



Assemblée générale

Distr. LIMITÉE

A/CN.9/WG.IV/WP.79
23 novembre 1998

FRANÇAIS
Original: ANGLAIS

COMMISSION DES NATIONS UNIES
POUR LE DROIT COMMERCIAL INTERNATIONAL
Groupe de travail sur le commerce électronique
Trente-quatrième session
Vienne, 8-19 février 1999

PROJET DE RÈGLES UNIFORMES SUR LES SIGNATURES ÉLECTRONIQUES

Note du Secrétariat

TABLE DES MATIÈRES

	<u>Paragraphes</u>	<u>Page</u>
INTRODUCTION	1 - 11	3
I. OBSERVATIONS GÉNÉRALES	12 - 14	4
II. PROJET DE DISPOSITIONS SUR LES SIGNATURES NUMÉRIQUES, LES AUTRES SIGNATURES ÉLECTRONIQUES, LES AUTORITÉS DE CERTIFICATION ET LES QUESTIONS JURIDIQUES CONNEXES	15 - 53	5
CHAPITRE PREMIER. CHAMP D'APPLICATION ET DISPOSITIONS GÉNÉRALES	15 - 20	5
CHAPITRE II. SIGNATURES ÉLECTRONIQUES	21 - 48	6
Section I. Signatures électroniques en général	21 - 23	6
Article premier. Définitions	21	6
Article 2. Respect des exigences légales	22 - 23	8
Section II. Signatures électroniques [renforcées]	24 - 44	9
Article 3. []	24 - 30	9
Article 4. Présomption d'attribution d'une signature électronique [renforcée]	31 - 33	11
Article 5. Présomption d'intégrité	34 - 37	12

TABLE DES MATIÈRES (suite)

	<u>Paragraphe</u> s	<u>Page</u>
Article 6. Prédétermination de la signature électronique [renforcée]	38 - 41	13
Article 7. Responsabilité du fait de l'utilisation non autorisée d'une signature électronique [renforcée]	42 - 44	14
Section III. Signatures numériques accompagnées de certificats	45 - 48	16
Article 8. Teneur d'un certificat [renforcé]	45 - 46	16
Article 9. Effet des signatures numériques accompagnées de certificats . . .	47 - 48	18
CHAPITRE III. AUTORITÉS DE CERTIFICATION ET QUESTIONS CONNEXES	49 - 53	20
Article 10. Garanties données au moment de l'émission d'un certificat [renforcé]	49 - 50	20
Article 11. Responsabilité contractuelle	51	21
Article 12. Responsabilité de l'autorité de certification envers les parties se fiant au certificat	52	22
Remarque générale concernant les projets d'articles 13 à 15	53	23
Article 13. Annulation d'un certificat	--	23
Article 14. Suspension d'un certificat	--	24
Article 15. Registre des certificats	--	24

INTRODUCTION

1. À sa vingt-neuvième session (1996), la Commission a décidé d'inscrire à son ordre du jour les questions relatives aux signatures numériques et aux autorités de certification. Le Groupe de travail sur le commerce électronique a été prié de réfléchir à l'opportunité de définir des règles uniformes concernant ces questions. Il a été convenu que les règles uniformes devant être élaborées devraient être consacrées notamment aux questions ci-après: fondement juridique des opérations de certification, y compris les nouvelles techniques d'authentification et de certification numériques; applicabilité de la certification; répartition des risques et des responsabilités entre utilisateurs, fournisseurs et tiers dans le contexte de l'utilisation de techniques de certification; questions spécifiques à la certification sous l'angle de l'utilisation des registres; et incorporation par référence¹.

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). 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 arrivé à la conclusion préliminaire qu'il était possible d'entreprendre l'élaboration d'un projet de règles uniformes, du moins sur les questions concernant les signatures numériques et les autorités de certification et peut-être sur des questions connexes. Le Groupe de travail a rappelé que dans le cadre des travaux futurs dans le domaine du commerce électronique, il pourrait être nécessaire de traiter, outre les questions relatives aux signatures numériques et aux autorités de certification, les sujets suivants: techniques autres que la cryptographie à clef publique; questions générales concernant les fonctions exercées par les tiers fournisseurs de services et contrats électroniques (A/CN.9/437, par. 156 et 157).

3. La Commission a approuvé les conclusions du Groupe de travail 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, la Commission est généralement convenue qu'aucune décision ne pouvait être prise à ce stade 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 (dénommée ci-après "la Loi type"). 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 que les Règles uniformes prennent en considération divers niveaux de sécurité et reconnaissent 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 généralement considéré que le Groupe de travail pourrait utilement envisager l'établissement d'un ensemble minimum de normes que les autorités de certification devraient strictement respecter, en particulier dans les cas de certification transnationale².

5. Le Groupe de travail a commencé à élaborer le projet de Règles uniformes en se fondant sur une note établie par le secrétariat (A/CN.9/WG.IV/WP.73).

6. À sa trente et unième session (1998), la Commission était saisie du rapport du Groupe de travail sur les travaux de sa trente-deuxième session (A/CN.9/446). Elle a pris note avec satisfaction des efforts déployés par le Groupe de travail lors de l'élaboration du projet de Règles uniformes. On a noté qu'à ses trente et unième et

trente-deuxième sessions, le Groupe de travail avait eu manifestement beaucoup de mal à se mettre d'accord sur les nouveaux problèmes juridiques qui découlait du recours accru aux signatures numériques et autres signatures électroniques. On a également fait observer qu'un consensus restait encore à réaliser sur la manière dont ces problèmes pouvaient être abordés dans un cadre juridique acceptable à l'échelon international. Toutefois, la Commission a estimé, dans l'ensemble, que les progrès accomplis jusqu'ici étaient le signe que le projet de Règles uniformes sur les signatures électroniques prenait progressivement la forme d'une structure utilisable.

