NATIONS UNIES **A**

Assemblée générale

A/CN.9/WG.IV/WP.84
Distr. LIMITÉE
8 décembre 1999
FRANÇAIS

Original: ANGLAIS

COMMISSION DES NATIONS UNIES
POUR LE DROIT COMMERCIAL INTERNATIONAL
Groupe de travail sur le commerce électronique
Trente-sixième session
New York, 14-25 février 2000

PROJET DE RÈGLES UNIFORMES SUR LES SIGNATURES ÉLECTRONIQUES

Note du Secrétariat

TABLE DES MATIÈRES

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 et à la possibilité de définir des règles uniformes concernant ces questions. Il a été convenu que les règles uniformes à élaborer 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 référence[1].

2. À sa trentième session (1997), la Commission était saisie du rapport du Groupe de travail sur les travaux de sa trente et unième session (A/CN.9/437). 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 sur les signatures électroniques" ou "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 respecter, en particulier dans les cas de certification transnationale[2].

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). Elle a noté qu'à ses trente et unième et trente-deuxième sessions, il avait eu des difficultés manifestes à parvenir à une position commune sur les nouvelles questions juridiques découlant de l'utilisation accrue des signatures numériques et autres signatures électroniques. Il a également été noté qu'il n'y avait toujours pas de consensus sur la manière dont ces questions pourraient être

abordées dans un cadre juridique internationalement acceptable. Toutefois, la Commission a estimé, dans l'ensemble, que les progrès accomplis jusqu'ici étaient le signe que le projet de règles uniformes sur les signatures électroniques prenait progressivement la forme d'une structure utilisable. La Commission a réaffirmé la décision qu'elle avait prise à sa trentième session sur la faisabilité de la rédaction de telles règles uniformes et s'est déclarée certaine que le Groupe de travail pourrait progresser encore dans ses travaux à sa trente-troisième session sur la base du projet révisé établi par le secrétariat (A/CN.9/WG.IV/WP.76). Au cours du débat, la Commission a noté avec satisfaction que le Groupe de travail était désormais unanimement considéré comme un forum international particulièrement important pour les échanges de vues sur les problèmes juridiques liés au commerce électronique et la recherche de solutions correspondantes[3].

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 compréhension des 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[4].

10. Le Groupe de travail a poursuivi l'élaboration du projet de Règles uniformes à sa trente-cinquième session (Vienne, septembre 1999) sur la base d'une note établie par le secrétariat (A/CN.9/WG.IV/WP.82). Le rapport sur les travaux de cette session figure sous la cote A/CN.9/465.

11. 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 (voir par. 6 à 9). Les dispositions qui ont été nouvellement revues sont signalées par soulignement. Pour plus de commodité, tous les projets de dispositions ont été regroupés à l'annexe I de la présente note.

12. 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

13. 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 l[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

14. 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.

15. 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.

16. 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).

17. 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.

18. 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.

19. 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". À la trente-cinquième session du Groupe de travail, le maintien de la notion de "signature électronique renforcée", décrite comme particulièrement apte à fournir une certitude quant à l'utilisation d'un certain type de signature électronique, à savoir les signatures numériques appliquées au moyen d'infrastructures à clef publique, a bénéficié d'un appui. Mais on a fait valoir, à l'opposé, que cette notion compliquait inutilement la structure des Règles uniformes. En outre, elle se prêterait à des malentendus en laissant entendre que différents niveaux de

fiabilité technique pourraient correspondre à un nombre également diversifié d'effets juridiques. De nombreuses délégations ont exprimé la crainte que l'on considère une signature électronique renforcée comme une notion juridique distincte plutôt que comme la simple expression d'un ensemble de critères techniques dont l'utilisation rendait une méthode de signature particulièrement fiable. Tout en reportant sa décision finale sur la question de savoir si les Règles uniformes se fonderaient sur la notion de "signature électronique renforcée", le Groupe de travail a généralement convenu que, lors de l'établissement d'une version révisée des Règles uniformes en vue de la poursuite du débat à une session ultérieure, il serait utile de présenter une version des projets d'articles qui ne se fondait pas sur cette notion (A/CN.9/465, par. 66).

