



Assemblée générale

Distr. LIMITÉE

A/CN.9/WG.IV/WP.82
29 juin 1999

FRANÇAIS
Original: ANGLAIS

COMMISSION DES NATIONS UNIES
POUR LE DROIT COMMERCIAL INTERNATIONAL
Groupe de travail sur le commerce électronique
Trente-cinquième session
Vienne, 6-17 septembre 1999

PROJET DE RÈGLES UNIFORMES SUR LES SIGNATURES ÉLECTRONIQUES

Note du Secrétariat

TABLE DES MATIÈRES

	<u>Paragraphes</u>	<u>Page</u>
INTRODUCTION	1 - 12	2
I. OBSERVATIONS GÉNÉRALES	13 - 20	4
II. PROJETS D'ARTICLES SUR LES SIGNATURES ÉLECTRONIQUES	21 - 71	6
Article premier. Champ d'application	21	6
Article 2. Définitions	22 - 33	6
Article 3. [Non-discrimination] [Neutralité technique]	34	12
Article 4. Interprétation	35	12
Article 5. Dérogation conventionnelle	36 - 40	12
Remarques générales concernant les projets d'articles 6 à 8	41	13
Article 6. [Respect des exigences concernant la signature] [Présomption de signature]	42 - 44	14
Article 7. [Présomption d'original]	45	16
Article 8. Détermination de la signature électronique [renforcée]	46	16
Remarques générales concernant les projets d'articles 9 et 10	47 - 49	17
Article 9. [Responsabilités] [Devoirs] du détenteur de la signature	50 - 55	17
Article 10. Foi accordée à une signature électronique renforcée	-	21
Article 11. Foi accordée à un certificat	56 - 58	22
Article 12. [Obligations] [Devoirs] d'un certificateur d'informations	59 - 68	24
Article 13. Reconnaissance des signatures et certificats étrangers	69 - 71	34

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"). 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 que 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.

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

5. 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). Il a été 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 découlaient du recours accru aux signatures numériques et autres signatures électroniques. Il a également été 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 montraient que le projet de Règles uniformes sur les signatures

électroniques prenait progressivement la forme d'une structure utilisable. La Commission a réaffirmé la décision qu'elle avait prise à sa trentième session en ce qui concerne la faisabilité de l'élaboration de Règles uniformes et exprimé sa conviction 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 noté avec satisfaction 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 posait le commerce électronique et pour chercher des solutions à ces problèmes³.

6. À sa trente-deuxième session (1999), la Commission était saisie du rapport du Groupe de travail sur les travaux de ses trente-troisième (juillet 1998) et trente-quatrième (février 1999) sessions (A/CN.9/454 et 457). Elle a dit sa satisfaction quant aux efforts faits par le Groupe de travail pour rédiger le projet de Règles uniformes sur les signatures électroniques. On s'est généralement accordé à penser que des progrès sensibles avaient été faits lors de ces sessions concernant la définition d'une position commune sur les aspects juridiques des signatures électroniques, mais on a également senti que le Groupe de travail avait eu du mal à parvenir à un consensus sur les principes législatifs sur lesquels les Règles uniformes devraient être fondées.

7. Selon une opinion, l'approche qu'avait adoptée jusqu'ici le Groupe de travail ne tenait pas suffisamment compte de la nécessité, pour le monde des affaires, de souplesse dans l'utilisation des signatures électroniques et autres techniques d'authentification. Telles qu'actuellement envisagées, les Règles uniformes mettaient trop l'accent sur les signatures numériques et sur une application particulière de ces dernières impliquant la certification d'un tiers. On a donc proposé de limiter les travaux sur les signatures électroniques aux aspects juridiques de la certification transnationale ou de les reporter purement et simplement jusqu'à ce que la pratique commerciale soit mieux établie. Selon une opinion allant dans le même sens, aux fins du commerce international, la plupart des questions juridiques liées à l'utilisation des signatures électroniques avaient déjà été résolues dans la Loi type de la CNUDCI sur le commerce électronique. La réglementation de certaines utilisations des signatures électroniques était peut-être nécessaire en dehors du droit commercial, mais le Groupe de travail ne devrait pas s'engager dans une activité de ce type.

8. Selon l'avis qui a largement prévalu, le Groupe de travail devrait poursuivre sa tâche sur la base de son mandat original (voir ci-dessus, par. 3). S'agissant du besoin de règles uniformes sur les signatures électroniques, on a expliqué que, dans de nombreux pays, les gouvernements et les organes législatifs qui avaient entrepris d'élaborer une législation sur les questions relatives aux signatures électroniques, y compris la mise en place d'une infrastructure fondée sur la clef publique ou d'autres projets sur des questions étroitement liées (voir A/CN.9/457, par. 16), attendaient des orientations de la CNUDCI. Quant à la décision prise par le Groupe de travail de se concentrer sur les questions et la terminologie de la cryptographie à clef publique, on a rappelé que le jeu des relations entre trois types distincts de parties (les détenteurs des clefs, les autorités de certification et les parties se fiant à la clef) correspondaient à un modèle possible de cryptographie à clef publique, mais que d'autres étaient aussi concevables (sans intervention d'une autorité de certification indépendante, par exemple). L'un des principaux avantages qu'il y avait à se concentrer sur les questions relatives à la cryptographie à clef publique était que l'on pouvait ainsi structurer plus facilement les Règles uniformes par référence à trois fonctions (ou rôles) associées aux paires de clefs, à savoir la fonction d'émetteur de la clef (ou titulaire), la fonction de certification et la fonction de confiance. On s'est généralement accordé à penser que ces trois fonctions étaient communes à tous les modèles de cryptographie à clef publique, et qu'il fallait les traiter de la même façon, qu'elles soient exercées par trois entités séparées ou que deux d'entre elles soient assurées par la même personne (par exemple, lorsque l'autorité de certification était également une partie se fiant à la clef). En outre, on a largement estimé qu'en se concentrant sur les fonctions typiques de la cryptographie à clef publique et non sur un modèle particulier, on parviendrait peut-être plus facilement à élaborer, à un stade ultérieur, une règle tout à fait neutre techniquement (ibid., par. 68).

9. À l'issue du débat, la Commission a réaffirmé ses décisions précédentes quant à la faisabilité de la rédaction de règles uniformes (voir ci-dessus, par. 3 et 5) et s'est déclarée certaine que le Groupe de travail pourrait progresser encore à ses prochaines sessions.

10. La présente note contient un projet révisé de dispositions élaboré à la suite des délibérations et décisions du Groupe de travail et des délibérations et décisions de la Commission à sa trente-deuxième session, dont il est rendu compte ci-dessus. Il tient compte des décisions prises par le Groupe de travail à sa trente-quatrième session. Les dispositions qui ont été nouvellement revues sont signalées par soulignement.

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.

Référence à des lois nationales et à d'autres textes

12. Pour certains articles on a, à des fins d'information et de comparaison, fait figurer en petits caractères, sous le titre ci-dessus, des extraits de lois nationales et d'autres textes. Les lois nationales citées sont celles dont le secrétariat a connaissance et qui sont accessibles. Les autres textes émanent d'organisations internationales ou sont très connus et accessibles à tous. Les abréviations renvoient aux lois et textes suivants:

- Allemagne Loi de 1997 sur les signatures numériques (Article 3 de la loi sur les services d'information et de communication approuvée le 13 juin 1997 et entrée en vigueur le 1^{er} août 1997);
- Illinois États-Unis d'Amérique; Loi de 1998 sur la sécurité du commerce électronique (Loi 3180 du Parlement de l'Illinois, 1997; 5Ill. Comp. Stat. 175, entrée en vigueur en août 1998);
- Minnesota États-Unis d'Amérique; Loi sur l'authentification électronique (Minnesota Statutes §325, entrée en vigueur en mai 1997);
- Missouri États-Unis d'Amérique; Loi sur les signatures numériques, 1998 (1998 SB 680, entrée en vigueur en juillet 1998);
- Singapour Loi de 1998 sur les transactions électroniques, loi n°25 de 1998.
- Principes directeurs de l'ABA "Principes directeurs relatifs aux signatures numériques", Section des sciences et techniques de l'American Bar Association, 1996;
- Conseil européen Proposition de directive du Parlement européen et du Conseil sur un cadre commun pour les signatures électroniques, 1999 (7015/99);
- Guidec Chambre de commerce internationale, "General Usage for International Digitally Ensured Commerce", 1997.

I. OBSERVATIONS GÉNÉRALES

13. 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.

14. 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.

15. 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).

16. 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. Le projet de Règles uniformes a été élaboré en partant du principe que ces Règles constitueraient un instrument juridique séparé. Deux nouveaux articles s'inspirant de dispositions de la Loi type ont été ajoutés, à savoir les articles premier (Champ d'application) et 4 (Interprétation). Les transactions dans lesquelles interviennent des consommateurs ne sont pas expressément exclues du champ d'application des Règles uniformes, mais la note figurant dans la Loi type a été reprise à l'article premier du projet de Règles uniformes afin de préciser que ces dernières ne sont pas conçues pour se substituer à quelque disposition du droit national que ce soit traitant de la protection du consommateur.

17. Le Groupe de travail souhaitera peut-être examiner la question de savoir si un préambule aux Règles uniformes serait susceptible d'en préciser l'objet, 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.

18. À la trente-troisième session du Groupe de travail, on 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). Le Groupe de travail a conclu qu'en l'absence d'un terme plus approprié, le terme "renforcée" serait conservé. C'est pourquoi il figure entre crochets dans le présent projet révisé de Règles uniformes. À la trente-quatrième session (A/CN.9/457, par. 39), on a estimé qu'il pourrait être nécessaire de réexaminer la définition de l'expression "signature électronique renforcée" en même temps que l'architecture générale des Règles uniformes, une fois que l'on aurait clarifié l'objectif de la prise en considération de deux catégories de signature électronique, notamment en ce qui concernait leurs effets juridiques. On a été d'avis que traiter de signatures électroniques renforcées offrant un degré élevé de fiabilité n'était justifié que si les Règles uniformes prévoyaient un équivalent fonctionnel pour des utilisations spécifiques des signatures manuscrites, ce qui pourrait s'avérer particulièrement difficile à réaliser au niveau international sans pour autant être d'une grande utilité pour les transactions commerciales internationales. Il faudrait donc peut-être préciser l'avantage supplémentaire à attendre de l'utilisation d'une "signature électronique renforcée" par rapport à une simple "signature électronique".

19. Compte tenu du débat sur la nécessité de créer une catégorie de "signatures électroniques renforcées", le présent projet révisé de Règles uniformes propose une autre approche dont le Groupe de travail pourra discuter. La définition de l'expression "signature électronique renforcée" figurant à l'alinéa (b) de l'article 2 a été mise entre crochets. Des remarques relatives à la possible modification de cette définition figurent à la suite de l'article 2. Les parties pertinentes de cette définition sont reprises aux projets d'articles 6, 7 et 8 à titre d'options. L'objectif est d'aider le Groupe de travail à déterminer s'il faut éliminer les références tant aux signatures électroniques qu'aux

signatures électroniques renforcées de sorte que les Règles uniformes ne visent qu'une seule catégorie de signature électronique. Les remarques relatives à des propositions particulières figurent à la suite des articles correspondants.

20. Le projet de texte révisé ne limite pas l'application des Règles uniformes aux cas où, soit il existe des exigences juridiques de forme, soit la loi prévoit des conséquences en l'absence de certaines conditions telles que la signature ou l'original. Ainsi, le champ d'application des Règles uniformes est potentiellement plus large que celui de la Loi type, bien que le projet d'article 6 reprenne l'exigence de forme qui figure à l'article 7 de la Loi type. Le Groupe de travail souhaitera peut-être envisager cet élargissement du champ d'application des Règles uniformes.

II. PROJETS D'ARTICLES SUR LES SIGNATURES ÉLECTRONIQUES

Article premier. Champ d'application

Les présentes règles s'appliquent aux signatures électroniques utilisées dans le contexte de relations commerciales* et ne se substituent à aucune loi visant à protéger les consommateurs.

* Le terme "relations commerciales" devrait être interprété au sens large, comme désignant toute relation d'ordre commercial, qu'elle soit contractuelle ou non contractuelle. Les relations d'ordre commercial comprennent, sans s'y limiter, les transactions suivantes: fourniture ou échange de marchandises ou de services; accord de distribution; représentation commerciale; affacturage; crédit-bail; construction d'usines; services consultatifs; ingénierie; licence; investissement; financement; opération bancaire; assurance; accord d'exploitation ou concession; coentreprise et autres formes de coopération industrielle ou commerciale; transport de marchandises ou de voyageurs par voie aérienne ou maritime, par chemin de fer ou par route.

Références aux documents de la CNUDCI

A/CN.9/457, par. 53 à 64.

Remarques

21. Le projet d'article premier a été initialement proposé à la trente-quatrième session du Groupe de travail en tant que paragraphe 1 d'un article consacré à l'autonomie des parties (projet d'article E, A/CN.9/457, par. 55 et 60). Dans la mesure où cette disposition traite à vrai dire de questions relatives au champ d'application des Règles uniformes, elle fait l'objet dans le présent projet de texte d'un article distinct ayant pour titre "Champ d'application". Comme convenu par le Groupe de travail (A/CN.9/457, par. 64), le projet d'article premier est accompagné d'une note qui reprend la définition du terme "commercial" figurant à l'article premier de la Loi type sur le commerce électronique, et reproduit le libellé de la note** de la Loi type concernant la question des consommateurs. Les mots "signatures électroniques utilisées dans le contexte de" ont été ajoutés à l'article pour définir plus précisément l'objet des Règles uniformes.

