur la foi d'une communication, si une telle mesure peut avoir force exécutoire. Toutefois, la présomption d'exactitude peut être contestée s'il est démontré qu'un certificat émis par une autorité de certification agréée n'est, en fait, ni exact ni fiable (voir A/CN.9/WG.IV/WP.73, par. 39 à 44).

CHAPITRE III. AUTORITÉS DE CERTIFICATION ET QUESTIONS CONNEXES

Article 10. Garanties données au moment de l'émission d'un certificat

1. Lorsqu'elle émet un certificat, l'autorité de certification garantit [à toute personne qui se fie raisonnablement à ce certificat]:

a) qu'elle s'est conformée à toutes les conditions applicables [prévues dans les présentes Règles];

b) que toutes les informations données dans le certificat sont exactes à la date de son émission, [sauf si l'autorité de certification a déclaré dans le certificat que l'exactitude de certaines informations n'est pas confirmée];

c) qu'à sa connaissance, n'a été omis du certificat aucun fait matériel connu qui compromettrait la fiabilité des informations y étant contenues; et

[d) que si elle a publié une déclaration relative aux pratiques d'authentification, elle s'est conformée à cette déclaration pour l'émission du certificat.]

2. Lorsqu'elle émet un certificat [renforcé] [sécurisé], l'autorité de certification garantit également, en ce qui concerne [le signataire] [le sujet] indiqué dans le certificat, [à toute personne qui se fie raisonnablement au certificat]:

a) que la clef publique et la clef privée du [signataire] [sujet] indiquées dans le certificat constituent une paire de clefs opérationnelle, et

b) qu'à la date de l'émission du certificat, la clef privée:

i) est celle du [signataire] [sujet] indiqué dans le certificat; et

ii) correspond à la clef publique donnée dans le certificat.

Références

A/CN.446, par. 134 à 145 (projet d'article 10);
A/CN.9/WG.IV/WP.73, par. 61 à 63;
A/CN.9/437, par. 51 à 73 (projet d'article H); et
A/CN.9/WG.IV/WP.71, par. 70 à 72.

Remarques

39. Le projet d'article 10 est fondé sur une distinction entre les certificats [renforcés] [sécurisés] et une catégorie plus large de certificats. Le maintien de cette distinction dépendra de la décision que prendra le Groupe de travail concernant la mesure dans laquelle les Règles uniformes devraient traiter les signatures numériques utilisées à des fins autres que l'établissement d'une équivalence prédéterminée avec des signatures manuscrites (voir ci-dessus par. 20).

Article 11. Responsabilité contractuelle

Variante A

1. Entre une autorité de certification émettant un certificat et le détenteur de ce certificat [ou toute autre partie se fiant au certificat, qui a une relation contractuelle avec l'autorité de certification], les droits et obligations des parties [et toute restriction à cet égard] sont déterminés par convention [sous réserve de la loi applicable].

[2. Sous réserve de l'article 10, une autorité de certification peut, par convention, s'exonérer de sa responsabilité en cas de préjudice [dû au fait qu'une personne s'est fiée au certificat] [dû à des erreurs dans les informations contenues dans le certificat, à des défaillances techniques ou à d'autres circonstances de même nature. Toutefois, la clause limitant ou excluant la responsabilité de l'autorité de certification ne peut être invoquée dans le cas où l'exclusion ou la limitation de la responsabilité contractuelle serait manifestement inéquitable eu égard à l'objet du contrat].]

[3. L'autorité de certification n'est pas autorisée à limiter sa responsabilité s'il est prouvé que le préjudice a résulté d'un acte ou omission de ladite autorité agissant avec l'intention de causer un préjudice ou témérairement et en sachant qu'un préjudice pourrait en résulter.]

Variante B

Conformément à la loi applicable, les droits et obligations d'une autorité de certification, d'un [signataire] [sujet] indiqué dans un certificat, et de toute autre partie sont régis par la ou les conventions conclues par ces parties dans la mesure où ces conventions traitent de ces droits et obligations et de toute restriction à cet égard.