7. La Commission a réaffirmé la décision qu'elle avait prise à sa trente et unième session en ce qui concerne la faisabilité de l'élaboration de Règles uniformes. La Commission était généralement d'avis que les progrès réalisés jusqu'ici montraient que le projet de Règles uniformes sur les signatures électroniques prenait progressivement la forme d'une structure utilisable et que le Groupe de travail pourrait accomplir de nouveaux progrès à sa trente-troisième session sur la base du projet révisé établi par le secrétariat (A/CN.9/WG.IV/WP.76). La Commission a également fait observer que l'on reconnaissait généralement désormais que le Groupe de travail était une instance internationale particulièrement importante pour échanger des vues sur les problèmes juridiques que posaient le commerce électronique et la recherche de solutions à ces problèmes.

8. Le Groupe de travail a poursuivi la révision des Règles uniformes à sa trente-troisième session, sur la base d'une note établie par le secrétariat (A/CN.9/WG.IV/WP.76). Le rapport sur les travaux de cette session est publié sous la cote A/CN.9/454.

9. 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 trente et unième session, dont il est rendu compte ci-dessus. Il tient compte des décisions prises par le Groupe de travail à sa trente-troisième session.

10. 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.

11. 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

12. 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 électroniques 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.

13. 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.

14. 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

15. 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 ou si elles devraient être incorporées dans une version élargie de la Loi type, comme troisième partie, par exemple.

16. 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 (Définitions pertinentes), 3 (Interprétation) et 4 (Dérogation conventionnelle) 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, si l'on inclut un article inspiré de l'article premier de la Loi type, les transactions dans lesquelles interviennent des consommateurs ne seraient pas exclues du champ d'application des Règles uniformes sauf si la loi applicable à ce type de transactions dans l'État adoptant était incompatible avec elles.

17. 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.

18. 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 électroniques par la mise en place d'une structure de sécurité et l'affirmation de l'égalité entre les messages manuscrits et les messages électroniques s'agissant de leur effet juridique.

19. À sa trente-troisième session, le Groupe de travail s'est demandé s'il était bien approprié d'employer les qualificatifs "renforcée" ou "sécurisée" pour décrire des techniques de signature capables d'offrir une plus grande fiabilité que les "signatures électroniques" en général (A/CN.9/454, par. 29). Il a conclu qu'en l'absence d'un terme plus approprié, le terme "renforcée" serait conservé. C'est pourquoi le terme est mis entre crochets dans le présent projet révisé de Règles uniformes.

20. Lorsqu'il examinera la relation entre les Règles uniformes et l'article 7 de la Loi type, le Groupe de travail souhaitera peut-être se demander si l'application de ces Règles devrait être limitée aux cas dans lesquels existent des conditions de forme juridique ou dans lesquels la loi prévoit les conséquences de l'absence de certaines conditions, telles que l'écrit ou une signature. Il convient de rappeler que la signification des termes "conditions de forme" a été examinée lors de l'élaboration de la Loi type. Le paragraphe 68 du Guide sur l'incorporation indique que, dans le cadre de la Loi type, le terme "loi" doit être interprété comme renvoyant non seulement aux dispositions législatives et réglementaires, mais aussi aux règles découlant de la jurisprudence et autres règles processuelles. Par conséquent, ce terme couvre aussi les règles de la preuve. Lorsque la loi n'exige pas de condition particulière, mais prévoit les conséquences de l'absence de conditions, par exemple l'écrit ou une signature, il faut en tenir également compte dans la notion de "loi" telle qu'employée dans la Loi type.

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]" 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 agréée 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]" désigne un certificat [d'identification] émis pour étayer des signatures électroniques [renforcées].

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.9/454, par. 20;
A/CN.9/WG.IV/76, par. 16 à 20;
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

21. À sa précédente session, le Groupe de travail a, faute de temps, reporté l'examen du projet d'article premier à une session ultérieure (voir A/CN.9/454, par. 19). Le texte du projet d'article premier figurant dans la présente note est donc identique à celui qui figurait dans le document A/CN.9/WG.IV/76, sauf pour ce qui est du terme "sécurisée" relatif aux signatures électroniques, qui a été supprimé.

Article 2. Respect des exigences légales

1. Pour ce qui est d'un message de données authentifié à l'aide d'une signature électronique [autre qu'une signature électronique [renforcée]], cette signature satisfait à toute exigence légale concernant une signature si la fiabilité de la méthode utilisée pour l'aposer est suffisante au regard de l'objet pour lequel le message de données a été créé ou communiqué, compte tenu de toutes les circonstances, y compris toute convention 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] 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 le projet d'article 6] ou aux présomptions créées par les articles 3, 4 et 5.
4. Les dispositions du présent article ne s'appliquent pas dans les situations suivantes: [...]

Références

- A/CN.9/454, par. 21 à 27;
A/CN.9/WG.IV/WP.76, par. 21; et
A/CN.9/446, par. 27 à 46 (projet d'article premier).

Remarques

22. Le projet d'article 2 a pour objet de confirmer le lien entre l'article 7 de la Loi type et les Règles uniformes. Son paragraphe 1 prévoit une reconnaissance appropriée de l'autonomie des parties. Le Groupe de travail souhaitera peut-être examiner la question de savoir si les mots figurant entre crochets dans ce paragraphe

["autre qu'une signature électronique renforcée"] doivent être conservés, dans la mesure où ils laissent entendre qu'une signature électronique renforcée ne satisfait pas à l'exigence de l'article 7 de la Loi type, ce qui semble contredire l'effet de la variante B du projet d'article 3.