20. Compte tenu du débat sur la nécessité de créer une catégorie "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, mais n'est employée dans aucune des dispositions de fond des Règles uniformes. Les parties pertinentes de cette définition ont été insérées, quand il y a lieu, dans les dispositions correspondantes. 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. Des remarques relatives à la possible modification de cette définition figurent à la suite de l'article 2. Les remarques relatives à des propositions particulières figurent à la suite des articles correspondants.

21. Comme il a été convenu par le Groupe de travail à sa trente-cinquième session, le présent projet révisé de Règles uniformes se fonde sur le principe que les cas où "la loi exige une signature" ne se limitent pas aux cas où une signature électronique est utilisée pour satisfaire à une prescription légale impérative selon laquelle certains documents doivent être signés pour être valides. Dans la mesure où la loi contient très peu de prescriptions de ce type applicables aux documents utilisés dans les transactions commerciales, une telle interprétation erronée aurait pour résultat pratique de réduire indûment le champ d'application des Règles uniformes. Conformément à l'interprétation des mots "la loi" adoptée par la Commission au paragraphe 68 du Guide pour l'incorporation de la Loi type (selon laquelle "le terme 'loi' doit être interprété comme renvoyant non seulement aux dispositions législatives et réglementaires mais également aux règles découlant de la jurisprudence et autres règles processuelles"), les Règles uniformes (et la Loi type) doivent viser de manière très large l'utilisation des signatures électroniques, puisque la plupart des documents utilisés dans le contexte des transactions commerciales devraient probablement, dans la pratique, satisfaire aux exigences du droit de la preuve concernant la preuve écrite (A/CN.9/465, par. 67).

II. PROJETS D'ARTICLES SUR LES SIGNATURES ÉLECTRONIQUES

Article premier. Champ d'application

Les présentes Règles s'appliquent lorsque des signatures électroniques sont utilisées dans le contexte* d'activités commerciales**. Elles ne se substituent à aucune règle de droit visant à protéger les consommateurs.

* La Commission propose le texte suivant aux États qui souhaiteraient étendre l'applicabilité des présentes Règles:

"Les présentes Règles s'appliquent lorsque des signatures électroniques sont utilisées, sauf dans les situations suivantes: [...]."

** Le terme "commercial" 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.9/465, par. 36 à 42;
A/CN.9/WG.IV/WP.82, par. 21;
A/CN.9/457, par. 53 à 64.

Remarques

22. Les premiers mots du projet d'article premier ont été modifiés à des fins de cohérence avec l'article premier de la Loi type (voir A/CN.9/465, par. 38). La note * vise à suivre le même principe que celui qui avait été adopté dans la Loi type, selon lequel "rien dans la Loi type ne devrait empêcher un État d'élargir le champ d'application de la Loi type pour couvrir les utilisations du commerce électronique en dehors du domaine commercial" (Guide pour l'incorporation de la Loi type, par. 26). Le Groupe de travail a décidé, à sa trente-cinquième session, qu'un tel principe devrait s'appliquer également aux signatures électroniques (ibid., par. 39).

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 audit 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.9/465, par. 42;
A/CN.9/WG.IV/WP.82, par. 22 à 33;
A/CN.9/457, par. 22 à 47; 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

23. Le Groupe de travail a décidé, à sa trente-cinquième session, de reporter l'examen des définitions figurant au projet d'article 2 jusqu'à ce qu'il ait achevé d'examiner les dispositions de fond des Règles uniformes (A/CN.9/465, par. 42).