Variante C

Lorsqu'une autorité de certification, un [signataire] [sujet] identifié dans le certificat, ou toute autre partie, concluent des conventions, les droits et obligations de ces parties, et toute restriction à cet égard, visés dans les conventions sont régis par ces dernières conformément à la loi applicable et dans la mesure permise par elle.

Références

A/CN.9/446, par. 146 à 154 (projet d'article 11);
A/CN.9/WG.IV/WP.73, par. 64 et 65;
A/CN.9/437, par. 51 à 73 (projet d'article H); et
A/CN.9/WG.IV/WP.71, par. 70 à 72

Remarques

40. Avant d'étudier les différentes variantes proposées pour le projet d'article 11, le Groupe de travail pourrait souhaiter examiner la question de savoir si cet article doit être conservé dans les Règles uniformes. À la trente-deuxième session du Groupe, il a été déclaré qu'il portait sur des questions qui seraient mieux traitées dans le contrat ou la loi applicable. En particulier, on a fait observer qu'il n'était peut-être pas nécessaire d'énoncer à nouveau le principe de l'autonomie des parties, qui était déjà exposé à l'article 4 de la Loi type, et que d'autres points traités dans le projet d'article empiétaient sur la législation nationale pour des questions pouvant ne pas se prêter à une unification. On a estimé que le fait de traiter les questions de la responsabilité contractuelle dans le contrat et dans la loi applicable en dehors des Règles uniformes était une alternative acceptable, mais, selon l'avis qui a prévalu, il valait la peine de tenter d'établir une certaine unification sur cette question importante (voir A/CN.9/446, par. 148).

Article 12. Responsabilité de l'autorité de certification envers les parties se fiant au certificat

1. Sous réserve des dispositions du paragraphe 2, lorsqu'une autorité de certification émet un certificat, elle est responsable envers toute personne se fiant raisonnablement à ce certificat :

a) des erreurs y figurant, sauf si elle prouve qu'elle ou ses agents ont pris [toutes] les mesures [raisonnables] [commercialement raisonnables] [qui étaient appropriées compte tenu de l'objet pour lequel le certificat avait été émis, au vu de toutes les circonstances] pour éviter des erreurs dans le certificat;

b) du non-enregistrement de l'annulation du certificat, sauf si elle prouve qu'elle ou ses agents ont pris [toutes] les mesures [raisonnables] [commercialement raisonnables] [qui étaient appropriées compte tenu de l'objet pour lequel le certificat avait été émis, au vu de toutes les circonstances] pour enregistrer l'annulation promptement après réception de l'avis d'annulation[; et

c) des conséquences imputables au non-respect :

i) de toute procédure énoncée dans la déclaration relative aux pratiques d'authentification publiée par l'autorité de certification; ou

ii) de toute procédure énoncée dans la loi applicable].

2. Il n'est pas raisonnable de se fier à un certificat dans la mesure où cela est contraire aux informations contenues [ou incorporées par référence] dans ledit certificat [ou dans une liste d'annulation] [ou dans les informations relatives à l'annulation]. [Il n'est pas raisonnable en particulier de se fier au certificat si :

a) cela est contraire à l'objet pour lequel le certificat a été émis;

b) il y a dépassement de la valeur pour laquelle le certificat est valide; ou

c) [...].]"

Références

A/CN.9/446, par. 155 à 173 (projet d'article 12);
A/CN.9/WG.IV/WP.73, par. 66 et 67;
A/CN.9/437, par. 51 à 73 (projet d'article H); et
A/CN.9/WG.IV/WP.71, par. 70 à 72

Remarques

41. Le projet d'article 12 reflète la décision prise par le Groupe de travail à sa trente-deuxième session (A/CN.9/446, par. 173). À cette session, une opinion a été exprimée selon laquelle le projet d'article 12 devrait s'appliquer uniquement aux autorités de certification émettant des certificats d'identification.