23. Le paragraphe 2 du projet d'article 2 a été inclus pour assurer une cohérence avec l'article 7 de la Loi type et pour les raisons exposées ci-dessus concernant la signification du terme "loi". Le paragraphe 3 précise bien que les règles qui s'appliquent aux signatures électroniques ayant un niveau de "renforcement" ou de "sécurisation" élevé, comme par exemple dans le cas des procédures d'octroi de licences aux autorités de certification ou d'autres règles éventuelles pour les signatures numériques ne s'appliquent pas de manière générale à tous les types de "signatures électroniques".

Section II. Signatures électroniques [renforcées]

Article 3.

Variante A

Article 3. Conformité de la signature électronique [renforcée] aux exigences légales

1. Lorsque la loi exige une signature, cette exigence est satisfaite par une signature électronique [renforcée], [à moins qu'il ne soit prouvé que cette signature ne satisfait pas aux exigences de l'article 7 de la Loi type].
2. Le paragraphe 1 s'applique, que l'exigence légale qui y est visée ait la forme d'une obligation ou que la loi prévoise simplement certaines conséquences s'il n'y a pas de signature.
3. Les dispositions du présent article ne s'appliquent pas dans les situations suivantes: [...].

Variante B

Article 3. Présomption de signature

1. Un message de données est présumé avoir été signé si une signature électronique [renforcée] y est apposée ou y est logiquement associée.
2. Les dispositions du présent article ne s'appliquent pas dans les situations suivantes: [...].

Variante C

Article 3. Conséquences de l'utilisation d'une signature électronique [renforcée]

1. Lorsque des conséquences juridiques découlent [de l'utilisation] d'une signature, elles découlent aussi d'une signature électronique [renforcée].
2. Les dispositions du présent article ne s'appliquent pas dans les situations suivantes: [...].

Références

- A/CN.9/454, par. 28 à 39;
A/CN.9/WG.IV/WP.76, par. 22 et 23;

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

Variante A

24. La variante A offre une règle pour les signatures électroniques renforcées qui est un raccourci pour satisfaire aux exigences énoncées à l'article 7 de la Loi type. Cette variante du projet d'article 3 et le projet d'article 2 établissent les bases des Règles uniformes. Tout d'abord, le projet d'article 2 reprend le principe énoncé à l'article 7 de la Loi type selon lequel une signature électronique peut satisfaire à une exigence légale concernant une signature si elle remplit certaines conditions. La variante A du projet d'article 3 dispose ensuite qu'une signature électronique [renforcée] remplit effectivement ces conditions et l'on a ainsi un raccourci pour satisfaire aux exigences énoncées à l'article 7.

25. La disposition qui confirme que l'expression "la loi" s'applique, que l'exigence légale ait la forme d'une obligation ou que la loi prévoie simplement certaines conséquences de l'absence d'une condition particulière, a été répétée au paragraphe 2 de la variante A, pour veiller à ce que cette expression ait le même sens dans le projet de règles uniformes et la Loi type.

26. Si l'on conserve les termes entre crochets figurant dans le projet de variante A, on a alors un raccourci pour satisfaire aux exigences de l'article 7 de la Loi type, avec une restriction possible lorsqu'il peut être prouvé que les exigences de cet article ne sont pas satisfaites. Le Groupe de travail souhaitera peut-être examiner la question de savoir s'il convient de conserver ces termes au projet d'article 3.

Variante B

27. La variante B vise à créer la présomption qu'un message de données peut être considéré comme "signé" s'il est authentifié par une signature électronique renforcée. Cette présomption établit une distinction entre la "signature" d'un message et la question de l'identification du signataire. Elle peut être importante lorsqu'une signature n'est pas exigée par la loi, comme il est énoncé à l'article 7 de la Loi type, mais que son apposition sur un message de données peut être importante à d'autres fins, ou lorsque la loi exige qu'un message soit signé sans préciser l'identité du signataire ou encore lorsque la question de l'identité du signataire ne se pose pas.

28. Dans son libellé actuel, la variante B peut s'appliquer à des situations autres que celles envisagées à l'article 7. Le Groupe de travail souhaitera peut-être examiner si ces deux branches de l'article 7 (c'est-à-dire lorsque la loi exige une signature ou lorsque les conséquences de l'absence d'une signature sont précisées) couvrent toutes les situations dans lesquelles une signature pourrait être utilisée ou produire un effet juridique. Une disposition inspirée de la variante B pourrait sinon être utile. On pourrait alors conserver la variante B en plus de la variante A, dans la mesure où elle couvrirait les autres situations.

29. La mention, dans l'ancien projet d'article 3, du moment où la signature est apposée a été supprimée, mais le Groupe de travail souhaitera peut-être examiner s'il conviendrait d'inclure cette notion dans une autre partie du projet de Règles uniformes.

Variante C

30. Cette variante vise à établir, dans les Règles uniformes, un principe clair de non-discrimination, tel qu'il apparaît dans l'article 5 de la Loi type. L'objectif est de garantir que lorsque l'utilisation d'une signature entraîne des conséquences juridiques, que cette signature soit ou non exigée par la loi, ces conséquences sont les mêmes pour les signatures manuscrites et les signatures électroniques. L'effet de cette variante est très proche de celui de la variante B, dans la mesure où les deux se fondent sur le droit interne pour prévoir les conséquences de la signature d'un message (variante B) ou de l'emploi d'une signature (variante C).

Article 4. Présomption d'attribution d'une signature électronique [renforcée]

1. Une signature électronique [renforcée] est présumée être celle de la personne par laquelle, ou au nom de laquelle, elle est supposée avoir été créée, sauf s'il est établi que cette signature n'a été apposée ni par le signataire supposé, ni par une personne habilitée à agir en son nom.
2. Les dispositions du présent article ne s'appliquent pas dans les situations suivantes: [...].