Article 2. 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 au dit message, et] [toute méthode dans le cadre d'un message de données] pouvant être utilisée[s] pour identifier le détenteur de la signature dans le cadre du message de données et indiquer qu'il approuve l'information qui y est contenue;

[b) Le terme “signature électronique renforcée” désigne une signature électronique dont on peut démontrer par l’application d’une [procédure de sécurité] [méthode]:

- i) qu’elle est particulière au détenteur de la signature [aux fins pour lesquelles] [dans le contexte où] elle est utilisée;
- ii) qu’elle a été créée et apposée au message de données par le détenteur de la signature ou à l’aide d’un moyen dont seul ce détenteur a le contrôle [et par nulle autre personne];
- [iii) qu’elle a été créée et est liée au message de données auquel elle se rapporte d’une manière qui offre une garantie fiable quant à l’intégrité du message”;]

c) Le terme “certificat” désigne un message de données ou un autre enregistrement émis par un certificateur d’informations et supposé établir l’identité d’une personne ou d’une entité détenant [une paire de clefs particulière] [un dispositif de signature particulier];

d) Le terme “message de données” désigne l’information créée, envoyée, reçue ou conservée par des moyens électroniques ou optiques ou des moyens analogues, notamment, mais non exclusivement, l’échange de données informatisées (EDI), la messagerie électronique, le télégraphe, le télex et la télécopie;

e) Le terme “détenteur de la signature” [détenteur du dispositif] [détenteur de la clef] [titulaire] [détenteur du dispositif de signature] [signataire] désigne une personne par qui, ou au nom de qui, une signature électronique renforcée peut être créée et apposée à un message de données.

f) Le terme “certificateur d’informations” désigne une personne ou une entité qui, dans le cours de ses affaires, [fournit des services d’identification] [certifie les informations] qui servent à faciliter l’utilisation de signatures électroniques [renforcées].”

Références aux documents de la CNUDCI

A/CN.9/457, par. 22 à 27; 66 et 67; 89; 109;

A/CN.9/WG.IV/WP.80, par. 7 à 10;

A/CN.9/WG.IV/WP.79, par. 21;

A/CN.9/454, par. 20;

A/CN.9/WG.IV/WP.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

Définition de l’expression “signature électronique”

22. La définition de l’expression “signature électronique” a été révisée conformément à la décision prise par le Groupe de travail à sa trente-quatrième session (A/CN.9/457, par. 23 à 32). Les mots entre crochets “[toute méthode dans le cadre d’un message de données]” ont été inclus dans le texte pour aligner le libellé de la définition figurant dans les Règles uniformes sur celui de l’article 7 de la Loi type.

Définition de l'expression "signature électronique renforcée"

23. Conformément à la décision prise par le Groupe de travail à sa trente-quatrième session (A/CN.9/457, par. 39), la définition de l'expression "signature électronique renforcée" a été révisée de manière à inclure à l'alinéa b) iii) le libellé apparaissant entre crochets, qui constitue un lien nécessaire entre la signature renforcée apposée sur le message de données et l'information contenue dans ce message, sous la forme d'une fonction d'intégrité. Le Groupe de travail voudra peut-être se demander si la notion d'intégrité doit faire partie intégrante de la définition d'une signature électronique renforcée ou si elle se rattache davantage à l'idée d'original, comme c'est le cas dans l'article 8 de la Loi type et le projet d'article 7 des présentes Règles uniformes. Le libellé qui figurait précédemment en tant qu'alinéa ii), ["peut être utilisée pour identifier objectivement le détenteur de la signature dans le cadre du message de données"] a été omis du texte révisé car il figure déjà dans la définition de l'expression "signature électronique" à l'alinéa a).

24. Au début de l'alinéa b), l'ajout du terme "méthode", comme variante de "procédure de sécurité", vise à aligner plus étroitement la terminologie sur celle de la Loi type.

25. A l'alinéa b) ii), les mots "et par nulle autre personne" ont été placés entre crochets car leur insertion soulève un certain nombre de questions. Premièrement, le fait de les inclure dans la définition d'une signature électronique renforcée peut donner à entendre que toute signature qui n'est pas créée et apposée par son détenteur (et qui pourrait donc ne pas être autorisée) n'est pas une signature électronique renforcée. Cette interprétation peut avoir pour effet d'exclure ces signatures du champ d'application de certains articles des Règles uniformes, par exemple les projets d'articles 8, 9 et 10. En particulier, l'application des parties du projet d'article 9 qui ont trait à la responsabilité dans les cas où les dispositifs de signature seraient compromis risquerait d'être incertaine.

26. Deuxièmement, l'inclusion de ces mots impliquerait que, pour qu'une procédure de sécurité ou une méthode soit une signature électronique renforcée, elle puisse démontrer que la signature a été effectivement créée et apposée par son détenteur. Dans la mesure où cela risque d'être impossible pour certaines technologies, une telle exigence pourrait laisser entendre qu'il est nécessaire d'utiliser, en plus du dispositif de signature, un identificateur personnel en recourant par exemple à la biométrie ou à une technique du même type.

27. Une autre question que le Groupe de travail voudra peut-être examiner dans le cadre de l'alinéa b) ii) est la relation entre l'exigence d'un moyen dont "seul ce détenteur a le contrôle" et le paragraphe 2 du projet d'article 9 qui prévoit un contrôle conjoint. Cette question se pose aussi dans le cadre de la définition de l'expression "détenteur de la signature" ci-dessous.

28. A l'alinéa b) iii) les mots "garantie raisonnable" ont été remplacés par les mots "garantie fiable" par souci de cohérence avec la terminologie de l'article 8 de la Loi type.

Définition du terme "certificat"

29. Par souci d'être complet on a inclus dans les Règles uniformes une définition du terme "certificat". Cette définition s'inspire de celle de l'expression "certificat d'identification" figurant dans le document A/CN.9/WG.IV/WP.79 mais cette dernière expression n'a pas été reprise telle quelle dans les Règles uniformes. Le Groupe de travail voudra peut-être se demander si les mots placés entre crochets, "ou une autre caractéristique importante", peuvent être supprimés pour la raison suivante. La notion d'identité peut englober davantage que le nom du détenteur de la signature et renvoyer à d'autres caractéristiques importantes, comme la position ou l'autorité, soit en association avec un nom, soit sans référence à un nom. Partant, il ne serait pas nécessaire d'établir une distinction entre l'identité et d'autres caractéristiques importantes, ni de limiter les Règles uniformes aux cas où seuls sont utilisés les certificats d'identification qui désignent nommément le détenteur de la signature. Pour une autre conception du sens du mot "identité", voir le rapport "Background Paper on Electronic Authentication Technologies

and Issues”, atelier conjoint OCDE-secteur privé sur l’authentification électronique, Californie, 2-4 juin 1999, pages 6 à 9.

30. Le Groupe de travail voudra peut-être examiner la question de savoir si les mots “confirmer l’identité” sont appropriés, étant entendu que le certificat peut en fait non pas confirmer l’identité du détenteur de la signature mais plutôt identifier ce dernier moyennant certaines procédures et certifier que cette identité est liée au dispositif de signature ou à la clef publique indiqués dans le certificat. Pour faire en sorte que les Règles uniformes soient techniquement neutres, le Groupe de travail voudra peut-être également envisager l’emploi d’une formulation neutre de ce point de vue, comme “dispositif de signature”, à la place de “paire de clefs”, dans la mesure où cette dernière expression renvoie spécifiquement aux signatures numériques. L’emploi des mots “paire de clefs” dans la définition du terme “certificat” peut être approprié lorsque des certificats ne sont utilisés que dans un contexte de signature numérique.

Définition du terme “message de données”

31. On a inclus une définition de “message de données” dans le projet de Règles uniformes par souci d’être complet. Le Groupe de travail voudra peut-être examiner la nécessité d’inclure cette définition dans le cadre de la relation entre les Règles uniformes et la Loi type.

Définition du terme “détenteur de la signature”

32. À sa trente quatrième session (A/CN.9/457, par. 47), le Groupe de travail n’a pas conclu son débat sur la définition de “détenteur de la signature”. La définition révisée comprend désormais, entre crochets, un certain nombre de mots qui, de l’avis du Groupe de travail, seraient peut-être plus appropriés que l’expression “détenteur de la signature”. Il conviendra peut-être de revoir cette définition dans le cadre de l’alinéa b) ii) concernant la définition de “signature électronique renforcée” ci-dessus et du paragraphe 2 du projet d’article 9, comme noté au paragraphe 27.

Définition du terme “certificateur d’informations”

33. Le Groupe de travail n’a pas examiné cette définition à sa précédente session et elle reste donc inchangée. Toutefois, compte tenu des débats déjà consacrés à ce point (A/CN.9/457, par. 109), il voudra peut-être se demander si les mots “dans le cours de ses affaires”, qui y figurent, doivent être interprétés comme signifiant que les activités liées à la certification devraient être les activités professionnelles exclusives d’un certificateur d’informations ou si, pour englober des cas tels que la délivrance de certificats par des sociétés de cartes de crédit, il faudrait viser également l’émission de certificats comme activité accessoire d’une entité.

Références à des lois nationales et à d’autres textes

Principes directeurs de l’American Bar Association (ABA)

Première partie: Définitions

1.5 Certificat

Un message qui, au moins,

- 1) identifie l’autorité de certification qui l’émet;
- 2) nomme ou identifie son titulaire;
- 3) contient la clef publique du titulaire;
- 4) indique la période d’effet; et
- 5) est signé numériquement par l’autorité de certification qui l’émet.

1.6 Autorité de certification

Toute personne qui délivre un certificat.

1.27 Partie se fiant au certificat

Toute personne qui a reçu un certificat et une signature numérique vérifiable par référence à une clef publique indiquée dans le certificat et qui est en mesure de s'y fier.

1.30 Signataire

Toute personne qui crée une signature numérique pour un message.

1.31 Titulaire

Toute personne qui:

- 1) est le sujet nommé ou identifié dans un certificat émis à son intention; et
- 2) détient une clef privée qui correspond à une clef publique indiquée dans ce certificat.

Projet de directive de la Communauté européenne

Article 2

Définitions

Aux fins de la présente directive, on entend par:

1. "Signature électronique", une donnée sous forme numérique jointe ou liée logiquement à d'autres données électroniques et servant de méthode d'authentification;
 - 1a. "Signature électronique avancée", une signature électronique qui satisfait aux exigences suivantes:
 - a) être liée uniquement au signataire;
 - b) permettre d'identifier le signataire;
 - c) être créée par des moyens que le signataire puisse garder sous son contrôle exclusif; et
 - d) être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectée;
 2. "Signataire", toute personne qui détient un dispositif de création de signature et qui agit soit pour son propre compte, soit pour celui de l'entité qu'elle représente;
 3. "Données relatives à la création de signature", des données uniques telles que des codes ou des clefs cryptographiques privées, que le signataire utilise pour créer une signature électronique;
 - 3a. "Dispositif de création de signature", un dispositif logiciel ou matériel configuré pour exploiter les données relatives à la création de signature.
 - 3b. "Dispositif de création de signature sécurisée", un dispositif de création de signature qui satisfait aux exigences de l'annexe III.
 4. "Données relatives à la vérification de signatures", des données telles que des codes ou des clefs cryptographiques publiques, qui sont utilisées pour vérifier la signature électronique;
 - 4a. "Dispositif de vérification de signature", un dispositif logiciel ou matériel configuré pour exploiter les données relatives à la vérification de signatures;
 - 4b. "Certificat", une attestation numérique qui lie des données relatives à la vérification de signature à une personne et confirme l'identité de cette personne;
 5. [...]
 6. "Prestataire de service de certification", toute personne physique ou morale qui délivre des certificats ou fournit d'autres services liés aux signatures électroniques.

Allemagne

§2 Définitions

- 1) Au sens de la présente loi, une signature numérique est un sceau apposé sur des données numériques créé à l'aide d'une clef privée et qui permet, par l'utilisation de la clef publique correspondante à laquelle est joint un certificat émis par un certificateur ou par l'Autorité conformément au paragraphe 3, de déterminer qui est le propriétaire de la clef et de s'assurer que les données n'ont pas été falsifiées.
- 2) Au sens de la présente loi, un certificateur est une personne physique ou morale qui se porte garant de l'attribution de clefs publiques à des personnes physiques et possède une licence à ce titre en vertu du paragraphe 4;
- 3) Au sens de la présente loi, un certificat est une attestation numérique concernant l'attribution à une personne physique d'une clef publique auquel est jointe une signature numérique (certificat de clef), ou une attestation numérique spéciale qui renvoie sans risque d'erreur à un certificat de clef et renferme d'autres informations (certificat d'attributs).

GUIDEC

VI. Glossaire

2. Certificat

Message sécurisé par une personne, et qui atteste l'exactitude de faits pertinents aux effets juridiques de l'acte d'une autre personne.

4. Certificateur

Personne qui émet un certificat par lequel elle atteste l'exactitude d'un fait pertinent aux effets juridiques de l'acte d'une autre personne.

12. Certificat de clef publique

Certificat rattachant à son titulaire une clef publique qui correspond à une clef privée détenue par ce titulaire.

14. Titulaire

Personne qui est le sujet d'un certificat.

Illinois

Article 5. Enregistrements et signatures électroniques en général

Article 5-105. Définitions

Le terme "certificat" désigne un enregistrement qui, au minimum: a) identifie l'autorité de certification qui l'émet, b) nomme ou identifie d'une autre manière son titulaire, ou un dispositif ou un agent électronique sous le contrôle du titulaire; c) contient une clef publique correspondant à une clef privée sous le contrôle du titulaire; d) précise sa période d'effet; et e) est signé numériquement par l'autorité de certification qui l'émet.

Les termes "autorité de certification" désignent une personne qui autorise l'émission d'un certificat et en est à l'origine.

Les termes "signature électronique" désignent une signature sous forme électronique jointe ou logiquement associée à un enregistrement électronique.

Les termes "dispositif de signature" désignent une information unique, telle que codes, algorithmes, lettres, chiffres, clefs privées ou numéros d'identification personnels, ou un dispositif matériel à configuration unique, qui est requise, seule ou en association avec d'autres informations ou dispositifs, pour créer une signature électronique attribuable à une personne déterminée.