Remarque générale concernant les projets d'articles 13 à 16

42. À sa précédente session, le Groupe de travail a, faute de temps, reporté l'examen des projets d'articles 13 à 16 à une future session (voir A/CN.9/446, par. 174). Sauf pour ce qui est de la mise en forme visant essentiellement à assurer la cohérence des diverses dispositions incluses dans le texte révisé des Règles uniformes,

le texte des articles 13 à 16 figurant dans la présente note est, quant au fond, identique au texte figurant dans le document A/CN.9/WG.IV/WP.73.

Article 13. Annulation d'un certificat

1. Pendant la période d'effet d'un certificat, l'autorité de certification qui l'a émis doit l'annuler conformément aux politiques et procédures régissant l'annulation énoncées dans la déclaration applicable relative aux pratiques d'authentification ou, en l'absence de telles politiques et procédures, promptement après:

a) réception d'une demande d'annulation par le [signataire] [sujet] indiqué dans le certificat, et confirmation que la personne demandant l'annulation en est le [signataire] [sujet] [légitime], ou est un agent du [signataire] [sujet] habilité à demander l'annulation;

b) réception d'une preuve fiable du décès du [signataire] [sujet] si ce dernier est une personne physique; ou

c) réception d'une preuve fiable que le [signataire] [sujet] a été dissous ou a cessé d'exister, lorsqu'il s'agit d'une personne morale.

2. Le [signataire] [sujet] titulaire d'une paire de clefs certifiée est tenu d'annuler le certificat correspondant ou d'en demander l'annulation lorsqu'il sait que la clef privée a été perdue, compromise ou risque d'être utilisée à mauvais escient à d'autres égards. Si le [signataire] [sujet] n'annule pas le certificat dans un tel cas, il est responsable de tout préjudice encouru par une personne s'étant fiée à un message du fait qu'il a failli à son obligation d'annuler le certificat.

3. Que le [signataire] [sujet] indiqué dans le certificat consente ou non à l'annulation, l'autorité de certification qui a émis le certificat doit l'annuler rapidement après avoir appris:

a) qu'un fait matériel présenté dans le certificat est faux;

b) que la clef privée ou le système informatique de l'autorité de certification a été compromis d'une manière qui compromet la fiabilité du certificat; ou

c) que la clef privée ou le système informatique du [signataire] [sujet] a été compromis.

3. Lors de l'annulation d'un certificat en vertu du paragraphe 3, l'autorité de certification doit aviser le [signataire] [sujet] et les parties se fiant au certificat conformément aux politiques et aux procédures qui régissent la notification des annulations énoncées dans la déclaration applicable relative aux pratiques d'authentification ou, en l'absence de telles politiques et procédures, il doit aviser rapidement le [signataire] [sujet] et publier dans les meilleurs délais un avis d'annulation si le certificat a été publié, et en informer par ailleurs, sur demande, toute partie s'étant fiée au certificat.

4. [Entre le [signataire] [sujet] et l'autorité de certification,] l'annulation prend effet à partir du moment où elle est [reçue] [enregistrée] par l'autorité de certification.

[5. Entre l'autorité de certification et toute autre partie se fiant au certificat, l'annulation prend effet à partir du moment où elle est [enregistrée] [publiée] par l'autorité de certification.]

Références

A/CN.9/446, par. 174 (projet d'article 13);
A/CN.9/WG.IV/WP.73, par. 68;
A/CN.9/437, par. 125 à 139 (projet d'article F); et
A/CN.9/WG.IV/WP.71, par. 66 et 67.

Remarques

43. Le projet d'article 13 tient compte des différentes vues exprimées à la trente et unième session du Groupe de travail en énonçant une norme par défaut régissant l'annulation des certificats. Toutefois, une autorité de certification peut à tout moment contourner la norme par défaut en établissant dans la déclaration relative à ses pratiques d'authentification des procédures qui régissent l'annulation et en les appliquant. En ce qui concerne le moment auquel l'annulation prend effet, le Groupe de travail pourrait souhaiter prendre une décision quant à la nécessité d'établir une distinction entre la situation du signataire et celle de toute autre partie se fondant sur le certificat (voir A/CN.9/437, par. 130).