Références

- A/CN.9/454, par. 40 à 53;
A/CN.9/WG.IV/WP.76, par. 24;
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

31. Le projet d'article 4 établit une présomption d'attribution pour les signatures électroniques [renforcées], et prévoit aussi deux cas où celle-ci ne s'applique pas. Il porte donc sur des questions traitées à l'article 13 de la Loi type, quoiqu'avec quelques différences rédactionnelles. Le projet d'article 4, par exemple, a la forme d'une présomption d'attribution réfragable. Le paragraphe 2 de l'article 13 de la Loi type, en revanche, a la forme d'une présomption irréfragable, et le paragraphe 3 du même article établit une règle autorisant le destinataire à agir en se fondant sur l'attribution du message de données. Le projet d'article 4 traite de l'attribution d'une signature, alors que l'article 13 de la Loi type traite de l'attribution des messages de données. Les critères d'attribution de la signature dans le projet d'article 4 sont légèrement différents de ceux qui sont fixés dans l'article 13 de la Loi type pour l'attribution du message de données.

32. Le Groupe de travail souhaitera peut-être examiner la relation entre le projet d'article 4 et l'article 13 de la Loi type et, en particulier, se demander s'il est juridiquement nécessaire d'établir une distinction entre l'attribution du message et l'attribution de la signature qui y est apposée. Il faut tenir compte du fait que, pour des raisons techniques, il pourrait être impossible d'établir une telle distinction. Il se peut que l'attribution d'une signature doive suivre l'attribution d'un message de données, ou vice versa, auquel cas une seule règle d'attribution serait nécessaire.

33. Le projet d'article 4 a pour autre caractéristique de traiter de l'utilisation non autorisée de la signature électronique. À cet égard, il reprend des questions traitées par l'article 13 de la Loi type. Il dispose, par exemple, que la présomption d'attribution ne s'applique pas dans deux cas – lorsque la signature n'a été apposée ni par le signataire supposé, ni par une personne autorisée par le signataire supposé. L'article 13, en revanche, dispose

que, même si le message n'a pas été autorisé, le destinataire peut le considérer comme étant celui de l'expéditeur supposé. Le Groupe de travail voudra peut-être examiner la nécessité d'inclure dans les Règles uniformes une nouvelle règle sur l'utilisation non autorisée d'une signature, ainsi que la relation entre cette règle et le projet d'article 7 sur la responsabilité.

Article 5. Présomption d'intégrité

1. *Variante A*

Si une [procédure de sécurité fiable] [signature électronique renforcée] est correctement [appliquée à] [apposée sur] une certaine partie d'un message de données et indique que cette partie du message n'a pas été modifiée depuis un moment précis, il est présumé que la partie du message de données en question n'a pas été modifiée depuis lors.

Variante B

Si une procédure de sécurité est capable d'établir [de manière fiable] [avec un degré de certitude élevé] qu'une certaine partie d'un message de données n'a pas été modifiée depuis un moment précis et que cette procédure, appliquée correctement, indique que le message de données n'a pas été modifié, il est présumé que [l'intégrité du message de données a été préservée] [le message de données n'a pas été modifié] depuis lors.

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

Références

- A/CN.9/454, par. 54 à 63;
A/CN.9/WG.IV/WP.76, par. 25 et 26;
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

34. Le projet d'article 5 a été révisé conformément à la décision prise par le Groupe de travail à sa trente-troisième session (A/CN.9/454, par. 54 à 63). Ce texte révisé vise à établir une présomption d'intégrité du message de données. À cette fin, les deux variantes du projet d'article exigent que la procédure de sécurité ait été effectivement appliquée ou la signature apposée et donne un résultat qui montre que le message n'a pas été modifié. Une fois cette preuve apportée, la présomption n'aurait que peu de valeur. Le Groupe de travail souhaitera peut-être examiner la question de savoir si le projet d'article devrait prendre la forme d'une présomption ou d'une règle de droit.

35. Selon une des possibilités prévues dans la variante A, l'apposition de la signature atteste l'intégrité. Le Groupe de travail souhaitera peut-être examiner s'il convient d'inclure à la fois l'apposition et la vérification de cette signature (et l'utilisation de la fonction de condensation ou d'abrégement) ou si l'application d'une procédure de sécurité est une formulation préférable.

36. Le paragraphe 1 du projet d'article 5, tant dans la variante A que dans la variante B, crée un lien direct entre le fait de signer un message et l'intégrité de ce message, lien qui n'est peut-être pas toujours utile ou

nécessaire. Dans certains cas, la fonction d'intégrité fait partie intégrante de la technique de signature électronique utilisée (comme cela peut être le cas avec certains types de signatures électroniques [renforcées]), et une présomption quant à l'intégrité énonce simplement ce qui est un résultat direct de l'utilisation de cette technique. Dans d'autres cas, la technique de signature utilisée peut ne pas permettre de satisfaire à une exigence d'intégrité, même si elle peut être considérée, sous tous ses autres aspects, comme une signature électronique [renforcée]. Il y aura en outre des cas où il pourra être nécessaire de prouver l'intégrité d'un message qui n'est pas signé. Une règle établissant un lien direct entre l'intégrité et la signature peut alors être inutile.

37. Lorsque l'intégrité est requise pour montrer qu'un message est un original, l'article 8 de la Loi type s'applique. Le Groupe de travail souhaitera peut-être examiner les questions de savoir si une présomption d'intégrité devrait être incluse dans les présentes Règles en tant que règle de droit et si la fonction d'intégrité devrait être incluse dans la définition d'une signature électronique [renforcée] et examiner par ailleurs la relation entre le présent projet d'article et l'article 8 de la Loi type.