Définition des termes "signature électronique"

24. La définition des termes "signature électronique" a été rédigée conformément à la décision du 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 des termes "signature électronique renforcée"

25. À sa trente-cinquième session, le Groupe de travail s'est posé la question de savoir s'il fallait utiliser la notion de "signature électronique renforcée" dans les Règles uniformes. Le maintien de cette notion, décrite comme particulièrement apte à fournir une certitude quant à l'utilisation d'un certain type de signature électronique, à savoir les signatures numériques appliquées au moyen d'infrastructures à clef publique, a bénéficié d'un appui. Mais on a fait valoir, à l'opposé, qu'elle compliquait inutilement la structure des Règles uniformes. En outre, elle se prêterait à des malentendus en laissant entendre que différents niveaux de fiabilité pourraient correspondre à un nombre également diversifié d'effets juridiques. De nombreuses délégations ont exprimé la crainte que l'on considère une signature électronique renforcée comme une notion juridique distincte plutôt que comme la simple expression d'un ensemble de critères techniques dont l'utilisation rendait une méthode de signature particulièrement fiable. Tout en reportant sa décision finale sur la question de savoir si les Règles uniformes se fonderaient sur la notion de "signature électronique renforcée", le Groupe de travail a généralement convenu que, lors de l'établissement d'une version révisée des Règles uniformes en vue de la

poursuite du débat à une session ultérieure, il serait utile de présenter une version des projets d'articles qui ne se fondait pas sur cette notion (A/CN.9/465, par. 66).

26. 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" inclut, 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 devrait 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 utilisé pour identifier objectivement le détenteur de la signature dans le cadre du message de données" a été omis du texte actuel car il figure déjà dans la définition des termes "signature électronique" à l'alinéa a).

27. 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.

28. 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 11. 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.

29. 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.

30. 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 projet d'article 9 qui énonce les obligations de "chaque" détenteur d'un dispositif de signature. Cette question se pose aussi dans le cadre de la définition de l'expression "détenteur de la signature" ci-dessous.

31. A l'alinéa b) iii) les mots "garantie fiable" visent à assurer une cohérence avec la terminologie de l'article 8 de la Loi type.

Définition du terme "certificat"

32. Si l'on veut être complet, il pourrait être nécessaire d'inclure 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 du dispositif de 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 du dispositif de 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.

33. 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 du dispositif de 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" ou "dispositif de création 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"

34. Il pourrait être nécessaire d'inclure une définition de "message de données" dans le projet de Règles uniformes si l'on veut 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"

35. 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 projet d'article 9, comme noté au paragraphe 30. Compte tenu de la proposition faite à la trente-cinquième session du Groupe de travail, le terme "détenteur de la signature" a été remplacé dans la présente note par "détenteur du dispositif de signature" (voir A/CN.9/465, par. 78 à 82).

Définition du terme "certificateur d'informations"

36. 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. Compte tenu d'une proposition formulée à la trente-cinquième session du Groupe de travail, le terme "certificateur d'informations" a été remplacé dans le reste du texte par "prestataire de services de certification" (A/CN.9/465, par. 125). Le Groupe de travail souhaitera peut-être prendre une décision quant à la terminologie à employer.

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 privé qui correspond à une clef publique indiquée dans ce certificat.

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;
2. "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 détectable;
3. "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;
4. "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;
5. "dispositif de création de signature", un dispositif logiciel ou matériel configuré pour mettre en application les données afférentes à la création de signature;
6. "dispositif sécurisé de création de signature", un dispositif de création de signature qui satisfait aux exigences de l'annexe III;
7. "données afférentes à la vérification de signature", des données, telles que des codes ou des clefs cryptographiques publiques, qui sont utilisées pour vérifier la signature électronique;
8. "dispositif de vérification de signature", un dispositif logiciel ou matériel configuré pour mettre en application les données afférentes à la vérification de signature;
9. "certificat", une attestation électronique qui lie des données afférentes à la vérification de signature à une personne et confirme l'identité de cette personne;
10. "certificat qualifié", un certificat qui satisfait aux exigences visées à l'annexe I et qui est fourni par un prestataire de service de certification satisfaisant aux exigences visées à l'annexe II;
11. "prestataire de service de certification", toute entité ou 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. [Neutralité technique] [Égalité de traitement des signatures]

Aucune des dispositions des présentes Règles n'est appliquée de manière à exclure, restreindre ou priver d'effet juridique toute méthode [de signature électronique] [satisfaisant aux exigences mentionnées au paragraphe 1 de l'article 6 des présentes Règles] [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] [ou satisfaisant autrement aux exigences de la loi applicable].