Singapour

Première partie. Article 2. Interprétation

Le terme "certificat" désigne un enregistrement visant à appuyer des signatures numériques et qui est censé confirmer l'identité ou d'autres caractéristiques importantes de la personne détenant une paire de clefs particulière;

Les termes "autorité de certification" désignent une personne ou un organisme qui émet un certificat;

Les termes "signature électronique" désignent les lettres, caractères, chiffres, ou autres symboles sous forme numérique joints ou logiquement associés à un enregistrement électronique, et utilisés ou adoptés dans l'intention d'authentifier ou d'approuver l'enregistrement électronique;

Les termes "paire de clefs", dans un système cryptographique asymétrique, désignent une clef privée et la clef publique à laquelle elle est mathématiquement liée, avec pour caractéristique le fait que la clef publique peut vérifier une signature numérique créée par la clef privée;

Les termes "clef privée" désignent la clef d'une paire de clefs utilisée pour créer une signature numérique;

Les termes "clef publique" désignent la clef d'une paire de clefs utilisée pour vérifier une signature numérique;

Le terme "titulaire" désigne une personne qui est le sujet nommé ou identifié dans un certificat qui lui est délivré, et qui détient une clef privée correspondant à une clef publique indiquée dans ce certificat.

Article 3. [Non-discrimination] [Neutralité technique]

[Aucune des dispositions des présentes Règles n'est appliquée] [Les dispositions des présentes Règles ne sont pas appliquées] de manière à exclure, restreindre ou priver d'effet juridique toute méthode [de signature] satisfaisant aux exigences de [l'article 7 de la Loi type sur le commerce électronique].

Références aux documents de la CNUDCI

A/CN.9/457, par. 53 à 64.

Remarques

34. Le projet d'article 3 a été initialement proposé à la trente-quatrième session du Groupe de travail en tant que paragraphe 3 d'un article portant sur l'autonomie des parties (projet d'article E, A/CN.9/457, par. 55 et 60). Dans la mesure où ce paragraphe 3 traitait des questions de non-discrimination et de neutralité technique, et non de l'autonomie des parties, il fait l'objet, dans le présent projet, d'un article distinct pour le titre duquel deux variantes sont données: "Non-discrimination" et "Neutralité technique". Les mots "à exclure, restreindre ou priver d'effet juridique" ont remplacé les mots "à exclure, restreindre, ou pénaliser" pour préciser le but et l'objet de cette disposition. La référence à l'article 7 de la Loi type sur le commerce électronique serait une référence à cette Loi telle qu'incorporée dans le droit interne.

Article 4. Interprétation

1. Pour l'interprétation des présentes Règles uniformes, il est tenu compte de leur origine internationale et de la nécessité de promouvoir l'uniformité de leur application et le respect de la bonne foi dans le commerce électronique.

2. Les questions concernant les matières régies par les présentes Règles uniformes qui ne sont pas expressément réglées par elles sont tranchées selon les principes généraux dont elles s'inspirent.

Remarques

35. Le projet d'article 4 reprend l'article 3 de la Loi type sur le commerce électronique auquel ont été ajoutés les mots "dans le commerce électronique". On l'a inclus dans le présent texte par souci d'être complet. Le Groupe de travail voudra peut-être s'interroger sur la question de savoir si les Règles uniformes devraient maintenant prendre la forme d'un texte qui ne ferait pas partie de la Loi type, mais qui y serait clairement associé. Si le Groupe de travail en décide ainsi, le projet d'article 4 pourrait fournir des principes directeurs pour l'interprétation des Règles uniformes par les tribunaux et autres autorités nationales ou locales. Il devrait avoir pour effet de favoriser l'interprétation du texte uniforme, une fois incorporé dans la législation locale, compte tenu de ses origines et de son caractère internationaux, plutôt que par référence aux concepts du droit local uniquement.

Article 5. Dérogation conventionnelle

Variante A

[Les parties sont libres, par convention expresse ou tacite, de déroger à tout aspect des présentes Règles ou de s'en écarter.] [Il est possible de déroger à tout aspect des présentes Règles ou de s'en écarter, par convention expresse ou tacite.] à moins que cette dérogation ou cet écart ne porte atteinte aux droits des tiers.

Variante B

1. Les présentes Règles sont sans effet sur tout droit qui pourrait exister de modifier par convention l'une des règles de droit visées aux articles 6 et 7.

2. Il est possible de déroger à tout aspect des articles 9 à 12 des présentes Règles ou de s'en écarter par convention expresse ou tacite, à moins que cette dérogation ou cet écart ne porte atteinte aux droits des tiers.

Références aux documents de la CNUDCI

A/CN.9/457, par. 53 à 64.

Remarques

36. La variante A du projet d'article 5 reflète la décision prise par le Groupe de travail à sa trente-quatrième session d'inclure, pour l'examiner ultérieurement, une disposition garantissant la liberté des parties de convenir entre elles de la possibilité de déroger aux dispositions des présentes Règles ou de s'en écarter uniquement pour les transactions les concernant. Une telle convention, toutefois, ne peut porter atteinte aux droits des parties qui ne sont pas parties à cette convention, à savoir les tiers. Cette disposition sur l'autonomie se rapporte uniquement aux présentes Règles et n'a pas d'incidences sur les dispositions d'ordre public ou sur les dispositions impératives applicables aux contrats telles que les dispositions relatives aux contrats léonins.

37. La variante B reconnaît que les dispositions des projets d'articles 6 et 7 des Règles uniformes, qui s'inspirent des articles 7 et 8 de la Loi type, font référence à des prescriptions légales qui peuvent avoir un caractère impératif dans le droit national et ne pas être modifiables par convention. Le paragraphe 1 autorise des dérogations conventionnelles lorsque ces prescriptions impératives du droit national peuvent être modifiées dans le sens souhaité. Ainsi formulé, il reprend le libellé du paragraphe 2 de l'article 4 de la Loi type qui traite de la même question.

38. Le paragraphe 2 de la variante B préserve l'autonomie complète des parties au regard des projets d'article 9 à 12. Il repose sur le principe que les dispositions des projets d'article 9 à 12 seraient des règles de droit positif qui s'appliqueraient en l'absence de convention entre les parties contractantes visant à déroger à ces dispositions ou à en modifier l'application entre elles. Les parties seraient libres de changer ces dispositions ou de ne pas les accepter. Le paragraphe 2 vise à garantir qu'une convention de cette nature ne portera pas préjudice aux tiers, mais ne vise pas à invalider une partie quelconque de la convention passée entre les parties.

39. Les dispositions relatives à la reconnaissance internationale ne seraient pas modifiables par convention, sauf si cette possibilité y est expressément prévue.

40. Le Groupe de travail voudra peut-être examiner la formulation du projet d'article 5 et les questions qu'il soulève quant au respect de ce qui peut constituer des prescriptions légales de caractère impératif dans les projets d'article 6 et 7. Il voudra peut-être également examiner comment le principe de l'autonomie des parties devrait s'appliquer aux projets d'articles 9 à 12. Cette disposition pourrait établir, par exemple, des règles par défaut qui s'appliqueraient en l'absence de convention contraire entre les parties contractantes, ou établir des règles que les parties pourraient convenir d'appliquer.

Remarques générales concernant les projets d'articles 6 à 8

41. Lors d'un débat à sa trente-quatrième session sur le champ d'application des Règles uniformes (A/CN.9/457, par. 48 à 52), le Groupe de travail a décidé d'axer son attention sur les règles applicables aux technologies qui étaient actuellement utilisées dans les transactions commerciales, comme les techniques numériques dans une infrastructure à clef publique. En conséquence il a été décidé que le Groupe de travail se concentrerait sur les projets d'article F à H (dans le présent projet, articles 9 à 12) dans le cadre de l'infrastructure à clef publique. Le débat sur les projets d'article A à D (dans le présent projet, articles 2, 6, 7 et 8) a été reporté à une date ultérieure, après l'examen des articles F à H. On a fait observer que le projet d'article B (dans le présent texte révisé, article 6 – Respect des exigences concernant la signature), en particulier, pourrait jouer un rôle important dans la définition du champ d'application des articles F à H. En outre, on a fait valoir que l'article E (dans le présent projet, article 5 – Dérogation conventionnelle), qui traitait du principe de l'autonomie des parties, serait important pour aborder l'examen des obligations des parties dans les articles F à H.

Article 6. [Respect des exigences concernant la signature] [Présomption de signature]

Variante A

1. Lorsque, dans le cas d'un message de données, il est fait usage d'une signature électronique renforcée, le message de données est présumé signé.
2. Lorsque la loi exige la signature d'une certaine personne, cette exigence est satisfaite dans le cas d'un message de données s'il est fait usage d'une signature électronique dont la fiabilité 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 tout accord en la matière.
- [3. Lorsque la loi exige la signature d'une certaine personne, cette exigence est satisfaite dans le cas d'un message de données s'il est fait usage d'une signature électronique renforcée.]
4. Les paragraphes 2 et 3 s'appliquent, que l'exigence qui y est visée ait la forme d'une obligation ou que la loi prévoit simplement certaines conséquences s'il n'y a pas de signature.
5. Les dispositions du présent article ne s'appliquent pas dans les situations suivantes: [...].

Variante B

1. Lorsque, dans le cas d'un message de données, il est fait usage d'une [méthode] [signature électronique] qui:
 - a) est particulière au détenteur de la signature [aux fins pour lesquelles][dans le contexte où] elle est utilisée;
 - [b) peut être utilisée pour identifier objectivement le détenteur de la signature dans le cadre du message de données; et]
 - c) a été créée et apposée au message de données par le détenteur de la signature ou à l'aide d'un moyen dont seul ce détenteur a le contrôle [et par nulle autre personne];

le message de données est présumé signé.

2. Lorsque la loi exige la signature d'une certaine personne, cette exigence est satisfaite dans le cas d'un message de données, s'il est fait usage d'une signature électronique dont la fiabilité 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.
3. Le paragraphe 2 s'applique, que l'exigence qui y est visée ait la forme d'une obligation ou que la loi prévoit simplement certaines conséquences s'il n'y a pas de signature.
4. Les dispositions du présent article ne s'appliquent pas dans les situations suivantes: [...].

Références aux documents de la CNUDCI

A/CN.9/457, par. 48 à 52;

A/CN.9/WG.IV/WP.80, par. 11 et 12.

Remarques

Variante A

42. La variante A pose que lorsqu'il est fait usage d'une signature électronique renforcée dans le cas d'un message de données, ledit message peut être présumé signé. Le paragraphe 2 reprend le principe de l'article 7 de la Loi type, selon lequel une signature électronique peut satisfaire à l'exigence légale de signature si elle répond à certaines conditions de fiabilité. Le Groupe de travail se souviendra qu'au paragraphe 58 du Guide pour l'incorporation de la Loi type sont mentionnés les facteurs à prendre en considération pour déterminer le niveau de fiabilité approprié. Le paragraphe 3 qui, en disposant qu'une signature électronique renforcée remplit ces conditions, permet de satisfaire plus brièvement aux exigences énoncées à l'article 7 de la Loi type, figure entre crochets. Le Groupe de travail souhaitera peut-être se poser la question de savoir si cette disposition est toujours nécessaire au vu du paragraphe 1.

Variante B

43. La variante B vise à établir une présomption de signature et la satisfaction d'une exigence légale de signature dans le contexte d'une catégorie unique de signature électronique. Il n'y est donc pas question de "signature électronique renforcée". Le paragraphe 1 de cette variante pose que, lorsqu'il est fait usage, dans le cas d'un message de données, d'une méthode qui satisfait certaines exigences, le message de données peut être présumé signé. Cette méthode doit satisfaire aux conditions énoncées dans la définition de la "signature électronique renforcée" figurant à l'alinéa b) du projet d'article 2 sauf en ce qui concerne les critères d'intégrité mentionnés au sous-alinéa b) iii). L'alinéa b) du paragraphe 1 figure entre crochets puisqu'il ne serait nécessaire que si c'est le terme "méthode" qui est retenu au début du paragraphe 1, plutôt que le terme "signature électronique".

44. 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.

Références à des lois nationales et à d'autres textes

Singapour

Partie V. Enregistrements électroniques et signatures sécurisées

Signature électronique sécurisée

17. S'il est possible, par l'application d'une procédure de protection réglementaire ou d'une procédure de protection commercialement raisonnable convenue entre les parties, de vérifier qu'une signature électronique était, au moment ou elle a été faite:

- a) particulière à la personne qui l'utilise;
- b) susceptible d'identifier cette personne;
- c) créée d'une façon ou à l'aide d'un moyen dont seule cette personne a le contrôle; et
- d) liée à l'enregistrement électronique auquel elle se rapporte de telle façon que si cet enregistrement était modifié, la signature électronique serait invalidée;

cette signature est considérée comme une signature électronique sécurisée.

Présomptions relatives aux enregistrements électroniques et aux signatures sécurisées

18. [...]

- 2) Dans toute procédure où il est fait usage d'une signature électronique sécurisée, il est présumé, sauf preuve du contraire, que:

- a) la signature électronique sécurisée est la signature de la personne à laquelle elle se rapporte; et
- b) la signature électronique sécurisée a été apposée par cette personne dans l'intention de signer ou d'approuver l'enregistrement électronique.

Article 7. [Présomption d'original]

1. Lorsque, dans le cas d'un message de données, [il est fait usage d'une signature électronique renforcée] [il est fait usage d'une signature électronique [méthode] qui offre une garantie fiable quant à l'intégrité de l'information à compter du moment où elle a été créée pour la première fois sous sa forme définitive, en tant que message de données ou autre], le message de données est présumé original.
2. Les dispositions du présent article ne s'appliquent pas dans les situations suivantes: [...].

Références aux documents de la CNUDCI

A/CN.9/457, par. 48 à 52;
A/CN.9/WG.IV/WP.80, par. 13 et 14.

Remarques

45. L'objectif du projet d'article 7 est de confirmer la relation avec l'article 8 de la Loi type et l'exigence d'intégrité. Pour le paragraphe 1, deux options sont proposées: selon la première, l'utilisation d'une signature électronique renforcée, telle que définie à l'alinéa b) du projet d'article 2, établira la présomption que le message de données est un original; selon la deuxième, lorsqu'il est fait usage d'une signature électronique ou d'une méthode qui offre une garantie fiable d'intégrité, le message de données peut être présumé original. Bien qu'il ne soit pas toujours nécessaire qu'un original soit signé, une forme de signature électronique, renforcée ou non, peut être utilisée pour vérifier l'intégrité du message de données ou de l'enregistrement.