Article 6. Prédétermination de la signature électronique [renforcée]

1. *[L'organe ou l'autorité indiqué par l'État adoptant comme compétent en la matière]* peut déterminer:
 - a) qu'une signature électronique est [une signature électronique [renforcée]] [satisfait aux exigences de l'article 7 de la Loi type];
 - b) qu'une procédure de sécurité satisfait aux exigences de l'article 5].
2. Toute détermination en vertu du paragraphe 1 doit être conforme aux normes techniques internationales reconnues.
3. [Sous réserve [des présentes Règles et] de la loi applicable], les parties peuvent convenir qu'une signature électronique doit être traitée entre elles:
 - a) comme une signature électronique [renforcée]];
 - b) comme satisfaisant aux exigences de l'article 7 de la Loi type].

Références

A/CN.9/454, par. 64 à 75;
A/CN.9/WG.IV/WP.76, par. 27;
A/CN.9/446, par. 37 à 45 (projet d'article premier); et
A/CN.9/WG.IV/WP.73, par. 27.

Remarques

38. La précédente version du paragraphe 1 du projet d'article 6 indiquait que la signature satisfaisait aux exigences du paragraphe b) du projet d'article premier (définition d'une signature électronique [renforcée]). Le texte révisé du projet d'article 6 permet de déterminer qu'une signature électronique est une signature électronique [renforcée] ou, autre possibilité, que la signature électronique satisfait aux exigences de l'article 7, ce qui crée un raccourci clair. Si une signature électronique est une signature électronique [renforcée] au titre de la variante A du projet d'article 3, il n'est pas nécessaire de préciser qu'elle satisfait aux exigences de l'article 7, ce qui découle clairement de sa qualité de signature [renforcée].

39. La version révisée du paragraphe 1 b) du projet d'article 6, sur laquelle le Groupe de travail s'était mis d'accord à sa trente-troisième session (A/CN.9/454, par. 73), renvoie aux "exigences de l'article 5". Tel que révisé à la même session (A/CN.9/454, par. 61), le projet d'article 5 ne fixe plus de conditions pour l'intégrité. Le Groupe de travail souhaitera peut-être revenir sur l'insertion d'une référence au projet d'article 5 au paragraphe 1 b) du projet d'article 6.

40. Les mots "dans la mesure où celles-ci existent" ont été supprimés du paragraphe 2 du projet d'article 6, car ils ont été jugés inutiles dans le cadre d'une loi type. Dans la mesure où de telles normes existent, les États qui adoptent les règles uniformes devraient être incités à les observer et une note à cet effet pourrait être incluse, dans un guide pour l'incorporation par exemple.

41. Le libellé du paragraphe 3 du projet d'article 6 a été modifié, afin de tenir compte de la préoccupation exprimée à la trente-troisième session du Groupe de travail (A/CN.9/454, par. 71), à savoir que si l'autonomie des parties doit être respectée, toute convention entre elles concernant l'utilisation d'une signature électronique ne devrait pas affecter les tiers. Le nouveau texte tient compte également d'autres remarques (A/CN.9/454, par. 75) concernant l'emploi des termes "déterminer l'effet d'une signature" (soulignement ajouté) et leur interprétation possible dans des systèmes juridiques différents. Le paragraphe 3 reprend le libellé du paragraphe 1 en proposant la détermination du statut [renforcé] comme solution de rechange à la détermination que la signature satisfait aux exigences de l'article 7 de la Loi type.

Article 7. Responsabilité du fait de l'utilisation non autorisée d'une signature électronique [renforcée]

Variante A

Lorsque l'utilisation d'une signature électronique [renforcée] n'a pas été autorisée et lorsque le signataire supposé n'a pas exercé un soin raisonnable pour éviter l'utilisation non autorisée de sa signature et pour empêcher que le destinataire ne s'y fie,

Variante X la signature est néanmoins considérée comme autorisée, sauf si la partie qui s'y est fiée savait ou aurait dû savoir qu'elle ne l'était pas.

Variante Y le signataire supposé ne peut être tenu responsable que du coût du rétablissement des parties dans la situation qui était la leur avant l'utilisation non autorisée de la signature, sauf si la partie qui s'y est fiée savait ou aurait dû savoir que cette signature n'était pas celle du signataire supposé.

Variante Z le signataire supposé est tenu responsable du préjudice causé [et doit verser des dommages-intérêts à la partie s'étant fiée à la 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

1. Lorsque:

- a) l'utilisation d'une signature électronique [renforcée] n'a pas été autorisée;
- b) le signataire supposé n'a pas exercé un soin raisonnable pour éviter l'utilisation non autorisée de sa signature et pour empêcher que le destinataire ne s'y fie; et
- c) le destinataire s'est, à son détriment, fié de bonne foi à la signature;

la signature est [attribuée] [attribuable] au signataire supposé aux fins de la détermination de la responsabilité pour le coût du rétablissement des parties dans la situation qui était la leur avant l'utilisation non autorisée de la signature.

2. Le paragraphe 1 ne s'applique pas si le destinataire savait ou aurait dû savoir que l'utilisation de la signature n'était pas autorisée.

Variante C

1. Lorsqu'une signature électronique [renforcée] est apposée à un message de données et lorsque:

- a) son utilisation n'a pas été autorisée;
- b) le signataire supposé n'a pas exercé un soin raisonnable pour éviter l'utilisation non autorisée de sa signature; et
- c) le destinataire s'est, à son détriment, fié de bonne foi à la signature,

le message de données est attribué au signataire supposé sauf s'il [n'est ni juste ni équitable] [serait manifestement inéquitable] de le faire, compte tenu des raisons pour lesquelles le message de données a été utilisé et d'autres circonstances pertinentes.