Références aux documents de la CNUDCI

A/CN.9/465, par. 43 à 48;
A/CN.9/WG.IV/WP.82, par. 34;
A/CN.9/457, par. 53 à 64.

Remarques

37. Le projet d'article 3 vise à tenir compte de certaines des suggestions de rédaction formulées à la trente-cinquième session du Groupe de travail (A/CN.9/465, par. 47 et 48). Dans le cadre de ses débats sur le projet d'article 3, le Groupe de travail souhaitera peut-être déterminer s'il convient d'indiquer clairement dans les Règles uniformes que toute méthode utilisée ou envisagée à des fins autres que la création de l'équivalent fonctionnel d'une signature manuscrite juridiquement signifiante (à savoir une méthode satisfaisant aux exigences du projet d'article 6 ou satisfaisant autrement aux exigences de la loi applicable) n'entre pas dans le champ d'application desdites Règles.

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.

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.

Références aux documents de la CNUDCI

A/CN.9/465, par. 49 et 50;
A/CN.9/WG.IV/WP.82, par. 35.

Remarques

38. À la trente-cinquième session (A/CN.9/465, par. 50), les membres du Groupe de travail se sont généralement accordés sur le fond du projet d'article 4.

Article 5. [Dérogation conventionnelle] [Autonomie des parties] [Liberté contractuelle]

Il est possible de déroger aux présentes Règles ou [de les modifier] [d'en modifier l'effet] par convention, à moins que lesdites Règles ou la loi de l'État adoptant en disposent autrement.

Références aux documents de la CNUDCI

A/CN.9/465, par. 51 à 61;
A/CN.9/WG.IV/WP.82, par. 36 à 40;
A/CN.9/457, par. 53 à 64.

Remarques

39. Le texte du projet d'article 5 tient compte d'une proposition largement appuyée par le Groupe de travail à sa trente-cinquième session (A/CN.9/465, par. 59), tendant à laisser aux parties la liberté de décider entre elles de déroger aux dispositions des Règles uniformes ou de les modifier. Cette disposition sur l'autonomie des parties ne vaut que pour ces Règles et l'intention n'est pas de porter atteinte à l'ordre public ou aux lois impératives applicables aux contrats, telles que les dispositions relatives aux contrats léonins.

40. Le libellé entre crochets a été inclus comme variante plus proche du libellé de l'article 6 de la Convention des Nations Unies sur les contrats de vente internationale de marchandises (appelée ci-après "la Convention sur les ventes"), conformément à la suggestion du Groupe de travail (ibid., par. 61).

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

1. 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 méthode] [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.

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

Variante A

3. [Une méthode] [Une signature électronique] est présumée fiable en ce qu'elle satisfait à l'exigence indiquée au paragraphe 1 lorsqu'elle garantit:

a) que les données utilisées pour la création d'une signature électronique sont particulières au détenteur du dispositif de [création de] signature dans le contexte dans lequel elles sont utilisées;

b) que le détenteur du dispositif de [création de] signature [a] [a eu au moment pertinent] seul le contrôle de ce dispositif;

c) que la signature électronique est liée [aux informations] [au message de données ou à la partie de ce message] [auxquelles] [auquel] elle se rapporte [d'une manière qui garantit l'intégrité de ces informations];

d) que le détenteur du dispositif de [création de] signature est objectivement identifié dans le contexte [dans lequel le dispositif est utilisé] [du message de données].