Article 8. Détermination de la signature électronique [renforcée]

1. *[L'organe ou l'autorité indiqué par l'État adoptant comme compétent en la matière]* peut déterminer [qu'une signature électronique est une signature électronique renforcée] [quelles [méthodes] [signatures électroniques] satisfont aux exigences énoncées aux articles 6 et 7].
2. Toute détermination en vertu du paragraphe 1 doit être conforme aux normes internationales reconnues.

Références aux documents de la CNUDCI

A/CN.9/457, par. 48 à 52;
A/CN.9/WG.IV/WP.80, par. 15.

Remarques

46. Le projet d'article 8 vise à indiquer clairement qu'un État adoptant peut désigner un organe ou une autorité habilitée à déterminer quelles techniques particulières remplissent les conditions requises pour être considérées comme une signature électronique renforcée. La deuxième option proposée pour le paragraphe 1 vise à harmoniser le projet d'article 8 avec les options figurant dans la version révisée des articles 6 et 7. Le paragraphe 2 a pour but d'encourager les États à veiller à ce que toute détermination en vertu du paragraphe 1 soit conforme aux normes internationales, chaque fois qu'il y a lieu, et faciliter ainsi l'harmonisation des pratiques en matière de signatures électroniques renforcées ainsi que l'utilisation et la reconnaissance internationale des signatures.

Remarques générales concernant les projets d'articles 9 et 10

47. Le Groupe de travail voudra peut-être examiner la relation, dans la pratique, entre les projets d'articles 9 et 10. Il existe un certain nombre de combinaisons possibles entre les devoirs énoncés au projet d'article 9 et les conséquences du manquement à ces devoirs eu égard au projet d'article 10. Deux de ces combinaisons serviront à illustrer certains des problèmes à examiner.

48. Le premier cas est celui où le détenteur de la signature ne manque pas au devoir de faire preuve de la diligence voulue conformément au paragraphe 1-c) de l'article 9, mais où la signature ne s'en trouve pas moins compromise pour quelque autre raison. Le détenteur de la signature n'a pas connaissance du fait que sa signature est compromise et n'en avertit donc pas le certificateur d'informations, mais il est improbable qu'il ait ainsi manqué au devoir énoncé au paragraphe 1-b) de l'article 9. Selon le projet d'article 10, la partie se fiant à la signature ne pouvait pas apprendre que la signature était compromise en consultant les renseignements fournis par le certificateur d'informations, et pouvait donc se fier à la signature. Cette situation soulève un certain nombre de questions: Est-il raisonnable pour la partie se fiant à la signature de le faire dans un tel cas? La partie se fiant à la signature supporte-t-elle le risque lié à la confiance? Quelle est la conséquence de cette confiance pour le détenteur de la signature? Le détenteur de la signature est-il lié par ce qui a été signé au moyen de la signature compromise?

49. Le deuxième cas est celui où le détenteur de la signature manque effectivement au devoir de faire preuve de la diligence voulue conformément au paragraphe 1-c) du projet d'article 9, et où la signature est compromise. Le détenteur de la signature sait que la signature a été compromise et en avertit le certificateur d'informations. Selon le projet d'article 10, la partie se fiant à la signature pouvait apprendre que la signature était compromise d'après les renseignements fournis par le certificateur d'informations, et donc ne pas se fier à la signature. Le détenteur de la signature est alors responsable au titre du paragraphe 3 du projet d'article 9, pour avoir manqué aux devoirs énoncés au paragraphe 2, et pour le préjudice subi, conformément au paragraphe 4. Dans ce cas de figure, les conséquences sont beaucoup plus claires que dans le cas exposé au paragraphe 48.

Article 9. [Responsabilités] [Devoirs] du détenteur de la signature

1. Le détenteur d'une signature [a le devoir]:

a) De faire preuve [Fait preuve] de la diligence voulue pour veiller à ce que les déclarations faites par lui concernant l'émission, la suspension ou l'annulation d'un certificat, ou figurant dans ce certificat soient exactes et complètes;

b) D'avertir [Avertit] les personnes voulues sans retard excessif [s'il sait que sa signature a été compromise] [si sa signature a été ou risque d'être compromise];

c) De faire preuve [Fait preuve] de la diligence voulue pour garder le contrôle de sa signature et éviter qu'elle ne soit utilisée sans autorisation, à partir du moment où il détient seul le contrôle du dispositif de signature.

2. Dans le cas [de codétenteurs] [où plus d'une personne a le contrôle] [de la clef] [du dispositif de signature], les [obligations] [devoirs] [prévues][prévus] au paragraphe 1 sont [conjointes] [conjoint] et solidaires.

3. Le détenteur d'une signature est responsable de [l'inexécution des obligations [devoirs] énoncées [énoncés] [la non-satisfaction des exigences énoncées] au paragraphe 1.

4. [La responsabilité du détenteur de la signature ne peut être supérieure au préjudice qu'il avait prévu ou aurait dû prévoir au moment de l'inexécution de ses obligations en considérant les faits dont il savait ou aurait dû savoir qu'ils pouvaient découler de [l'inexécution de ses obligations [devoirs]] [la non-satisfaction des exigences] énoncées [énoncés] au paragraphe 1.]

Références aux documents de la CNUDCI

A/CN.9/457, par. 65 à 98;

A/CN.9/WG.IV/WP.80, par. 18 et 19.

Remarques

Article 9, paragraphe 1

50. Le paragraphe 1 du projet d'article 9 a été revu conformément aux décisions prises par le Groupe de travail à sa trente-quatrième session (A/CN.9/457, par. 73 à 92). Selon le Groupe de travail, le devoir énoncé à l'alinéa a) devrait être limité au processus de certification (A/CN.9/457, par. 92), sans quoi il pourrait être interprété de façon large comme recouvrant les déclarations faites par le détenteur de la signature à une partie se fiant à cette dernière. Étant donné que les déclarations faites dans le cadre de cette relation devraient être régies par le droit du contrat sous-jacent, l'alinéa a) a été remanié de façon à limiter le devoir du détenteur de la signature au processus d'émission, de suspension ou d'annulation d'un certificat.

51. L'alinéa b) a été revu de façon à y inclure les deux variantes dont le Groupe de travail était convenu (A/CN.9/457, par. 83). L'expression "ou aurait dû savoir" n'a pas été incluse car il serait difficile, pour le détenteur de la signature, de satisfaire à un devoir de notification reposant sur une information dont il aurait dû avoir connaissance mais qu'il ignorait en réalité.

52. L'alinéa c) ne porte pas seulement sur l'obligation d'empêcher l'utilisation non autorisée de la signature, mais également sur celle de garder le contrôle de la clef. Cette disposition révisée mentionne également le moment à partir duquel le détenteur d'une signature a le devoir de faire preuve de la diligence voulue. Elle tient ainsi compte de l'avis qui a prévalu au sein du Groupe de travail selon lequel, si le détenteur de la clef n'a le devoir de protéger la clef que pour les paires de clefs effectivement protégées par un certificat, en revanche son devoir de protéger ces clefs certifiées contre toute utilisation abusive devrait être rétroactif jusqu'au moment où il a obtenu seul le contrôle de la paire de clefs (A/CN.9/457, par. 67).

Paragraphe 2

53. Le paragraphe 2 a été ajouté au projet d'article 9 afin de préciser ce qu'est l'obligation de diligence lorsque la même clef est détenue par plusieurs personnes. Le Groupe de travail souhaitera peut-être examiner cette disposition et sa relation avec les exigences énoncées à l'article 2 concernant le contrôle unique de la clef.

Paragraphe 3

54. Ce paragraphe a été revu conformément aux décisions prises par le Groupe de travail à sa trente-quatrième session (A/CN.9/457, par. 93 à 98). La référence aux "conséquences de l'inexécution des obligations [du détenteur de la signature] énoncées au paragraphe 1" a été supprimée i) pour éviter d'avoir à examiner si l'obligation non respectée était contractuelle ou non, et ii) pour éviter toute incertitude pouvant découler de l'emploi du terme "conséquences", qui pourrait laisser penser que toutes les conséquences possibles étaient envisagées, sans donner d'idée quant à la faiblesse du lien causal entre l'inexécution de l'obligation et ces conséquences.

Paragraphe 4

55. Ce paragraphe s'inspire de l'article 74 de la Convention des Nations Unies sur les contrats de vente internationale de marchandises et a été inclus pour examen par le Groupe de travail. Il établit une règle basée sur le critère de prévisibilité du préjudice, mais est limité à l'inexécution des obligations du détenteur de la signature énoncées au paragraphe 1. À la trente-quatrième session du Groupe de travail (A/CN.9/457, par. 93 à 98), on a exprimé la crainte que la responsabilité qui pourrait naître dans le contexte d'un contrat de vente de marchandises ne soit pas la même que la responsabilité qui pourrait découler de l'utilisation d'une signature et ne pourrait pas être quantifiée de la même façon. On a également fait remarquer que le critère de prévisibilité n'était peut-être pas approprié dans le contexte d'une relation contractuelle entre le détenteur de la signature et le certificateur d'informations, mais qu'il pouvait se révéler utile dans le contexte d'une relation entre le détenteur de la signature et une partie se fiant à la signature. Le Groupe de travail souhaitera peut-être examiner ces questions lors de ses futures délibérations sur ce projet d'article ainsi que la relation entre le projet d'article 9 et le projet d'article 10.

Références à des lois nationales et à d'autres textes

Alinéa a) du paragraphe 1: déclarations

Principes directeurs de l'American Bar Association

4.2. Obligations du titulaire

Toutes les déclarations faites par le titulaire à une autorité de certification, y compris toutes les informations dont le titulaire a connaissance et qui figurent dans le certificat, doivent être exactes et faites de bonne foi, qu'elles soient confirmées ou non par l'autorité de certification.

GUIDEC

VII. Sécurisation d'un message

7. Déclarations faites au certificateur

Un titulaire doit communiquer au certificateur tous les faits importants pour le certificat.

Illinois

Article 20. Devoirs des titulaires

Chapitre 20-101. Obtention d'un certificat

Toutes les déclarations pertinentes faites sciemment par une personne à une autorité de certification dans le but d'obtenir un certificat désignant cette personne comme le titulaire doivent être exactes, complètes, et faites de bonne foi.

Chapitre 20-105. Acceptation d'un certificat

[...]

b) En acceptant un certificat, le titulaire nommé dans ce certificat affirme à toute personne qui se fie raisonnablement aux informations qui y sont contenues, de bonne foi et pendant sa période d'effet, que:

- 1) il détient légitimement la clef privée correspondant à la clef publique indiquée dans le certificat;
- 2) toutes les déclarations faites par lui à l'autorité de certification et importantes pour les informations figurant dans le certificat sont exactes; et
- 3) toutes les informations figurant dans le certificat dont il a connaissance sont exactes.

Singapour

Partie IX. Devoirs des titulaires

Obtention d'un certificat

37. Toutes les déclarations faites par le titulaire à une autorité de certification dans le but d'obtenir un certificat, y compris toutes les informations connues du titulaire et figurant dans le certificat, sont exactes, complètes et faites de bonne foi, qu'elles soient confirmées ou non par l'autorité de certification.

Alinéa b) du paragraphe 1: notification

Principes directeurs de l'American Bar Association

4.4 Demande de suspension ou d'annulation

Tout titulaire ayant accepté un certificat doit demander à l'autorité de certification qui l'a émis de le suspendre ou de l'annuler si la clef privée correspondant à la clef publique mentionnée dans le certificat a été compromise.

Illinois

Article 20. Devoirs des titulaires

Chapitre 20-110. Annulation d'un certificat

Sauf si une autre règle de droit applicable en dispose autrement, lorsqu'une clef privée correspondant à la clef publique mentionnée dans un certificat valide est perdue, volée, accessible à une personne non autorisée ou compromise d'une autre manière au cours de la période d'effet du certificat, un titulaire ayant appris que la clef était compromise doit demander sans délai à l'autorité de certification qui l'a émis de révoquer le certificat et de publier un avis d'annulation partout où le titulaire a préalablement autorisé la publication du certificat, ou de notifier d'une autre manière cette annulation dans des conditions raisonnables.

Chapitre 10-125. Création et contrôle des dispositifs de signature

Sauf si une autre règle de droit applicable en dispose autrement, lorsque la création, la validité ou la fiabilité d'une signature électronique créée selon une procédure de sécurité remplissant les conditions requises en vertu [...] dépend du caractère secret ou du contrôle d'un dispositif de signature détenu par le signataire:

- 1) La personne qui génère ou crée le dispositif de signature doit le faire de façon fiable;
- 2) Le signataire et toutes les autres personnes ayant légitimement accès à ce dispositif de signature doivent faire preuve de la diligence voulue pour en conserver le contrôle et le caractère secret, et pour le protéger contre tout accès, divulgation ou utilisation non autorisés pendant la période où il est raisonnable de se fier à une signature créée à l'aide de ce dispositif;
- 3) Si le signataire, ou toute autre personne ayant légitimement accès au dispositif de signature, sait ou a des raisons de penser que le caractère secret ou le contrôle de ce dispositif de signature a été compromis, il doit faire un effort raisonnable pour avertir sans délai toutes les personnes dont il sait qu'elles sont susceptibles de subir de ce fait un préjudice ou, s'il a accès à un mécanisme de publication approprié [...], de publier un avis et désavouer toutes les signatures créées ultérieurement.

Singapour

Demande de suspension ou d'annulation

40. Tout titulaire qui a accepté un certificat demande dès que possible à l'autorité de certification qui l'a émis de le suspendre ou de l'annuler si la clef privée correspondant à la clef publique mentionnée dans le certificat a été compromise.

Alinéa c) du paragraphe 1: utilisation non autorisée

Principes directeurs de l'American Bar Association

4.3 Sauvegarde de la clef privée

Au cours de la période d'effet d'un certificat valide, le titulaire ne compromet pas la clef privée correspondant à une clef publique mentionnée dans ce certificat, et doit également éviter de la compromettre au cours de toute période de suspension.

GUIDEC

VII. Sécurisation d'un message

6. Sauvegarde du dispositif de sécurisation

Si une personne sécurise un message à l'aide d'un dispositif, elle doit faire preuve, au minimum, d'une diligence raisonnable pour éviter l'utilisation non autorisée de ce dispositif.