2. [Lorsque les alinéas a), b) et c) du paragraphe 1 s'appliquent, et lorsque le message de données n'est pas attribué au signataire supposé en vertu du paragraphe 1] [Lorsque le message de données n'est pas attribué au signataire supposé en vertu du paragraphe 1 pour des raisons d'iniquité manifeste], le signataire supposé est néanmoins responsable du coût du rétablissement du destinataire dans la position qui était la sienne avant l'utilisation de la signature non autorisée.

3. Le paragraphe 1 ne s'applique pas:

- a) dans la mesure où le destinataire savait ou aurait dû savoir, s'il avait exercé un soin raisonnable, que la signature n'était pas celle du signataire supposé;
- b) lorsque le destinataire a été avisé par le signataire supposé que la signature n'était pas la sienne et qu'il disposait d'un délai raisonnable pour agir en conséquence.

4. Il serait manifestement inéquitable d'attribuer une signature non autorisée à un signataire supposé au titre du paragraphe 1 lorsque:

- a) cela causerait au signataire supposé un préjudice sans aucune mesure avec la perte subie par le destinataire;
- b) [...]

Références

- A/CN.9/454, par. 76 à 88;
A/CN.9/WG.IV/WP.76, par. 28 à 30;
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

42. Le projet d'article 7 a été modifié, afin d'y inclure un certain nombre de variantes dont le Groupe de travail a discuté à sa trente-troisième session (A/CN.9/454, par. 76 à 88). Telles qu'actuellement libellées, les variantes A et B soulèvent des questions qui sont traitées à l'article 13 de la Loi type, en particulier au paragraphe 3. Il convient de noter, cependant, que l'article 13 de la Loi type porte sur l'attribution d'un message de données, alors que le projet d'article 7 porte sur l'utilisation non autorisée d'une signature.

43. La question de l'attribution est traitée de façon légèrement différente dans le projet d'article 7 et dans l'article 13. Ainsi, au titre du paragraphe 4 a et b de l'article 13, dans le cas d'un message non autorisé au sens du paragraphe 3 b de l'article 13, le destinataire peut se fier au message, à condition de ne pas avoir été avisé de l'absence d'autorisation, ou de n'avoir pu savoir que le message n'était pas autorisé. L'article 13 ne précise pas que le signataire supposé peut arguer du fait qu'il a agi raisonnablement pour protéger sa signature (c'est-à-dire en empêchant l'accès à une méthode utilisée par lui pour identifier le message de données comme étant le sien), ce qu'il peut faire en vertu de la variante B 1 b) du projet d'article 7. En outre, l'article 13 n'aborde pas la question d'une action de bonne foi du destinataire, à son détriment; par contre, il est clair que la variante B 1 c) du projet d'article 7 des Règles uniformes est fondée sur le préjudice subi par le destinataire et sur l'idée de restitution.

44. L'article 13 de la Loi type et le projet d'article 7 des Règles uniformes ne sont pas axés sur la même question. L'article 13 est centré sur l'attribution du message, alors que le projet d'article 7 établit une règle de responsabilité pour l'attribution de la signature. Le Groupe de travail se souviendra que le projet d'article 4 appelle une décision quant à la nécessité juridique d'établir une distinction entre l'attribution du message et l'attribution de la signature (voir ci-dessus par. 32). Il faudra peut-être examiner la relation entre les deux projets d'article pour veiller à ce qu'il n'y ait pas d'incertitude, lorsque le message de données est signé, sur la disposition à appliquer pour attribuer ledit message. Une des manières de procéder serait de prévoir une règle particulière applicable aux cas dans lesquels le message de données est signé à l'aide d'une signature électronique [renforcée]. La variante C du projet d'article 7 a été ajoutée à cette fin. Outre l'iniquité manifeste, le projet de paragraphe 3 de la variante C reprend les deux cas énoncés à l'article 13 où le message ne peut être attribué au signataire supposé, alors que le projet de paragraphe 4 donne quelques indications sur ce qui peut constituer une iniquité manifeste. Le Groupe de travail souhaitera peut-être examiner d'autres situations pouvant constituer une iniquité manifeste dans le contexte de l'attribution.

Section III. Signatures numériques accompagnées de certificats

Article 8. Teneur d'un certificat [renforcé]

Variante A

1. Aux fins des présentes Règles, un certificat [renforcé] 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;]
- [g) il identifie l'algorithme à appliquer].

Variante B

1. En divulguant à une quelconque partie les informations contenues dans un certificat, une autorité de certification [ou le sujet d'un certificat] s'assure que lesdites informations comprennent au moins les éléments énumérés au paragraphe 2, sauf dans la mesure où l'autorité de certification [ou le sujet, selon le cas] et ladite partie en conviennent expressément autrement.

Variante X

2. Les informations visées au paragraphe 1 sont les suivantes:

- a) pour tous les certificats,
 - i) l'identité de l'autorité de certification qui les utilise;
 - ii) la clef publique correspondant à une clef privée dont le [signataire] [sujet du certificat] a le contrôle;
 - iii) la signature, numérique ou autre, de l'autorité de certification qui [émet le certificat] [communique les informations];
- b) pour les certificats [...],
 - i) la période d'effet du certificat;
 - [ii) les restrictions, le cas échéant, à l'utilisation de la clef publique;]
 - [iii) l'identité de l'algorithme à appliquer.]