Variante B

3. En l'absence de preuve du contraire, il est présumé que l'utilisation d'une signature électronique prouve:

a) la conformité de la signature électronique à la norme de fiabilité énoncée au paragraphe 1;

b) l'identité du signataire présumé; et

c) l'approbation par le signataire présumé des informations auxquelles se rapporte la signature électronique.

4. La présomption établie au paragraphe 3 s'applique uniquement si:

a) la personne qui entend se fier à la signature électronique avise le signataire présumé qu'il se fie à cette signature [en tant qu'équivalent de la signature manuscrite du signataire présumé] [comme preuve des éléments énumérés au paragraphe 3]; et

b) Le signataire présumé n'avise pas promptement la personne qui adresse une notification en vertu de l'alinéa a) des raisons pour lesquelles il ne faut pas se fier à la signature électronique [comme équivalent de sa signature manuscrite] [comme preuve des éléments énumérés au paragraphe 3].

Variante C

3. En l'absence de preuve du contraire, il est présumé que l'utilisation d'une signature électronique prouve:

a) la conformité de la signature électronique à la norme de fiabilité énoncée au paragraphe 1;

b) l'identité du signataire présumé; et

c) l'approbation par le signataire présumé des informations auxquelles se rapporte la signature électronique.

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

Références aux documents de la CNUDCI

A/CN.9/465, par. 62 à 82;
A/CN.9/WG.IV/WP.82, par. 42 à 44;
A/CN.9/457, par. 48 à 52;
A/CN.9/WG.IV/WP.80, par. 11 et 12.

Remarques

41. Les paragraphes 1 et 2 ainsi que le dernier paragraphe du projet d'article 6 contiennent des dispositions tirées de l'article 7-1 b), 7-2 et 7-3 de la Loi type, respectivement. Un libellé inspiré de l'article 7-1 a) de la Loi type figure déjà dans la définition du terme "signature électronique" figurant à l'article 2 a) du projet de Règles uniformes. Toutefois, le projet d'article 2 a) décrit une méthode qui "peut" être utilisée pour remplir les fonctions d'une signature identifiée à l'article 7-1 a) de la Loi type. Si le Groupe de travail souhaite insister sur le fait que le paragraphe 1 vise avant tout le cas où tout type de signature électronique (y compris les méthodes d'authentification "non renforcées") est utilisé à des fins de signature (c'est-à-dire dans l'intention de créer un équivalent fonctionnel d'une signature manuscrite), il pourrait juger plus approprié de reprendre l'intégralité du texte du paragraphe 1 de l'article 7 de la Loi type. Le paragraphe 1 pourrait alors se lire comme suit:

"1) Lorsque la loi exige la signature d'une certaine personne, cette exigence est satisfaite dans le cas d'un message de données:

a) si [une méthode] [une signature électronique] est utilisée pour identifier la personne en question et pour indiquer qu'elle approuve l'information contenue dans le message de données; et

b) si la fiabilité de cette [méthode] [signature électronique] 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 de tout accord en la matière."

42. Il a été déclaré, à la trente-cinquième session du Groupe de travail, qu'il serait peut-être nécessaire d'inclure au projet d'article 6 une disposition rédigée comme suit: "Les conséquences juridiques de l'utilisation d'une signature s'appliquent également à l'utilisation des signatures électroniques" (voir A/CN.9/465, par. 74). Le Groupe de travail souhaitera peut-être examiner dans quelle mesure cette notion d'équivalence entre signatures manuscrites et électroniques devrait être développée dans le corps du texte des Règles uniformes ou s'il pourrait être suffisant (et plus conforme à la Loi type) d'indiquer dans le guide pour leur incorporation (qui sera établi ultérieurement) que, pour l'interprétation du paragraphe 1, il doit être tenu compte du fait que cette disposition a pour objet de garantir que lorsque l'utilisation d'une signature manuscrite aurait eu des conséquences juridiques, l'utilisation d'une signature électronique fiable aura les mêmes conséquences.