Article 14. Suspension d'un certificat

Pendant la période d'effet d'un certificat, l'autorité de certification l'ayant émis doit le suspendre conformément aux politiques et procédures régissant la suspension énoncées dans la déclaration applicable relative aux pratiques d'authentification ou, en l'absence de telles politiques et procédures, dans les meilleurs délais après réception d'une demande à cet effet émanant d'une personne dont l'autorité de certification peut raisonnablement penser qu'elle est le [signataire] [sujet] désigné dans le certificat ou une personne autorisée à agir en son nom.

Références

A/CN.9/446, par. 174 (projet d'article 14);
A/CN.9/WG.IV/WP.73, par. 69; et
A/CN.9/437, par. 133 à 135 (projet d'article F).

Remarques

44. À sa trente et unième session, le Groupe de travail a décidé que les Règles uniformes devaient contenir une disposition sur la suspension des certificats (voir A/CN.9/437, par. 133 et 134). En ce qui concerne le moment où une suspension prend effet, il pourra souhaiter décider s'il est nécessaire d'ajouter des dispositions s'inspirant des paragraphes 4 et 5 du projet d'article 13.

Article 15. Registre des certificats

1. L'autorité de certification tient un registre électronique des certificats émis accessible au public et indiquant la date d'expiration de chaque certificat, ou la date de suspension ou d'annulation.

2. Le registre est tenu par l'autorité de certification

Variante A pendant au moins [30] [10] [5] ans

Variante B pendant ... [*l'État adoptant spécifie la période pendant laquelle les renseignements pertinents doivent être conservés dans le registre*]

à compter de la date d'annulation ou d'expiration de la période d'effet de tout certificat émis par l'autorité de certification.

Variante C conformément aux politiques et procédures spécifiées par l'autorité de certification dans la déclaration applicable relative aux pratiques d'authentification.

Référence

A/CN.9/446, par. 174 (projet d'article 15);
A/CN.9/WG.IV/WP.73, par. 70 et 71;
A/CN.9/437, par. 140 à 148 (projet d'article G); et
A/CN.9/WG.IV/WP.71, par. 68 et 69.

Remarques

45. À la trente et unième session, aucune objection de principe n'a été soulevée contre l'inclusion dans les Règles uniformes d'une disposition concernant l'inscription des certificats dans un registre (voir A/CN.9/437, par. 142). La bonne tenue d'un registre largement accessible (parfois appelé "*depositary*") comprenant en particulier une liste des annulations de certificats peut être considérée comme un élément important de la fiabilité des signatures numériques. En ce qui concerne la façon dont les autorités de certification devraient tenir ces registres et ces listes, le Groupe de travail pourrait souhaiter examiner la question de savoir si les parties devraient être tenues de vérifier la situation du certificat en consultant le registre ou la liste pertinente avant de se fonder sur sa validité.

46. Plus généralement, le Groupe de travail souhaitera peut-être étudier si les Règles uniformes, en établissant des règles minima concernant les activités des autorités de certification, devraient traiter également les droits et obligations des parties se fiant aux certificats.

Article 16. Relations entre les parties se fiant aux certificats et l'autorité de certification

[1. Une autorité de certification n'est autorisée à demander que les renseignements qui lui sont nécessaires pour identifier l'utilisateur.

2. Sur demande, l'autorité de certification divulgue les renseignements suivants:

a) les conditions dans lesquelles le certificat peut être utilisé;

b) les conditions déterminant l'utilisation des signatures numériques;

c) le coût des services fournis par l'autorité de certification;

d) la politique ou les pratiques de l'autorité de certification concernant l'utilisation, la conservation et la communication de renseignements d'ordre personnel;

e) les prescriptions techniques de l'autorité de certification concernant le matériel de communication devant être utilisé par les parties se fiant aux certificats;

f) les conditions dans lesquelles l'autorité de certification met en garde les parties se fiant aux certificats en cas d'irrégularité ou de défaut de fonctionnement du matériel de communication;

g) toute limite de la responsabilité de l'autorité de certification;

h) toutes restrictions imposées par l'autorité de certification à l'utilisation du certificat;

i) les conditions dans lesquelles le [signataire] [sujet] est autorisé à restreindre l'utilisation du certificat.