Illinois

Chapitre 10-125. Création et contrôle de dispositifs de signature

Sauf si une autre règle de droit applicable en dispose autrement, lorsque la création, la validité ou la fiabilité d'une signature électronique créée au moyen d'une procédure de sécurité remplissant les conditions requises en vertu [...] dépend du caractère secret ou du contrôle d'un dispositif de signature détenu par le signataire:

- 1) la personne qui génère ou crée le dispositif de signature doit le faire de façon fiable;

2) le signataire et toutes les autres personnes ayant légitimement accès à ce dispositif de signature doivent faire preuve d'une diligence raisonnable pour conserver le contrôle et le caractère secret du dispositif de signature, et pour le protéger contre tout accès, divulgation ou utilisation non autorisés pendant la période où il est raisonnable de se fier à une signature créée à l'aide de ce dispositif;

3) si le signataire, ou toute autre personne ayant légitimement accès à ce dispositif de signature, sait ou a des raisons de penser que son caractère secret ou son contrôle a été compromis, il doit faire un effort raisonnable pour avertir sans délai toutes les personnes dont il sait qu'elles sont susceptibles de ce fait de subir un préjudice ou, lorsqu'il a accès à un mécanisme de publication approprié [...], publier un avis et désavouer toutes les signatures créées ultérieurement.

Paragraphes 3 et 4: responsabilité

Minnesota

325K.12 Déclarations et devoirs découlant de l'acceptation des certificats

Subd.4 Dédommagement par le titulaire

Lorsqu'il accepte un certificat, un titulaire s'engage à dédommager l'autorité de certification qui l'a émis pour toute perte ou tout préjudice causés par l'émission ou la publication d'un certificat sur la base:

- 1) d'une fausse déclaration du titulaire concernant des faits essentiels;
- 2) de la dissimulation, par le titulaire, d'un fait essentiel, si la déclaration ou la dissimulation a été faite avec l'intention de tromper l'autorité de certification ou une personne se fiant au certificat, ou s'apparente à la faute grave. Le dédommagement prévu au présent chapitre ne peut être ni refusé ni limité contractuellement. Toutefois, un contrat peut contenir des clauses compatibles et supplémentaires concernant le dédommagement.

Singapour

Partie IX. Devoirs des titulaires

Contrôle de la clef privée

39. 1) Lorsqu'il accepte un certificat émis par une autorité de certification, le titulaire identifié dans le certificat s'engage à faire preuve d'une diligence raisonnable pour conserver le contrôle de la clef privée correspondant à la clef publique indiquée dans ce certificat et pour empêcher qu'elle ne soit portée à la connaissance d'une personne non autorisée à créer la signature numérique du titulaire.

- 2) Ce devoir demeure pendant la période d'effet et pendant toute suspension du certificat.

Article 10. Foi accordée à une signature électronique renforcée

1. Une personne [est] [n'est pas] fondée à se fier à une signature électronique renforcée dans la mesure où il [est] [n'est pas] raisonnable de le faire.

2. Pour déterminer s'il [est] [n'est pas] raisonnable de se fier à la signature, il est tenu compte, s'il y a lieu, des facteurs suivants:

- a) La nature de l'opération sous-jacente que la signature est censée étayer;
- b) L'adoption ou non par la partie se fiant à la signature de mesures appropriées pour en déterminer la fiabilité;
- c) Le fait que la partie se fiant à la signature savait ou aurait dû savoir que celle-ci avait été compromise ou annulée;
- d) Toute convention ou toute pratique existant entre la partie se fiant à la signature et le titulaire ou tout usage commercial pouvant s'appliquer;
- e) Tout autre facteur pertinent.

Article 11. Foi accordée à un certificat

1. Une personne [est] [n'est pas] fondée à se fier à un certificat dans la mesure où il [est] [n'est pas] raisonnable de le faire.
2. Pour déterminer s'il [est] [n'est pas] raisonnable de se fier au certificat, il est tenu compte, s'il y a lieu, des facteurs suivants:
 - a) Toutes restrictions dont le certificat peut faire l'objet;
 - b) L'adoption ou non par la partie se fiant au certificat de mesures appropriées pour en déterminer la fiabilité, y compris la consultation d'une liste d'annulations de certificats, le cas échéant;
 - c) Toute convention ou toute pratique existant entre la partie se fiant au certificat et le certificateur d'informations ou le titulaire ou tout usage commercial pouvant s'appliquer;
 - d) [Tout] [Tous les] autre[s] facteur[s] pertinent[s].

Références aux documents de la CNUDCI

A/CN.9/457, par. 99 à 107;

A/CN.9/WG.IV/WP.80, par. 20 et 21.

Remarques

56. Les projets d'articles 10 et 11, qui portent respectivement sur la question de savoir s'il est raisonnable de se fier à une signature électronique renforcée et à un certificat, ont été remaniés conformément à l'avis qui a prévalu au sein du Groupe de travail à sa trente-quatrième session (A/CN.9/457, par. 107) quant à leur contenu. Présenté au départ sous la forme d'un article unique traitant de la foi accordée aussi bien aux signatures qu'aux signatures étayées par un certificat, le projet distingue à présent ces deux points du fait que des considérations différentes s'appliquent à chacun d'entre eux. Le Groupe de travail souhaitera peut-être examiner s'il est nécessaire d'inclure une règle sur la foi accordée aux certificats, en plus d'une règle concernant la foi accordée aux signatures, et quels facteurs devraient être pris en considération dans chaque cas pour déterminer si la foi accordée est raisonnable.

57. On a déclaré, dans le Groupe de travail, craindre qu'en indiquant dans les projets d'articles 10 et 11 qu'une personne était fondée à se fier à une signature ou à un certificat, on établisse une présomption quant à certains effets juridiques alors qu'en énonçant les facteurs à prendre en considération pour décider si la foi accordée pouvait être considérée comme raisonnable on évite d'aborder la question des effets juridiques que pourraient avoir la signature ou le certificat. Selon un avis contraire, le fait d'indiquer dans les projets d'articles qu'une personne était fondée à se fier à une signature ou à un certificat ajoutait un avantage qui n'existait pas dans la Loi type et ne créait pas d'effet juridique concernant la validité de la signature. Comme convenu par le Groupe de travail, les projets d'articles révisés comportent une formulation affirmative et une formulation négative et indiquent les facteurs à prendre en considération dans le cas des signatures et dans le cas des certificats.

58. Le lien entre, d'une part, les projets d'articles 10 et 11 et, d'autre part, l'article 13 de la Loi type a aussi suscité quelques craintes et on s'est demandé si les projets d'articles 9, 10 et 11, lus conjointement, constitueraient une règle sur l'attribution. Le Groupe de travail souhaitera peut-être examiner le lien existant entre, d'une part, les projets d'articles 10 et 11 et, d'autre part, le projet d'article 9 et l'article 13 de la Loi type.

Références à des lois nationales et à d'autres textes

Principes directeurs de l'American Bar Association

5.3 Signatures numériques non fiables

- 1) [...]
- 2) Sauf disposition contraire de la loi ou du contrat, une partie se fiant à une signature numérique assume le risque que cette signature ne soit pas valable en tant que signature ou authentification du message signé, s'il n'est pas raisonnable de s'y fier compte tenu des circonstances, conformément aux facteurs énumérés dans le principe directeur 5.4 (caractère raisonnable de la foi accordée à la signature).

5.4 Caractère raisonnable de la foi accordée à la signature

Les facteurs énumérés ci-après, notamment, sont importants pour déterminer s'il est raisonnable pour un destinataire de se fier à un certificat et à des signatures numériques vérifiables par référence à la clef publique mentionnée dans le certificat:

- 1) Les faits dont la partie se fiant à la signature a connaissance ou dont elle a été informée, y compris tous les faits énumérés dans le certificat ou y étant incorporés par référence;
- 2) La valeur ou l'importance du message portant la signature numérique, si celle-ci est connue;
- 3) La pratique existant entre la personne se fiant à la signature et le titulaire ainsi que les indices de fiabilité ou de non-fiabilité disponibles en dehors de la signature numérique;
- 4) L'usage commercial, en particulier les transactions effectuées à l'aide de systèmes fiables ou d'autres moyens informatiques.

2.3 Caractère prévisible de la foi accordée à un certificat

On peut prévoir que les personnes se fiant à une signature numérique se fieront également à un certificat valable contenant la clef publique à l'aide de laquelle la signature numérique peut être vérifiée.

GUIDEC

VIII. Certification

1. Effet d'un certificat valable

Une personne est fondée à penser qu'un certificat valable représente fidèlement le ou les faits qui y sont énoncés et à s'y fier, si elle n'a pas été avisée que le certificateur n'a pas rempli une des conditions essentielles requises dans la pratique en matière de messages sécurisés.

Singapour

Partie VI. Effet des signatures numériques

Signatures numériques non fiables

22. Sauf disposition contraire de la loi ou du contrat, une personne se fiant à un enregistrement électronique portant une signature numérique assume le risque que la signature numérique ne soit pas valable en tant que signature ou authentification de l'enregistrement électronique signé, s'il n'est pas raisonnable, en l'occurrence, de se fier à la signature numérique, compte tenu des facteurs suivants:
- a) Les faits dont la personne se fiant à l'enregistrement électronique portant la signature numérique a connaissance ou dont elle a été informée, y compris tous les faits énumérés dans le certificat ou incorporés dans celui-ci par référence;
 - b) La valeur ou l'importance de l'enregistrement électronique portant la signature numérique, si celle-ci est connue;
 - c) La pratique existant entre la personne se fiant à l'enregistrement électronique portant la signature numérique et le titulaire ainsi que les indices de fiabilité ou de non-fiabilité disponibles en dehors de la signature numérique; et
 - d) Tout usage commercial, en particulier les transactions effectuées à l'aide de systèmes fiables ou d'autres moyens électroniques.

Article 12. [Obligations] [Devoirs] d'un certificateur d'informations

1. Un certificateur d'informations [a l'obligation] [notamment]:
 - a) [D'agir] [Agit] conformément aux déclarations qu'il fait concernant ses pratiques;
 - b) [De prendre] [Prend] des mesures raisonnables pour s'assurer de l'exactitude de tous les faits ou informations qu'il certifie dans le certificat, [y compris l'identité du détenteur de la signature];
 - c) [De fournir] [Fournit] des moyens raisonnablement accessibles qui permettent à une partie se fiant au certificat de s'assurer:
 - i) De l'identité du certificateur d'informations;

- ii) Du fait que la personne qui est [nommée] [identifiée] dans le certificat détient [au moment pertinent] [la clef privée correspondant à la clef publique] [le dispositif de signature] indiqué[e] dans le certificat;
 - [iii) Du fait que les clefs sont une paire de clefs qui fonctionne];
 - iv) De la méthode employée pour identifier le détenteur de la signature;
 - v) De toutes restrictions quant aux fins ou à la valeur pour lesquelles la signature peut être utilisée; et
 - vi) Du fait que le dispositif de signature est valable et n'a pas été compromis;
- d) [De fournir] [Fournit] un moyen permettant au détenteur de la signature d'avertir qu'une signature électronique renforcée a été compromise et d'assurer [assure] un service prompt d'annulation;
- e) [De faire] [Fait] preuve de la diligence voulue afin de veiller à l'exactitude et à l'exhaustivité de toutes les déclarations faites par lui qui sont pertinentes pour l'émission, la suspension ou l'annulation d'un certificat ou qui figurent dans le certificat;
- f) [D'utiliser] [Utilise] des systèmes, des procédures et des ressources humaines fiables pour la fourniture de ses services.

Variante X

2. Un certificateur d'informations est [responsable] [comptable] de l'inexécution des [obligations] [devoirs] [conditions] énoncé[e]s au paragraphe 1.
3. La responsabilité du certificateur d'informations ne peut être supérieure à la perte qu'il prévoyait ou aurait dû prévoir au moment de l'inexécution à la lumière des faits ou problèmes dont il avait connaissance ou aurait dû avoir connaissance comme étant des conséquences possibles de son non-respect des [obligations] [devoirs] [conditions] énoncé[e]s au paragraphe 1.

Variante Y

2. Sous réserve du paragraphe 3, si le préjudice a été causé parce que le certificat était incorrect ou défectueux, un certificateur d'informations est tenu responsable du préjudice subi:
- a) Soit par une partie qui a passé un contrat avec le certificateur d'informations pour la délivrance d'un certificat;
 - b) Soit par une personne qui se fie raisonnablement à un certificat émis par le certificateur d'informations.
3. Un certificateur d'informations n'est pas tenu responsable en vertu du paragraphe 2:
- a) Si et dans la mesure où il a inclus dans le certificat une déclaration limitant la portée ou l'étendue de sa responsabilité envers toute personne; ou
 - b) S'il prouve qu'il [n'a pas été négligent] [a pris toutes les mesures raisonnables pour prévenir le préjudice].

Références aux documents de la CNUDCI

A/CN.9/457, par. 108 à 119;
A/CN.9/WG.IV/WP.80, par. 22 à 24.

Remarques

59. Le projet d'article 12 a été modifié conformément aux décisions prises par le Groupe de travail à sa trente-quatrième session (A/CN.9/457, par. 108 à 119).

Paragraphe 1

60. Le chapeau du paragraphe 1 comporte plusieurs options. Il s'agit d'abord de choisir entre l'emploi, dans la disposition, des mots "à l'obligation de" ou du présent de l'indicatif. Il est proposé, ensuite, d'utiliser ou non le mot "notamment". S'il est employé, le projet d'article 12 contiendrait une liste ouverte et indicative d'obligations. Ce libellé pourrait certes paraître contraignant aux certificateurs d'informations mais le Groupe de travail a estimé qu'il ne serait pas incompatible avec la règle générale qui leur est actuellement appliquée dans de nombreux systèmes juridiques. Si le mot "notamment" est omis, le projet d'article 12 contiendrait une liste exhaustive des obligations auxquelles doit se soumettre un certificateur d'informations, ce qui permettrait de déterminer avec exactitude l'étendue de sa responsabilité et d'éviter qu'un libellé différent ne pose problème dans des pays où un certificateur d'informations pourrait ne pas être soumis à une obligation générale de diligence raisonnable.