Variante Y

2. Les informations visées au paragraphe 1 sont les suivantes:

- a) l'identité de l'autorité de certification qui utilise [le certificat] [les informations];
- b) le nom ou l'identité du [signataire] [sujet du certificat] ou d'un dispositif ou d'un agent électronique sous le contrôle [du signataire] [du sujet du certificat] [de cette personne];
- c) la clef publique correspondant à une clef privée dont le [signataire] [sujet du certificat] a le contrôle;

- d) la signature, numérique ou autre, de l'autorité de certification [qui émet le certificat] [qui communique les informations];
3. Les certificats peuvent aussi contenir d'autres informations, notamment:
- a) la période d'effet du certificat;
 - [b) les restrictions, le cas échéant, à l'utilisation de la clef publique;]
 - [c) l'identité de l'algorithme à appliquer].

Références

- A/CN.9/454, par. 89 à 116;
- A/CN.9/WG.IV/WP.76, par. 31;
- 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, 59 et 60.

Remarques

45. Étant donné la rapidité de l'évolution des techniques et le développement de formes de certification qui ne sont pas basées sur le modèle tripartite (signataire, parties se fiant à la signature et autorité de certification), on s'est demandé, à la trente-troisième session du Groupe de travail, s'il était bien approprié d'inclure dans les Règles une seule disposition traitant de la teneur des certificats (A/CN.9/454, par. 90 à 97). La version révisée du projet d'article 8 inclut les deux variantes qui, de l'avis du Groupe de travail, (A/CN.9/454, par. 116), fourniraient la base d'un débat futur.

46. La Variante B tient compte de la crainte suivante: l'émission d'un certificat pourrait consister uniquement dans la délivrance dudit certificat à son titulaire impliquant alors une relation contractuelle, par opposition à la divulgation des informations contenues dans le certificat à toute tierce partie qui s'y fie. La variante B crée l'obligation de divulguer certaines informations contenues dans le certificat, sans la rattacher pour autant à l'obligation d'inclure lesdites informations dans un certificat comme condition préalable à leur divulgation. Lorsqu'un certificat ne contient pas une information, des problèmes pourraient se poser s'il y a néanmoins obligation de révéler cette information. Le Groupe de travail souhaitera peut-être examiner la question de savoir s'il serait préférable de prévoir une disposition énonçant les éléments d'information minimums à inclure dans le certificat et une autre disposition séparée traitant de l'obligation de divulgation.

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] si:

- Variante A*
- a) elle a été créée pendant la période d'effet d'un certificat valide et est [dûment] vérifiée [pendant ladite période] par référence à la clef publique indiquée dans le certificat;
 - b) le certificat est censé rattacher une clef publique à l'identité [du destinataire] [d'une personne] [de l'expéditeur];

- c) le certificat a été émis afin d'étayer des signatures numériques qui sont des signatures électroniques [renforcées]; et
- d) le certificat a été émis:
 - i) 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 leurs fonctions]; ou
 - ii) 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 leurs fonctions]; ou
 - iii) conformément à des normes commercialement appropriées et internationalement reconnues].

Variante B

- a) la signature numérique a été créée [de manière sûre] pendant la période d'effet d'un certificat valide et est [dûment] vérifiée [pendant ladite période] par référence à la clef publique indiquée dans le certificat; et
 - b) le certificat rattache une clef publique à l'identité [de la personne] [de l'expéditeur] [...] conformément aux procédures établies par:
 - i) [l'État adoptant indique l'organe ou l'autorité ayant pouvoir d'agréer les autorités de certification et de promulguer des règles concernant leurs fonctions]; ou
 - ii) 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; ou
 - iii) [des normes internationales et des pratiques ou usages commerciaux bien connus et habituellement observés dans le secteur concerné].
2. Une signature numérique qui ne satisfait pas aux conditions énoncées au paragraphe 1 est considérée comme une signature électronique [renforcée] si:
- a) il existe des preuves suffisantes montrant que:
 - i) le certificat rattache avec précision la clef publique à l'identité du [sujet du certificat] [...]; et
 - ii) la signature numérique a été dûment créée et vérifiée [pendant la période d'effet d'un certificat valide] par une procédure de sécurité fiable; ou
 - b) elle satisfait aux critères définissant les signatures électroniques [renforcées] énoncées dans d'autres dispositions des présentes Règles.

Références

- A/CN.9/454, par. 117 à 138;
- A/CN.9/WG.IV/WP.76, par. 32 à 38;
- 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

47. Le projet d'article 9 a été revu de manière à tenir compte de la décision prise par le Groupe de travail à sa trente-troisième session (A/CN.9/454, par. 136) d'inclure les variantes A et B dans le texte pour examen ultérieur. Cet article énonce les conditions qu'une signature numérique doit remplir pour être considérée comme une signature électronique [renforcée]. Une signature électronique [renforcée] est définie de manière générale au paragraphe b) du projet d'article premier comme une signature qui remplit certaines conditions. Le Groupe de travail souhaitera peut-être examiner la question de savoir si les conditions énoncées au projet d'article 9 s'ajoutent aux conditions générales de la définition ou visent à préciser ou développer ces conditions. La version actuelle du paragraphe 2 b) du projet d'article 9, toutefois, dispose qu'une signature numérique peut être considérée comme une signature électronique [renforcée], même si elle ne satisfait pas aux exigences du paragraphe 1 du projet d'article 9, à condition qu'elle satisfasse aux critères définissant une signature électronique [renforcée] énoncés dans d'autres dispositions des Règles. Il faudrait alors qu'elle satisfasse à la définition du projet d'article premier. S'il n'est pas clair, d'après son libellé, que le projet d'article 9 développe les conditions énoncées au projet d'article premier, les Règles établiront deux normes différentes pour ce qui doit être considéré comme une signature électronique [renforcée].

48. Le Groupe de travail souhaitera peut-être examiner le projet d'article 9 dans le contexte du projet d'article premier, en se concentrant en particulier sur la technologie des signatures numériques. Le projet d'article pourrait traiter plus particulièrement, par exemple, de la façon dont une signature numérique pourrait satisfaire aux exigences du paragraphe b) i) à iii) de l'article premier.