3. Les renseignements énumérés au paragraphe 1 sont communiqués au [signataire] [sujet] potentiel avant la conclusion définitive d'un accord de certification. Ces renseignements peuvent être communiqués par l'autorité de certification dans le cadre d'une déclaration relative aux pratiques d'authentification.

4. Avec préavis [d'un mois], le [signataire] [sujet] peut mettre fin à l'accord établissant une connexion avec l'autorité de certification. L'avis prend effet dès qu'il est reçu par l'autorité de certification.

5. Avec préavis [de trois mois], l'autorité de certification peut mettre fin à l'accord établissant une connexion avec elle. L'avis prend effet dès qu'il est reçu.]

Références

A/CN.9/446, par. 174 (projet d'article 16);
A/CN.9/WG.IV/WP.73, par. 72;
A/CN.9/437, par. 149 et 150 (projet d'article J); et
A/CN.9/WG.IV/WP.71, par. 76.

Remarques

47. À sa trente et unième session, le Groupe de travail a noté que les divers éléments énumérés dans le projet d'article 15 devraient être placés entre crochets, pour être examinés à un stade ultérieur (voir A/CN.9/437, par. 150).

CHAPITRE IV. SIGNATURES ÉLECTRONIQUES ÉTRANGÈRES

Article 17. Fourniture de services par des autorités de certification étrangères

1. Variante A Des [personnes] [entités] étrangères peuvent s'établir localement comme autorités de certification ou peuvent fournir des services de certification à partir d'un autre pays sans avoir un établissement local si elles satisfont aux mêmes normes objectives [et suivent les mêmes procédures] que les entités et personnes locales pouvant devenir des autorités de certification.

Variante B Sous réserve de la législation de l'État adoptant, une [personne] [entité] étrangère peut:

a) s'établir localement comme autorité de certification; ou

b) fournir des services de certification sans être établie localement si elle satisfait aux mêmes normes objectives et suit les mêmes procédures que les entités et personnes locales pouvant devenir des autorités de certifications.

Variante C Des [personnes] [entités] étrangères ne peuvent se voir refuser le droit de s'établir localement ou de fournir des services de certification au seul motif qu'elles sont étrangères

si elles satisfont aux mêmes normes objectives [et suivent les mêmes procédures] que les entités et personnes locales pouvant devenir des autorités de certification.

[2. Variante X La règle énoncée au paragraphe 1 ne s'applique pas dans les situations suivantes: [...].

Variante Y Des exceptions à la règle énoncée au paragraphe 1 peuvent être formulées si la sécurité nationale l'exige.]

Références

A/CN.9/446, par. 175 à 188 (projet d'article 17);
A/CN.9/WG.IV/WP.73, par. 73;
A/CN.9/437, par. 74 à 89 (projet d'article I); et
A/CN.9/WG.IV/WP.71, par. 73 à 75.

Remarques

48. En permettant à des entités étrangères de s'établir localement comme autorités de certification, le projet d'article 17 énonce simplement le principe de la non-discrimination à l'égard des entités étrangères, étant entendu que celles-ci doivent respecter les normes applicables aux autorités de certification nationales. Si ce principe est généralement accepté, il peut être néanmoins particulièrement utile de l'énoncer en ce qui concerne les autorités de certification, car l'on peut s'attendre à ce que ces dernières n'aient pas nécessairement un établissement matériel ou un autre lieu de commerce dans le pays où elles offrent des services.