61. Quant aux devoirs précis énoncés au paragraphe 1, ils ont été étendus compte tenu des vues exprimées par le Groupe de travail (A/CN.9/457, par. 112 à 114). En ce qui concerne l'alinéa c), les informations devant être fournies par des "moyens raisonnablement accessibles" sont notamment des informations qu'une partie se fiant à la signature pourrait raisonnablement s'attendre à trouver dans un certificat ainsi que d'autres informations qui ne pourraient être obtenues que par référence à une autre source, telle qu'une liste d'annulations de certificats. Le Groupe de travail souhaitera peut-être examiner s'il conviendrait d'indiquer que certaines de ces informations doivent être consignées dans un certificat et si une règle supplémentaire fixant le contenu minimum d'un certificat devrait être incluse dans les Règles uniformes.

62. Le sous-alinéa c-ii) du paragraphe 1 fait référence à une "paire de clefs" et à un "dispositif de signature". Afin que les Règles uniformes soient neutres quant aux techniques employées, le Groupe de travail souhaitera peut-être envisager l'emploi d'une expression neutre comme "dispositif de signature" à la place des mots "paire de clefs", étant donné que cette dernière expression désigne plus particulièrement les signatures numériques. L'emploi des mots "paire de clefs" en rapport avec la définition du "certificat" peut convenir dans les cas où les certificats ne sont utilisés que dans le contexte des signatures numériques.

63. Le sous-alinéa iii) a été inséré à l'alinéa c) du paragraphe 1 conformément à ce qui avait été proposé à la session précédente. Toutefois, le Groupe de travail souhaitera peut-être se demander si cet élément est nécessaire. Si la clef publique mentionnée dans le certificat correspond à la clef privée que possède le détenteur de la signature et si, par conséquent, il existe une correspondance mathématique entre ces deux clefs, on ne voit pas très bien quelle fonctionnalité supplémentaire apporterait une disposition exigeant que la paire de clefs soit "une paire de clefs opérationnelle". Il n'est pas certain non plus que le certificateur d'informations puisse communiquer, en plus de ce qui est requis en vertu du sous-alinéa c) ii) du paragraphe 1, des éléments d'information qui indiquent cette fonctionnalité supplémentaire.

Paragraphe 2 et 3

64. La variante X énonce une règle selon laquelle le certificateur d'informations est responsable de l'inexécution des obligations ou devoirs énoncés au paragraphe 1 tout en laissant aux législations nationales le soin de déterminer quelles pourraient être les conséquences de ce non-respect. Les mots "des conséquences de" ont été supprimés dans le projet révisé d'article 12 pour les mêmes raisons que celles invoquées pour leur suppression au paragraphe 3 du projet d'article 9, à savoir i) éviter d'avoir à se demander si l'obligation à laquelle il a été manqué était contractuelle ou non et ii) éviter toute incertitude pouvant découler de l'emploi du terme "conséquences", qui pourrait laisser croire que toutes les conséquences possibles étaient envisagées sans donner d'idée quant à la faiblesse du lien causal entre ces conséquences possibles et l'inexécution de l'obligation.

65. Le paragraphe 1 ayant été modifié de manière à y inclure deux variantes – une liste d'obligations exhaustive et une autre ouverte et indicative –, le Groupe de travail souhaitera peut-être examiner si la variante X serait plus appropriée au cas où le paragraphe 1 serait libellé sous forme de liste exhaustive.

66. Le paragraphe 3 de la variante X énonce une règle de prévisibilité du préjudice, qui se fonde sur l'article 74 de la Convention des Nations Unies sur les contrats de vente internationale de marchandises. Ce paragraphe vise à limiter l'étendue de toute responsabilité du certificateur d'informations qui pourrait découler des paragraphes 1 et 2.

Variante Y

67. Le Groupe de travail a estimé dans son ensemble (A/CN.9/457, par. 115) qu'il conviendrait de créer une règle uniforme qui ne se contenterait pas de renvoyer à la loi applicable mais énoncerait une règle générale de responsabilité pour négligence, sous réserve d'exonérations contractuelles éventuelles (à condition que cette limitation ne soit pas excessivement injuste) et sous réserve également que le certificateur d'informations s'exonère lui-même en démontrant qu'il s'est acquitté des obligations énoncées au paragraphe 1. Le paragraphe 2 de la variante Y traite de la question de savoir envers qui le certificateur d'informations peut être responsable. Le paragraphe 3 énonce une règle autorisant le certificateur d'informations à se fonder sur toute limitation de responsabilité indiquée dans le certificat et à montrer qu'il n'a pas fait preuve de négligence ou qu'il a pris les mesures raisonnables pour prévenir le préjudice.

68. Comme pour la variante X, le Groupe de travail souhaitera peut-être examiner si une disposition telle que celle qui est proposée dans la variante Y conviendrait si le paragraphe 1 donnait une liste exhaustive d'obligations et non s'il comportait une liste ouverte. Il souhaitera peut-être examiner également la nécessité de préciser, dans le projet de paragraphe 2 de la variante Y, que la responsabilité du certificateur d'informations se limite à l'inexécution par celui-ci des obligations énoncées au paragraphe 1.

Références à des lois nationales et à d'autres textes

Paragraphe 1 de l'article 12: obligations générales

Principes directeurs de l'American Bar Association

3 Autorités de certification

3.1 L'autorité de certification doit utiliser des systèmes fiables

Une autorité de certification doit utiliser des systèmes fiables pour la fourniture de ses services.

3.2 Divuligation

- 1) Une autorité de certification doit divulguer toute déclaration importante relative à ses pratiques de certification ainsi que tout avis d'annulation ou de suspension d'un certificat émis par elle.
- 2) Une autorité de certification doit faire des efforts raisonnables pour avertir toutes personnes dont elle sait qu'elles sont ou dont elle peut prévoir qu'elles seront lésées par l'annulation ou la suspension d'un certificat émis par elle.
- 3) [...]

4) En cas d'événement portant gravement atteinte à la fiabilité de son système ou au certificat émis par elle, l'autorité de certification doit faire des efforts raisonnables pour avertir toutes personnes dont elle sait qu'elles sont ou dont elle peut prévoir qu'elles seront lésées par cet événement ou doit agir conformément aux procédures décrites dans la déclaration relative à ses pratiques de certification.

3.7 Déclarations faites par l'autorité de certification dans le certificat

Par l'émission d'un certificat, une autorité de certification déclare à toute personne qui se fie raisonnablement au certificat ou à une signature numérique vérifiable à l'aide de la clef publique mentionnée dans ledit certificat, qu'elle confirme, conformément à toute déclaration applicable sur les pratiques de certification portée à la connaissance de la personne se fiant au certificat ou à la signature, ce qui suit:

- 1) l'autorité de certification a satisfait à toutes les exigences applicables des présents Principes directeurs pour l'émission d'un certificat et, si elle a publié le certificat ou l'a communiqué de toute autre manière à la personne se fiant raisonnablement au certificat ou à la signature, le titulaire mentionné dans le certificat a accepté,
- 2) le titulaire identifié dans le certificat détient la clef privée correspondant à la clef publique qui figure dans le certificat,
- 3) [...]
- 4) la clef publique et la clef privée du titulaire constituent une paire de clefs opérationnelle, et
- 5) toutes les informations consignées dans le certificat sont exactes, à moins que l'autorité de certification n'y ait indiqué, directement ou par référence, que l'exactitude de certaines informations spécifiées n'est pas confirmée.

En outre, l'autorité de certification déclare n'avoir omis dans le certificat aucun fait important connu qui, s'il était connu, compromettrait la fiabilité de ses déclarations faites en vertu des présents Principes directeurs.

3.9 Suspension du certificat à la demande du titulaire

Sauf lorsqu'un contrat conclu entre l'autorité de certification et le titulaire en dispose autrement, une autorité de certification doit suspendre un certificat le plus rapidement possible à la demande d'une personne qu'elle croit raisonnablement être:

- 1) le titulaire mentionné dans le certificat,
- 2) une personne dûment autorisée à agir au nom du titulaire, ou
- 3) une personne agissant au nom du titulaire, qui n'est pas disponible.

3.10 Annulation du certificat à la demande du titulaire

L'autorité de certification qui a émis un certificat doit l'annuler à la demande du titulaire qui y est mentionné, si elle a confirmation:

- 1) que la personne demandant l'annulation est le titulaire mentionné dans le certificat devant être annulé, ou
- 2) si la personne demandant l'annulation agit en qualité de mandataire, qu'elle a l'autorité suffisante pour le faire.

3.11 Annulation ou suspension sans le consentement du titulaire

Une autorité de certification doit suspendre ou annuler un certificat, que le titulaire qui y est mentionné ait donné ou non son consentement, si elle a confirmation:

- 1) qu'un fait essentiel consigné dans le certificat est faux,
- 2) qu'une condition essentielle préalable à l'émission du certificat n'a pas été remplie, ou
- 3) que la clef privée ou le système fiable de l'autorité de certification a été compromis au point de porter gravement atteinte à la fiabilité du certificat.

Après avoir procédé à la suspension ou à l'annulation, l'autorité de certification doit avertir immédiatement le titulaire mentionné dans le certificat suspendu ou annulé.

3.12 Avis de suspension ou d'annulation

Aussitôt après avoir suspendu ou annulé un certificat, une autorité de certification doit publier un avis de suspension ou d'annulation, si le certificat a été publié, et, s'il ne l'a pas été, informer de la suspension ou de l'annulation toute partie se fiant au certificat qui lui demande des renseignements.

Projet de directive de la Communauté européenne

Annexe II. Exigences concernant les prestataires de service de certification délivrant des certificats agréés

Les prestataires de service de certification doivent:

- a) Démontrer qu'ils jouissent du crédit nécessaire pour offrir des services de certification;
- b) Assurer le fonctionnement d'un service d'annuaire rapide et sûr et d'un service de révocation sûr et immédiat;
- ba) Assurer que la date et l'heure auxquelles un certificat est délivré ou révoqué peuvent être déterminées;
- c) Vérifier, par des moyens appropriés conformément à la législation nationale, l'identité et, le cas échéant, les attributions spécifiques de la personne à laquelle un certificat agréé est délivré;
- d) Employer du personnel ayant les connaissances spécifiques, l'expérience et les qualifications nécessaires à la fourniture des services et, en particulier, des compétences au niveau de la gestion, une expertise dans la technologie des signatures électroniques et une bonne pratique des procédures de sécurité pertinentes; ils doivent également utiliser des procédures et méthodes administratives et de gestion qui soient adaptées et conformes à des normes reconnues;

- e) Utiliser des systèmes fiables et des produits qui soient protégés contre toute modification et qui doivent assurer la sécurité technique et cryptographique des processus pris en charge par eux;
- f) Prendre des mesures contre la contrefaçon des certificats et, au cas où le prestataire de service de certification génère des données servant à la création de signatures, garantir la confidentialité au cours du processus de génération desdites données;
- g) Disposer des ressources financières suffisantes pour fonctionner conformément aux exigences prévues par la présente directive, en particulier pour endosser la responsabilité de dommages, en contractant, par exemple, une assurance appropriée;
- h) Enregistrer toutes les informations pertinentes concernant un certificat agréé pendant une période de temps appropriée, en particulier pour pouvoir fournir une preuve de la certification en justice. Ces enregistrements peuvent être effectués par des moyens électroniques;
- i) Ne pas stocker ou copier les données servant à la création de la signature de la personne à laquelle le prestataire de service de certification a offert des services de gestion de clefs;
- j) Avant d'établir une relation contractuelle avec une personne lui demandant un certificat à l'appui de sa signature électronique, informer cette personne par un moyen de communication durable des conditions précises d'utilisation des certificats, y compris des limites imposées à leur utilisation, de l'existence d'un régime volontaire d'accréditation et des procédures de réclamation et de règlement des litiges. Cette information doit être faite par écrit sous une forme qui puisse être transmise par voie électronique et dans une langue aisément compréhensible. Des éléments pertinents de cette information doivent également être mis à la disposition, sur demande, de tiers qui se fondent sur le certificat;
- k) Utiliser des systèmes fiables pour stocker les certificats sous une forme vérifiable de sorte que:
 - seules les personnes autorisées puissent introduire et modifier des données,
 - l'authenticité de l'information puisse être contrôlée,
 - les certificats soient disponibles au public uniquement dans les cas où le titulaire du certificat a donné son consentement, et
 - toute modification technique mettant en péril ces exigences de sécurité soit apparente pour l'opérateur.

Allemagne

§5 Émission de certificats

- 1) Le certificateur identifie de manière fiable les personnes qui demandent un certificat. Il confirme l'attribution d'une clef publique à une personne ainsi identifiée et assure l'accès à ce certificat, ainsi qu'aux certificats d'attributs, à tout moment et à toute personne par les voies de télécommunication accessibles au public, de manière vérifiable et avec l'accord du propriétaire de la clef.
- 2) À la requête d'une personne demandant un certificat, le certificateur consigne les informations concernant le pouvoir du demandeur de représenter un tiers ou l'autorisation à titre professionnel ou autre indiquée dans le certificat relatif à la signature ou dans un certificat d'attributs, à condition que l'autorisation ou le consentement du tiers concernant l'enregistrement du pouvoir de représentation soit établi de manière fiable.
- 3) À la requête d'une personne demandant un certificat, le certificateur inscrit dans ce dernier un pseudonyme à la place du nom du demandeur.
- 4) Le certificateur prend des mesures pour que les données figurant dans les certificats ne puissent être falsifiées d'une manière qui ne soit pas visible. Il prend également des mesures pour garantir la confidentialité des clefs privées. Les clefs privées ne peuvent pas être stockées par le certificateur.
- 5) Le certificateur emploie du personnel fiable pour exercer les activités de certification et utilise des composants techniques conformément à l'article 14 pour rendre les clefs accessibles et créer les certificats. Cette exigence s'applique également aux composants techniques qui rendent possible la vérification des certificats en vertu de la deuxième phrase du paragraphe 1.