43. Comme il est indiqué dans le rapport du Groupe de travail sur les travaux de sa trente-cinquième session (A/CN.9/465, par. 64), le paragraphe 1, dans la mesure où il reprend le paragraphe 1 de l'article 7 de la Loi type, détermine ce qui constitue une méthode de signature fiable compte tenu des circonstances. En vertu de cet article, une telle détermination ne peut émaner que d'un tribunal ou d'un autre juge des faits intervenant *ex post*, peut-être longtemps après l'utilisation de la signature électronique. En revanche, l'avantage escompté des Règles uniformes pour certaines techniques reconnues comme étant particulièrement fiables indépendamment des circonstances dans lesquelles elles sont utilisées, est de créer la certitude (soit par une présomption, soit par une règle de fond), au moment de l'utilisation de cette technique de signature électronique ou avant (*ex ante*), qu'une telle utilisation entraînera des effets juridiques équivalents à ceux d'une signature manuscrite. Tel est l'objet du paragraphe 3.

44. La variante A du paragraphe 3 est basée sur le libellé proposé et examiné à la trente-cinquième session du Groupe de travail (A/CN.9/465, par. 78 à 82), qui vise à exprimer des critères objectifs de fiabilité technique des signatures électroniques. À l'alinéa c), le lien nécessaire entre la signature et les informations signées a été formulé de manière qu'on ne puisse pas penser que la signature électronique ne s'applique qu'à la totalité du contenu d'un message de données. En fait, les informations signées ne constitueront, dans de nombreux cas, qu'une partie de l'information contenue dans le message de données.

45. Quand il examinera les variantes B et C, le Groupe de travail souhaitera peut-être préciser, à titre de principe général si, en ce qui concerne l'établissement des critères de "fiabilité" d'une signature électronique, les Règles uniformes devraient porter exclusivement sur les questions de fiabilité technique envisagées dans la variante A ou s'il conviendrait de tenir compte d'autres facteurs, qui remplaceraient ou compléteraient la variante A.

46. La variante B résulte d'une proposition formulée à la trente-cinquième du Groupe de travail (A/CN.9/465, par. 74 et 75). Si son adoption implique l'élimination de tout lien entre un niveau donné de fiabilité technique, d'une part, et les conséquences juridiques résultant de l'utilisation de signatures électroniques, d'autre part, les paragraphes 3 et 4 auront pour effet de créer, en faveur de toute technique pouvant être utilisée pour produire une signature électronique, ce que l'on a parfois appelé une "faible présomption", c'est-à-dire une présomption pouvant être aisément réfutée par le signataire présumé par simple déclaration. Le Groupe de travail souhaitera

peut-être déterminer à titre de principe général, s'il est réaliste d'imposer aux utilisateurs de signatures électroniques l'échange de notifications envisagé dans la variante B et si un tel échange permettrait d'atteindre le niveau souhaité de convivialité et de certitude prédéterminée quant aux effets juridiques des signatures électroniques.

47. La variante C résulte d'une proposition formulée à la trente-cinquième session du Groupe de travail (A/CN.9/465, par 76). Contrairement à la variante B, elle n'offre pas de mécanisme permettant de réfuter facilement la présomption qu'elle crée. Étant donné que pour établir "la preuve du contraire" il pourrait être nécessaire de procéder à des examens détaillés et coûteux des divers dispositifs et procédures techniques de création d'une signature électronique, elle aurait pour effet de créer une très forte présomption quant à l'efficacité juridique de toute technique utilisée pour produire une signature électronique.