Article 18. Approbation des certificats étrangers par les autorités de certification nationales

Variante A Les certificats émis par les autorités de certification d'un autre pays peuvent être utilisés pour des signatures numériques selon les mêmes modalités que les certificats soumis aux présentes Règles s'ils sont reconnus par une autorité de certification se conformant à ... [*la loi de l'État adoptant*], et si celle-ci garantit, à l'instar de ce qu'elle fait pour ses propres certificats, que les détails figurant dans le certificat sont exacts et, en outre, que le certificat est valide et en vigueur.

Variante B Les certificats émis par des autorités de certification étrangères peuvent être utilisés pour des signatures numériques selon les mêmes modalités que les certificats soumis aux présentes Règles à condition d'être dûment garantis par une autorité de certification se conformant à ... [*la loi de l'État adoptant*].

Références

A/CN.9/446, par. 189 à 195 (projet d'article 18);
A/CN.9/WG.IV/WP.73, par. 74;
A/CN.9/437, par. 74 à 89 (projet d'article I); et
A/CN.9/WG.IV/WP.71, par. 73 à 75.

Remarques

49. Le projet d'article 18 permet à une autorité de certification nationale de garantir, à l'instar de ce qu'elle fait pour ses propres certificats, que les détails figurant dans le certificat étranger sont exacts et que ce certificat est valide et en vigueur. Il renvoie aux questions désignées par l'expression "certification croisée" à la trente et unième session du Groupe de travail. Il contient essentiellement une disposition sur l'attribution de la

responsabilité à l'autorité de certification nationale en cas de non-conformité du certificat étranger (voir A/CN.9/437, par. 77 et 78).

Article 19. Reconnaissance de certificats étrangers

Variante A

1. Variante X Les certificats émis par des autorités de certification étrangères ne peuvent se voir refuser la même reconnaissance que les certificats émis par des autorités de certification nationales au motif qu'ils ont été émis par des autorités de certification étrangères.

Variante Y Les certificats émis par une autorité de certification étrangère sont reconnus comme équivalant juridiquement aux certificats émis par les autorités de certification se conformant à ... [*la loi de l'État adoptant*] si les pratiques de l'autorité de certification étrangère offrent un niveau de fiabilité au moins équivalent à celui qui est requis des autorités de certification en vertu des présentes Règles. [Cette reconnaissance peut se faire par une décision publiée de l'État ou par un accord bilatéral ou multilatéral entre les États concernés.]

2. Les signatures et les enregistrements conformes aux lois d'un autre État relatives aux signatures numériques ou autres signatures électroniques sont reconnus comme équivalant juridiquement aux signatures et enregistrements conformes aux présentes Règles si les lois de l'autre État exigent un niveau de fiabilité au moins équivalent à celui qui est exigé pour les enregistrements et signatures au titre de ... [*la loi de l'État adoptant*]. [Cette reconnaissance peut se faire par une décision publiée de l'État ou par un accord bilatéral ou multilatéral avec d'autres États.]

2 [3]. Les signatures numériques vérifiées par référence à un certificat émis par une autorité de certification étrangère ne peuvent se voir refuser leurs effets [par les tribunaux ou d'autres juges des faits] si le certificat est aussi fiable que nécessaire au vu de l'objet pour lequel il a été émis, compte tenu de toutes les circonstances.

3 [4]. Nonobstant le paragraphe précédent, les organismes publics et les parties à des transactions commerciales et autres peuvent spécifier qu'il est nécessaire de recourir à une autorité de certification, une catégorie d'autorité de certification ou une catégorie de certificats particuliers pour les messages ou les signatures qui leur sont soumis.

Variante B

1. Les certificats émis par une autorité de certification étrangère sont reconnus comme équivalant juridiquement aux certificats émis par les autorités de certification se conformant à ... [*la loi de l'État adoptant*] si les pratiques de l'autorité de certification étrangère offrent un niveau de fiabilité au moins équivalent à celui qui est requis des autorités de certification en vertu des présentes Règles.

[2. L'équivalence visée au paragraphe 1 peut être déterminée par une décision publiée de l'État ou par un accord bilatéral ou multilatéral avec d'autres États.]