§6 Obligation de donner des instructions

Le certificateur donne des instructions au demandeur en vertu du paragraphe 1 de l'article 5 concernant les mesures nécessaires pour contribuer à sécuriser les signatures numériques et à assurer leur vérification de manière fiable. Il donne aussi des instructions au demandeur concernant ceux des composants techniques qui répondent aux exigences des paragraphes 1 et 2 de l'article 14, et concernant l'attribution de signatures numériques créées avec une clef privée. Il signale au demandeur qu'il peut être nécessaire de signer une nouvelle fois des données accompagnées de signatures numériques avant que la sécurité d'une signature disponible ne diminue avec le temps.

§8 Blocage de certificats

- 1) Un certificateur bloque un certificat si le propriétaire d'une clef ou son représentant le demande, si le certificat a été émis à partir d'informations fausses conformément à l'article 7, si le certificateur a mis fin à ses activités et qu'elles ne sont pas reprises par un autre certificateur, ou si l'Autorité ordonne le blocage conformément à la deuxième phrase du paragraphe 5 de l'article 13. Il doit être indiqué à partir de quel moment la suspension prend effet. Une suspension rétroactive n'est pas autorisée.

GUIDEC

VIII Certification

2. Exactitude des déclarations figurant dans le certificat

Un certificateur doit s'assurer de l'exactitude de tous les faits énoncés dans un certificat valable, à moins qu'il ne soit manifeste d'après le certificat lui-même que certaines des informations n'ont pas été vérifiées.

3. Fiabilité du certificateur

Un certificateur doit:

- a) n'utiliser que des systèmes et procédés d'information techniquement fiables et employer du personnel de confiance pour émettre un certificat, pour suspendre ou annuler un certificat relatif à une clef publique et pour protéger sa clef privée, le cas échéant;
- b) ne pas avoir de conflits d'intérêts qui porterait atteinte à sa fiabilité dans l'émission, la suspension et l'annulation d'un certificat;
- c) s'abstenir de contribuer à l'inexécution par le titulaire de ses obligations;
- d) s'abstenir de tout acte ou omission qui nuirait gravement à la confiance accordée de manière raisonnable et prévisible à un certificat valable;
- e) agir d'une manière digne de confiance à l'égard d'un titulaire et des personnes qui se fient à un certificat valable.

4. Notification des pratiques et des problèmes

Un certificateur doit faire des efforts raisonnables pour notifier à toute personne qui pourrait, de manière prévisible, être visée par:

- a) toute déclaration importante relative à ses pratiques de certification, et
- b) tout fait important soit pour la fiabilité d'un certificat qu'il a émis, soit pour son aptitude à fournir ses services.

8. Suspension sur demande d'un certificat relatif à une clef publique

Le certificateur qui a émis un certificat doit le suspendre promptement à la demande d'une personne s'identifiant comme le titulaire nommé dans un certificat relatif à une clef publique, ou comme une personne qui serait en mesure d'avoir connaissance du fait que la sécurité de la clef privée d'un titulaire a été compromise, comme un agent, un employé, un associé ou un membre de la famille proche du titulaire.

9. Annulation sur demande d'un certificat relatif à une clef publique

Le certificateur qui a émis un certificat relatif à une clef publique doit l'annuler promptement:

- a) après avoir reçu une demande d'annulation du titulaire nommé dans le certificat ou d'un agent autorisé du titulaire, et
- b) après avoir eu confirmation que la personne demandant l'annulation était ce titulaire, ou un agent de ce titulaire habilité à demander l'annulation.

10. Suspension ou annulation d'un certificat relatif à une clef publique sans consentement

Le certificateur qui a émis un certificat relatif à une clef publique doit l'annuler si:

- a) il a eu confirmation qu'un fait pertinent énoncé dans le certificat est faux;
- b) il a eu confirmation que la fiabilité de son système d'information a été compromise d'une manière qui porte gravement atteinte à la fiabilité des certificats.

Le certificateur peut suspendre un certificat raisonnablement contestable pendant le temps nécessaire pour mener une enquête qui soit suffisante pour vérifier les motifs d'annulation conformément au présent article.

11. Notification de l'annulation ou de la suspension d'un certificat relatif à une clef publique

Le certificateur doit, dès qu'il suspend ou annule un certificat relatif à une clef publique, donner notification, comme il convient, de cette annulation ou de cette suspension.

Illinois

Article 15. Effet d'une signature numérique

Article 15-301. Services fiables

Sauf stipulation figurant de manière bien lisible dans la déclaration relative à ses pratiques de certification, l'autorité de certification et la personne tenant à jour un registre doivent exercer leur activité et fournir leurs services de manière fiable.

Article 15-305. Communication

a) Pour chaque certificat qu'elle émet afin que des tiers s'y fient pour vérifier les signatures numériques créées par les titulaires, l'autorité de certification doit publier ou mettre d'une autre manière à la disposition du titulaire et de toutes les parties se fiant au certificat:

- 1) le cas échéant, la déclaration relative à ses pratiques de certification applicable en l'espèce; et
- 2) son certificat qui l'identifie comme titulaire et qui contient la clef publique correspondant à la clef privée qu'elle utilise pour signer numériquement le certificat (son "certificat d'autorité de certification").

b) En cas d'événement compromettant gravement ses activités ou son système, son certificat, ou tout autre aspect de son aptitude à fonctionner de manière fiable, l'autorité de certification doit agir conformément aux procédures régissant un tel événement, qui sont spécifiées dans la déclaration relative à ses pratiques de certification ou, en l'absence de telles procédures, elle doit faire des efforts raisonnables pour avertir les personnes dont elle sait qu'elles risqueraient de manière prévisible de subir un préjudice en raison de cet événement.

Article 15-310. Émission d'un certificat

Une autorité de certification ne peut émettre un certificat à un éventuel titulaire afin de permettre à des tiers de vérifier les signatures numériques créées par ledit titulaire:

- 1) qu'après avoir reçu une demande d'émission de la part d'un titulaire éventuel, et
- 2) qu'après:

- A) s'être conformée à toutes les pratiques et procédures pertinentes énoncées dans la déclaration relative à ses pratiques de certification applicable, le cas échéant; ou
- B) en l'absence de déclaration relative à ses pratiques de certification visant ces questions, avoir vérifié de manière fiable que:
 - i) le titulaire potentiel est la personne à mentionner dans le certificat à émettre;
 - ii) l'information figurant dans le certificat à émettre est exacte; et
 - iii) le titulaire potentiel détient légitimement une clef privée capable de créer une signature numérique, et la clef publique à mentionner dans le certificat peut être utilisée pour vérifier une signature numérique apposée par cette clef privée.

Article 15-315. Informations à fournir au moment de l'émission du certificat

- a) En émettant un certificat afin que des tiers s'y fient pour vérifier les signatures numériques créées par le titulaire, l'autorité de certification donne l'assurance à ce dernier et à toute personne se fiant raisonnablement aux renseignements contenus dans le certificat, de bonne foi et pendant la période d'effet de ce dernier:
 - 1) qu'elle a traité, approuvé et émis, et qu'elle gérera et annulera au besoin le certificat conformément à la déclaration relative à ses pratiques de certification applicable, qui figure ou est incorporée par référence dans le certificat ou dont cette personne a été avisée, ou, autrement, conformément à la présente loi ou à la loi de la juridiction régissant l'émission du certificat;
 - 2) qu'elle a vérifié l'identité du titulaire comme indiqué dans le certificat ou dans la déclaration relative à ses pratiques de certification applicable, ou sinon, elle a vérifié l'identité du titulaire d'une manière fiable;
 - 3) qu'elle a vérifié que la personne demandant le certificat détenait la clef privée correspondant à la clef publique mentionnée dans le certificat; et
 - 4) que, sauf stipulation figurant de manière bien lisible dans le certificat ou dans la déclaration relative à ses pratiques de certification applicable, à sa connaissance à la date où le certificat a été émis, tous les autres renseignements figurant dans le certificat étaient exacts et n'étaient pas de nature à induire gravement en erreur.
- b) Si l'autorité de certification a émis le certificat conformément à la législation d'une autre juridiction, elle fournit également toutes les garanties et fait toutes les déclarations par ailleurs requises par la loi régissant l'émission du certificat.

Article 15-320. Annulation d'un certificat

- a) 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, qui sont énoncées dans la déclaration applicable relative à ses pratiques de certification, ou en l'absence de telles politiques et procédures, dès que possible après:
 - 1) avoir reçu une demande d'annulation du titulaire nommé dans le certificat et avoir eu confirmation que la personne demandant l'annulation était bien le titulaire ou un agent du titulaire habilité à demander l'annulation;
 - 2) avoir reçu une copie certifiée de l'acte de décès du titulaire, ou avoir eu confirmation par d'autres éléments de preuve fiables que le titulaire est décédé;
 - 3) s'être fait présenter des documents donnant effet à la dissolution de la société titulaire ou avoir eu confirmation par d'autres éléments de preuve que le titulaire avait été dissous ou avait cessé d'exister;
 - 4) avoir reçu notification d'une décision exigeant l'annulation, prononcée par un tribunal ou une juridiction compétente; ou
 - 5) avoir eu confirmation que:
 - A) un fait pertinent mentionné dans le certificat était faux,
 - B) il n'avait pas été satisfait à une condition essentielle préalable à l'émission du certificat,
 - C) la clef privée ou le fonctionnement du système de l'autorité de certification avaient été compromis d'une manière portant gravement atteinte à la fiabilité du certificat, ou
 - D) la clef privée du titulaire avait été compromise.
- b) Lorsqu'elle procède à cette annulation, l'autorité de certification doit en aviser le titulaire et les parties se fiant au certificat conformément aux politiques et procédures régissant les avis d'annulation, qui sont spécifiées dans la déclaration applicable relative à ses pratiques de certification ou, en l'absence de telles politiques et procédures, elle doit en aviser promptement le titulaire, publier promptement un avis d'annulation dans tous les registres où elle a antérieurement fait publier le certificat, et par ailleurs informer de l'annulation une partie se fiant au certificat qui lui adresse une demande de renseignements.

Singapour

Partie VIII. Obligations des autorités de certification

Système fiable

27. Une autorité de certification doit utiliser des systèmes fiables dans la prestation de ses services.

Divulgateion

- 28. 1) Une autorité de certification divulgue:
 - a) son certificat qui contient la clef publique correspondant à la clef privée qu'elle utilise pour signer numériquement un autre certificat (dénommé dans le présent article certificat de l'autorité de certification);
 - b) toute déclaration pertinente relative à ses pratiques de certification;
 - c) l'avis d'annulation ou de suspension de son certificat d'autorité de certification; et

- d) tout autre fait portant gravement atteinte soit à la fiabilité d'un certificat qu'elle a émis, soit à son aptitude à fournir ses services.
- 2) En cas d'événement portant gravement atteinte à la fiabilité du système ou au certificat de l'autorité de certification, cette dernière:
 - a) fait des efforts raisonnables pour aviser toute personne dont on sait qu'elle est ou qu'elle sera de manière prévisible touchée par cet événement; ou
 - b) agit conformément aux procédures régissant un tel événement qui sont spécifiées dans la déclaration relative à ses pratiques de certification.

Émission d'un certificat

29. 1) Une autorité de certification peut émettre un certificat à un candidat-titulaire uniquement après:
- a) avoir reçu une demande d'émission du candidat-titulaire; et
 - b) s'être conformée,
 - i) si elle a une déclaration relative à ses pratiques de certification, à toutes les pratiques et procédures qui y sont énoncées, y compris les procédures concernant l'identification du candidat-titulaire; ou
 - ii) en l'absence d'une déclaration relative à ses pratiques de certification, aux conditions énoncées au paragraphe 2.
 - 2) En l'absence d'une déclaration relative à ses pratiques de certification, l'autorité de certification s'assure elle-même ou par l'intermédiaire d'un agent autorisé que:
 - a) le candidat-titulaire est la personne qui doit être mentionnée dans le certificat à émettre;
 - b) si le candidat-titulaire a recours à un ou plusieurs agents, il a autorisé cet agent à avoir la garde de sa clef privée et à demander l'émission d'un certificat mentionnant la clef publique correspondante;
 - c) l'information figurant dans le certificat à émettre est exacte;
 - d) le candidat-titulaire détient légitimement la clef privée correspondant à la clef publique à mentionner dans le certificat;
 - e) le candidat-titulaire détient une clef privée capable de créer une signature numérique; et
 - f) la clef publique à mentionner dans le certificat peut être utilisée pour vérifier une signature numérique apposée par la clef privée détenue par le candidat-titulaire.

Déclarations lors de l'émission d'un certificat

30. 1) Lorsqu'elle émet un certificat, une autorité de certification informe toute personne se fiant raisonnablement audit certificat ou à une signature numérique vérifiable au moyen de la clef publique mentionnée dans le certificat, qu'elle a émis le certificat conformément à toute déclaration applicable relative à ses pratiques de certification, incorporée par référence dans le certificat ou dont la personne se fiant au certificat a été avisée.
- 2) En l'absence d'une telle déclaration, l'autorité de certification déclare s'être assurée:
- a) qu'elle s'est conformée à toutes les dispositions applicables de la présente loi pour l'émission du certificat et, si elle a publié le certificat ou l'a mis d'une autre manière à la disposition de la personne se fiant au certificat, que le titulaire mentionné dans le certificat l'a accepté;
 - b) que le titulaire identifié dans le certificat détient la clef privée correspondant à la clef publique mentionnée dans le certificat;
 - c) que la clef publique et la clef privée du titulaire constituent une paire de clefs opérationnelle;
 - d) que toutes les informations consignées dans le certificat sont exactes, à moins que l'autorité de certification n'ait inclus ou incorporé par référence dans le certificat une déclaration indiquant que l'exactitude de certaines informations spécifiées n'est pas confirmée; et
 - e) qu'elle n'a connaissance d'aucun fait essentiel qui, s'il avait été inclus dans le certificat, porterait atteinte à la fiabilité des déclarations visées aux alinéas a) à d).
- 3) Lorsqu'existe une déclaration applicable relative aux pratiques de certification, qui a été incorporée par référence dans le certificat ou dont la personne se fiant au certificat a été avisée, le paragraphe 2 s'applique dans la mesure où les déclarations ne sont pas incompatibles avec la déclaration relative aux pratiques de certification.