CHAPITRE III. AUTORITÉS DE CERTIFICATION ET QUESTIONS CONNEXES

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

1. Lorsqu'elle émet un certificat [renforcé], l'autorité de certification garantit [à toute personne qui se fie raisonnablement à ce certificat [renforcé]]:
 - 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 [renforcé] sont exactes à la date de son émission, [sauf si elle a déclaré dans le certificat [renforcé] que l'exactitude de certaines informations n'est pas confirmée];
 - c) qu'à sa connaissance, n'a été omis du certificat [renforcé] aucun fait substantiel 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 [renforcé].]

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

- a) que la clef publique et la clef privée du [signataire] [sujet] indiquées dans le certificat [renforcé] constituent une paire de clefs opérationnelle; et
- b) qu'à la date de l'émission du certificat [renforcé], la clef privée:
 - i) est celle du [signataire] [sujet] indiqué dans le certificat [renforcé];
 - ii) correspond à la clef publique donnée dans le certificat [renforcé],

Références

- A/CN.9/454, par. 139 à 144;
A/CN.9/WG.IV/WP.76, par. 39;
A/CN.9/446, 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

49. Le projet d'article 10 tient compte de la décision prise par le Groupe de travail à sa trente-troisième session (A/CN.9/454, par. 140 à 144), bien qu'il ait été convenu que cet article devrait être examiné ultérieurement en association avec les projets d'articles 11 et 12.

50. Le texte révisé du projet d'article 10 est limité dans son application aux signatures électroniques [renforcées] dans la mesure où il n'est peut-être pas approprié d'appliquer une norme obligatoire à tous les types de certificats, dont la diversité et les différents usages risquent d'augmenter à l'avenir.

Article 11. Responsabilité contractuelle

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. 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] [serait par elle-même inéquitable et aboutirait à un déséquilibre évident entre les parties] [donnerait de façon injustifiée un avantage excessif à une partie], eu égard à l'objet du contrat et à d'autres circonstances pertinentes.

Références

- A/CN.9/454, par. 145 à 157;
- A/CN.9/WG.IV/WP.76, par. 40;
- 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

51. Le projet d'article 11 tient compte de la décision du Groupe de travail à sa trente-troisième session (A/CN.9/454, par. 149) de conserver dans les Règles uniformes un article conçu sur le modèle de l'article 11. La crainte a été exprimée, à cette session, que les termes "manifestement inéquitable" ne soient pas compris dans tous les systèmes juridiques (A/CN.9/454, par. 152). Il a été rappelé au Groupe de travail que le paragraphe 2 était inspiré des principes d'UNIDROIT relatifs aux contrats de commerce international (art. 7.1.6) et qu'il tentait d'établir une norme uniforme pour l'évaluation de l'acceptabilité générale des clauses d'exonération. Le fait d'indiquer que la limitation ou l'exclusion de la responsabilité pouvait être "manifestement inéquitable" dénotait une approche souple en la matière, qui avait pour but de promouvoir une reconnaissance des clauses limitatives et exclusives plus large que cela ne serait le cas si les Règles uniformes mentionnaient uniquement la loi applicable en dehors d'elles (A/CN.9/WG.IV/WP.73, par. 64). D'autres mots ont été ajoutés entre crochets afin de mieux expliquer l'expression "manifestement inéquitable". Ces mots sont repris des notes explicatives de l'article 7.1.6 des Principes d'UNIDROIT.

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 ou omissions y apparaissant, sauf si elle prouve qu'elle-même ou ses agents ont pris toutes les mesures raisonnables pour éviter des erreurs ou des omissions 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 pour enregistrer l'annulation promptement après réception de l'avis d'annulation; et
- c) des conséquences imputables au non-respect de toute procédure énoncée dans la déclaration relative aux pratiques d'authentification qu'elle a publiée.

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 [dans la mesure où]:

- a) l'objet de cette démarche est contraire à l'objet pour lequel le certificat a été émis;
- b) il s'agit d'une transaction dont la valeur dépasse la valeur pour laquelle le certificat est valide; ou
- c) [...].]"

Références

- A/CN.9/454, par. 158 à 163;
A/CN.9/WG.IV/WP.76, par. 41;
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

52. À sa trente-troisième session, le Groupe de travail est convenu que les projets d'articles 10, 11 et 12 devraient être examinés conjointement à une session ultérieure pour veiller à ce que les obligations imposées aux autorités de certification correspondent aux règles de responsabilité énoncées dans les Règles uniformes (A/CN.9/454, par. 159), mais que le projet d'article 12 devrait être conservé et révisé pour tenir compte d'un certain nombre de changements de forme. Ces changements ont été apportés dans le présent texte révisé.

Remarques générales concernant les projets d'articles 13 à 15

53. Faute de temps, le Groupe de travail n'a procédé qu'à un examen préliminaire des projets d'articles 13, 14 et 15 (A/CN.9/454, par. 164 à 169). Quelques craintes ont été exprimées concernant leur niveau de précision et les hypothèses techniques sur lesquelles ils étaient fondés. Il a été proposé de ne pas les appliquer aux signatures numériques et, puisqu'ils traitaient des obligations principales d'une autorité de certification, de déterminer tout d'abord ce que devraient être ces obligations avant d'examiner les questions de responsabilité. Il a été convenu de conserver les projets d'articles entre crochets en vue d'un examen ultérieur.

[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 clés certifiée est tenu d'annuler le certificat correspondant ou d'en demander l'annulation lorsqu'il sait que la clé 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.

4. 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.

5. [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.

[6. 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.]"]

[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."

[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."]

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.*