3. Pour la détermination de l'équivalence, il est tenu compte des critères suivants:

a) ressources financières et humaines, y compris l'existence d'avoirs dans la juridiction;

b) fiabilité du matériel et des logiciels;

c) procédures utilisées pour le traitement des certificats et des demandes de certificat et la conservation des enregistrements;

d) possibilités d'accès à l'information pour les [signataires] [sujets] indiqués dans les certificats et les éventuelles parties se fiant aux certificats;

e) régularité et étendue des audits effectués par un organisme indépendant;

f) existence d'une déclaration de l'État, d'un organisme d'habilitation ou de l'autorité de certification concernant le respect ou l'existence des critères énumérés ci-dessus;

g) possibilités d'exercice de la compétence des tribunaux de l'État adoptant; et

h) importance des divergences entre la loi applicable à la responsabilité de l'autorité de certification et la loi de l'État adoptant.

Variante C

Une autorité de certification étrangère est jugée fiable [*dans l'État adoptant*] aux fins d'un certificat qu'elle émet pour étayer les signatures apposées à des messages de données si, lorsqu'elle émet un tel certificat, elle se conforme aux présentes Règles et à tout régime de licence national applicable à un certificat de ce type et est soumise au moins aux mêmes responsabilités que celles qui sont imposées par les présentes Règles et ce régime de licence.

Variante D

1. Une autorité étrangère est jugée fiable [*dans l'État adoptant]* aux fins d'un certificat qu'elle émet pour étayer les signatures apposées à des messages de données si, lorsqu'elle émet ledit certificat, elle offre un niveau de fiabilité [au moins] équivalent à celui [qui est requis] des autorités de certification nationales émettant de tels certificats.

2. Pour évaluer le niveau de fiabilité d'une autorité de certification, il est tenu compte des critères suivants:

a) ressources financières et humaines, y compris l'existence d'avoirs dans la juridiction;

b) fiabilité du matériel et des logiciels;

c) procédures utilisées pour le traitement des certificats et des demandes de certificat et la conservation des enregistrements;

d) possibilités d'accès à l'information pour les [signataires] [sujets] indiqués dans les certificats et les éventuelles parties se fiant auxdits certificats;

e) régularité et étendue des audits effectués par un organisme indépendant;

f) existence d'une déclaration de l'État, d'un organisme d'habilitation ou de l'autorité de certification concernant le respect ou l'existence des critères énumérés ci-dessus;

g) possibilité d'exercice de la compétence des tribunaux de l'État adoptant; et

h) importance des divergences entre la loi applicable à la responsabilité de l'autorité de certification et la loi de l'État adoptant.

Références

A/CN.9/446, par. 196 à 207 (projet d'article 19);
A/CN.9/WG.IV/WP.73, par. 75;
A/CN.9/437, par. 74 à 89 (projet d'article I); et
A/CN.9/WG.IV/WP.71, par. 73 à 75.

Remarques

50. Le projet d'article 19 porte sur les questions désignées par l'expression "reconnaissance transfrontière" à la trente et unième session du Groupe de travail (voir A/CN.9/437, par. 77 et 78). La variante A est fondée sur une proposition de regroupement des paragraphes 1 et 2 formulée à la trente-deuxième session du Groupe de travail (voir A/CN.9/446, par. 197 et 204). La variante B donne une liste indicative de critères à prendre en considération pour apprécier la fiabilité des certificats étrangers. Les variantes C et D sont axées sur la reconnaissance des autorités de certification étrangères. Il convient de noter que, si le Groupe de travail décide d'inclure dans les Règles uniformes les critères auxquels les autorités de certification doivent satisfaire (voir ci-dessus par. 19), il pourrait être nécessaire de prévoir de tels critères au projet d'article 19.

* * *

Notes

[1]Documents officiels de l'Assemblée générale, cinquante et unième session, Supplément n° 17 (A/51/17), par. 223 et 224.

[2]Ibid., cinquante-deuxième session, Supplément n° 17 (A/52/17), par. 249 à 251.