Suspension d'un certificat

31. Sauf convention contraire entre l'autorité de certification et le titulaire, l'autorité de certification qui a émis un certificat suspend ce dernier dès que possible après en avoir reçu la demande d'une personne dont elle peut raisonnablement penser qu'elle est:
- a) le titulaire mentionné dans le certificat;
 - b) une personne dûment autorisée à agir au nom du titulaire; ou
 - c) une personne agissant au nom du titulaire qui n'est pas disponible.

Annulation d'un certificat

32. Une autorité de certification annule un certificat qu'elle a émis:
- a) après avoir reçu une demande d'annulation du titulaire nommé dans le certificat; et avoir eu confirmation que la personne demandant l'annulation est bien le titulaire ou un agent de ce dernier habilité à demander l'annulation;
 - b) après avoir reçu une copie certifiée conforme de l'acte de décès du titulaire, ou avoir eu la confirmation par d'autres éléments de preuve que le titulaire était décédé; ou

c) sur présentation de documents donnant effet à une dissolution du titulaire, ou après confirmation par d'autres éléments de preuve que le titulaire a été dissous ou a cessé d'exister.

Annulation sans le consentement du titulaire

33. 1) Une autorité de certification annule un certificat, avec ou sans le consentement du titulaire mentionné dans ledit certificat, si elle a confirmation:

- a) qu'un fait pertinent mentionné dans le certificat est faux;
- b) qu'il n'a pas été satisfait à une exigence concernant l'émission du certificat;
- c) que sa clef privée ou son système fiable ont été compromis d'une manière qui porte gravement atteinte à la fiabilité du certificat;
- d) que le titulaire est décédé; ou
- e) que le titulaire a été dissous, mis en liquidation ou a cessé d'exister pour d'autres raisons.

2) Lorsqu'elle procède à une telle annulation, pour des motifs autres que ceux exposés aux alinéas d) ou e) du paragraphe 1, elle en avise immédiatement le titulaire mentionné dans le certificat annulé.

Avis de suspension

34. 1) En cas de suspension d'un certificat par une autorité de certification, celle-ci publie immédiatement un avis de suspension signé dans le registre à cet effet mentionné dans le certificat.

2) Lorsqu'un ou plusieurs registres sont indiqués, l'autorité de certification publie des avis signés de la suspension dans chacun d'entre eux.

Avis d'annulation

35. 1) En cas d'annulation d'un certificat par une autorité de certification, celle-ci publie immédiatement un avis signé d'annulation dans le registre à cet effet mentionné dans le certificat.

2) Lorsqu'un ou plusieurs registres sont indiqués, l'autorité de certification publie des avis signés de l'annulation dans chacun d'entre eux.

Article 12, paragraphes 2 et 3: responsabilité

Principes directeurs de l'American Bar Association

3.14. Responsabilité de l'autorité de certification se conformant aux présents principes directeurs

Toute autorité de certification qui se conforme aux présents principes directeurs et à toute loi ou contrat applicable n'est pas responsable du préjudice

- 1) subi par le titulaire d'un certificat qu'elle a émis, ou par toute autre personne, ou
- 2) causé par la confiance accordée à un certificat qu'elle a émis, à une signature numérique vérifiable par référence à une clef publique mentionnée dans un certificat, ou à des informations figurant dans ledit certificat ou un registre.

Projet de directive de la Communauté européenne

Article 6. Responsabilité

1. Les États Membres veillent au moins à ce qu'un prestataire de service de certification qui délivre au public un certificat agréé ou lui garantit un certificat soit responsable du préjudice subi par toute personne qui, de bonne foi, accorde crédit au certificat concernant:

- a) l'exactitude des informations contenues dans le certificat agréé à compter de la date où il a été délivré;
- b) [...]
- c) l'assurance que, au moment de la délivrance du certificat, la personne identifiée dans le certificat agréé détenait les données relatives à la création de signature correspondant aux données relatives à la vérification de signature mentionnées ou identifiées dans le certificat;
- d) l'assurance que les données relatives à la création de signature et les données relatives à la vérification de signature fonctionnent ensemble de façon complémentaire, au cas où le prestataire de service de certification génère les deux dispositifs;

sauf si le prestataire de service de certification prouve qu'il n'a commis aucune négligence.

1a. Les États Membres veillent au moins à ce qu'un prestataire de service de certification qui a délivré au public un certificat en tant que certificat agréé soit responsable de tout préjudice subi par une personne qui, de bonne foi, accorde crédit au certificat concernant l'omission d'enregistrer la révocation du certificat, sauf si le prestataire de service de certification prouve qu'il n'a commis aucune négligence.

3. Les États Membres veillent à ce qu'un prestataire de service de certification puisse indiquer, dans un certificat agréé particulier, les limites fixées à son utilisation; ces limites doivent être reconnaissables par des tiers. Le prestataire de service de certification ne doit pas être tenu responsable du préjudice résultant de l'usage contre-indiqué d'un certificat agréé qui comporte des limites à son utilisation.

4. Les États Membres veillent à ce qu'un prestataire de service de certification puisse indiquer, dans un certificat agréé, la valeur limite des transactions pour lesquelles le certificat peut être utilisé.

Missouri

Article 17.1

En précisant une limite de confiance recommandée dans un certificat, l'autorité de certification qui l'émet et le titulaire qui l'accepte recommandent que les personnes ne se fient au certificat que dans la mesure où le montant total en jeu ne dépasse pas la limite de confiance recommandée.

Article 17.2

Sauf dérogation à la présente disposition, une autorité de certification agréée:

- 1) N'est responsable d'aucun préjudice subi du fait de la confiance accordée à la signature numérique fautive ou falsifiée d'un titulaire, si, s'agissant de la signature numérique fautive ou falsifiée, elle s'est conformée à toutes les exigences pertinentes des articles 1 à 27 de la présente loi;
- 2) N'est pas responsable au-delà du montant indiqué dans le certificat comme étant la limite de confiance recommandée:
 - a) d'un préjudice subi du fait de la confiance accordée à la présentation erronée, dans le certificat, de tout fait que l'autorité de certification agréée est tenue de confirmer; ou
 - b) du non-respect des dispositions de l'article 10 de la présente loi dans l'émission du certificat.
- 3) Est tenue uniquement, en cas d'action en dommages-intérêts pour préjudice imputable à la confiance accordée au certificat, de verser des dommages-intérêts compensatoires directs ne comprenant pas:
 - a) des dommages-intérêts à titre de sanction ou des dommages-intérêts exemplaires;
 - b) des dommages pour manque à gagner, économies non réalisées ou occasions perdues; ou
 - c) un *pretium doloris*.

Singapour

Limites de la responsabilité des autorités de certification agréées

45. Sauf dérogation au présent article, une autorité de certification agréée:

- a) n'est responsable d'aucun préjudice subi du fait de la confiance accordée à la signature numérique fautive ou falsifiée d'un titulaire, si, s'agissant de la signature numérique fautive ou falsifiée, l'autorité de certification agréée s'est conformée aux dispositions de la présente loi;
- b) n'est pas responsable au-delà du montant indiqué dans le certificat comme étant la limite de confiance recommandée:
 - i) d'un préjudice subi du fait de la confiance accordée à la présentation erronée, dans le certificat, de tout fait que l'autorité de certification agréée est tenue de confirmer; ou
 - ii) du non-respect des dispositions des articles 29 et 30 dans l'émission du certificat.

Article 13. Reconnaissance des signatures et certificats étrangers

1. Pour déterminer si, ou dans quelle mesure, un certificat [une signature] produit légalement ses effets, il n'est pas tenu compte du lieu où le certificat [la signature] a été émis [émise], ni de l'État dans lequel l'émetteur a son établissement.

Variante A

2. Les certificats émis par un certificateur d'informations étranger sont reconnus comme équivalant juridiquement aux certificats émis par les certificateurs d'information soumis à ... [la loi de l'État adoptant] si les pratiques du certificateur d'informations étranger offrent un niveau de fiabilité au moins équivalent à celui qui est requis des certificateurs d'informations en vertu 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 entre les États concernés].

3. Les signatures conformes aux lois d'un autre État relatives aux signatures numériques ou autres signatures électroniques sont reconnues comme équivalant juridiquement aux signatures conformes à ... [la loi de l'État adoptant] si les lois de l'autre État exigent un niveau de fiabilité au moins équivalent à celui qui est exigé pour les signatures en vertu 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.]

4. Nonobstant le paragraphe précédent, les parties à des transactions commerciales et autres peuvent spécifier qu'il est nécessaire de recourir à un certificateur d'informations, une catégorie de certificateurs d'informations ou une catégorie de certificats particuliers pour les messages ou signatures qui leurs sont soumis.

Variante B

2. Les certificats émis par un certificateur d'informations étranger sont reconnus comme équivalant juridiquement aux certificats émis par les certificateurs d'informations soumis à ... [la loi de l'État adoptant] si les pratiques du certificateur d'informations étranger offrent un niveau de fiabilité au moins équivalent à celui qui est requis des certificateurs d'informations en vertu de ... [la loi de l'État adoptant].

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

4. 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 certificats et la conservation des enregistrements;
- d) possibilités d'accès à l'information pour les [signataires] [sujets] identifiés 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 au comportement de l'autorité de certification et la loi de l'État adoptant.

Références aux documents de la CNUDCI

- A/CN.9/454, par. 173;
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 D); et
A/CN.9/WG.IV/WP.71, par. 73 à 75.

Remarques

69. Le projet d'article 13 porte sur les questions ayant trait à ce que le Groupe de travail avait appelé la "reconnaissance transfrontière" à sa trente et unième session (A/CN.9/437, par. 77 et 78). Le paragraphe 1 s'inspire d'une proposition faite à la trente-quatrième session du Groupe de travail (A/CN.9/457, par. 120), selon laquelle ce dernier voudrait peut-être envisager de prévoir un article établissant que les certificats ne doivent pas faire l'objet d'une discrimination en fonction du lieu où ils sont émis.

70. La variante A a été rédigée à partir d'une combinaison de plusieurs paragraphes proposés par le Groupe de travail à sa trente-deuxième session (A/CN.9/446, par. 197 à 204). Elle expose ainsi les critères pouvant être

appliqués dans l'État adoptant en vue de reconnaître les certificats émis par des certificateurs d'informations étrangers et les signatures conformes aux lois d'un autre État. Pour le paragraphe 4 il a été tenu compte de l'avis qui a prévalu au sein du Groupe de travail, selon lequel il faudrait reconnaître aux parties à des transactions commerciales et autres le droit de choisir le certificateur d'informations, la catégorie de certificateur d'informations ou la catégorie de certificats auxquels elles souhaitent recourir pour les messages ou les signatures qu'elles reçoivent. L'expression "parties à des transactions commerciales et autres" engloberait les organismes publics agissant en qualité d'entité commerciale.

71. La variante B donne une liste indicative de critères à prendre en compte pour déterminer la fiabilité des certificats étrangers.

Références à des lois nationales et à d'autres textes

Projet de directive de la Communauté européenne

Article 7 Aspects internationaux

1. Les États Membres veillent à ce que les certificats délivrés au public comme certificats agréés par un prestataire de service de certification établi dans un pays tiers soient juridiquement reconnus comme équivalents aux certificats délivrés par un prestataire de service de certification établi dans la Communauté européenne:

- a) si le prestataire de service de certification remplit les conditions énumérées dans la présente directive et a été accrédité dans le cadre d'un régime volontaire d'accréditation établi dans un État membre de la Communauté européenne; ou
- b) si un prestataire de service de certification établi dans la Communauté, qui satisfait aux exigences visées dans la présente directive, garantit le certificat; ou
- c) si le certificat ou le prestataire de service de certification est reconnu dans le cadre d'un accord bilatéral ou multilatéral entre la Communauté et des pays tiers ou des organisations internationales.

2. Afin de promouvoir les services de certification internationaux impliquant des pays tiers et la reconnaissance juridique des signatures électroniques avancées émanant de pays tiers, la Commission fera, le cas échéant, des propositions visant à l'instauration effective de normes et d'accords internationaux applicables aux services de certification. En particulier et si besoin est, elle soumettra des propositions au Conseil concernant des mandats de négociation d'accords bilatéraux et multilatéraux avec des pays tiers et des organisations internationales. Le Conseil statue à la majorité qualifiée.

Allemagne

§15 Certificats étrangers

- 1) Les signatures numériques qui peuvent être vérifiées à l'aide d'une clef publique pour laquelle il existe un certificat étranger provenant d'un autre État Membre de l'Union européenne ou d'un autre État Partie à l'Accord portant création de l'Espace économique européen sont équivalentes aux signatures numériques conformes à la présente loi, à condition d'offrir un niveau de sûreté équivalent.
- 2) Le paragraphe 1 s'applique également à d'autres États, à condition que des accords supranationaux ou internationaux relatifs à la reconnaissance des certificats aient été conclus.

Illinois

Article 25. Utilisation de signatures et enregistrements électroniques par les organismes publics

Chapitre 25-115. Interopérabilité

Dans la mesure où cela est raisonnable compte tenu des circonstances, les règles adoptées par le Département des services centraux de gestion ou par un organisme public concernant l'utilisation d'enregistrements ou de signatures électroniques doivent être formulées de manière à encourager et favoriser la cohérence et l'interopérabilité avec les règles analogues adoptées par des organismes publics d'autres États et par le Gouvernement fédéral.

Singapour

Partie X. Réglementation relative aux autorités de certification

Reconnaissance des autorités de certification étrangères

43. Le Ministre peut, par règlement, disposer que le contrôleur peut reconnaître des autorités de certification établies hors de Singapour lorsqu'elles satisfont aux exigences réglementaires relatives à l'un des points suivants:

- a) La limite de confiance recommandée, le cas échéant, figurant sur un certificat émis par l'autorité de certification;
- b) La présomption énoncée à l'article 20 b) ii) [signature numérique pouvant être considérée comme une signature électronique sécurisée dans certaines circonstances] et à l'article 21 [présomption d'exactitude du certificat s'il est accepté par le titulaire].

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.*

³ *Ibid., cinquante-troisième session, Supplément n° 17 (A/53/17), par. 208.*