Références à des lois nationales et à d'autres textes

Directive de la Communauté européenne

Article 5
Effets juridiques des signatures électroniques
1. Les États membres veillent à ce que les signatures électroniques avancées basées sur un certificat qualifié et créées par un dispositif sécurisé de création de signature:
a) répondent aux exigences légales d'une signature à l'égard de données électroniques de la même manière qu'une signature manuscrite répond à ces exigences à l'égard de données manuscrites ou imprimées sur papier; et
b) soient recevables comme preuves en justice.
2. Les États membres veillent à ce que l'efficacité juridique et la recevabilité comme preuve en justice ne soient pas refusées à une signature électronique au seul motif que:
– la signature se présente sous forme électronique, ou
– qu'elle ne repose pas sur un certificat qualifié, ou
– qu'elle ne repose pas sur un certificat qualifié délivré par un prestataire accrédité de service de certification, ou
– qu'elle n'est pas créée par un dispositif sécurisé de création de signature.

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. Un message de données est présumé être sous sa forme originale lorsqu'il est fait usage, pour ce message de données, [d'une méthode] [d'une signature électronique] [dans le contexte de l'article 6] qui:

a) 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; et

b) lorsqu'il est exigé qu'une information soit présentée, cette information peut être montrée à la personne à laquelle elle doit être présentée;

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

Références aux documents de la CNUDCI

A/CN.9/465, par. 83 à 89;
A/CN.9/WG.IV/WP.82, par. 45;
A/CN.9/457, par. 48 à 52;
A/CN.9/WG.IV/WP.80, par. 13 et 14.

Remarques

48. Le texte du projet d'article 7 résulte de la décision prise par le Groupe de travail à sa trente-cinquième session (A/CN.9/465, par. 89). Cet article a pour objet de confirmer le lien avec l'article 8 de la Loi type et l'exigence d'intégrité. Tel qu'actuellement rédigé, le paragraphe 1 n'implique aucun lien entre la fonction de préservation de l'intégrité de l'information et la fonction de signature au titre du projet d'article 6. L'indépendance des deux articles, qui peuvent s'appliquer de manière cumulative ou séparée à diverses techniques d'authentification, est fondée sur la reconnaissance du fait que, dans un environnement papier, les deux fonctions correspondantes peuvent être également conçues comme séparées.

Article 8. Satisfaction des exigences des articles 6 et 7

Variante A

1. *[L'Organe ou l'autorité indiqué par l'État adoptant comme compétent en la matière]* peut déterminer quelles méthodes satisfont aux exigences des articles 6 et 7.

2. Toute détermination en vertu du paragraphe 1 est conforme aux normes internationales reconnues.

Variante B

1. Il peut être déterminé qu'une ou plusieurs méthodes de signature électronique satisfont aux exigences des articles 6 et 7.

2. Toute détermination en vertu du paragraphe 1 est conforme aux normes internationales reconnues.

Références aux documents de la CNUDCI

A/CN.9/465, par. 90 à 98;
A/CN.9/WG.IV/WP.82, par. 46;
A/CN.9/457, par. 48 à 52;
A/CN.9/WG.IV/WP.80, par. 15.

Remarques

49. Le projet d'article 8 vise à indiquer clairement qu'un État adoptant peut désigner un organe ou une autorité habilité à déterminer à quelles techniques particulières peuvent s'appliquer les présomptions établies aux projets d'articles 6 et 7. Selon la décision prise par le Groupe de travail à sa trente-cinquième session, le projet d'article 8 ne doit pas être interprété d'une manière qui amènerait, par exemple, à interdire aux utilisateurs de recourir à des techniques dont il n'a pas été déterminé qu'elles satisfaisaient aux exigences des projets d'articles 6 et 7, si ces utilisateurs avaient convenu de procéder ainsi entre eux. Les Parties devraient aussi être libres de démontrer, devant un tribunal judiciaire ou arbitral, que la méthode de signature qu'elles avaient choisie satisfaisait effectivement aux exigences des projets d'articles 6 et 7, même si elle n'avait pas fait l'objet d'une détermination préalable à cet effet. Il ne faut pas voir dans le projet d'article 8 une recommandation aux États concernant le seul moyen d'assurer la reconnaissance des techniques de signature, mais plutôt une indication des limites à appliquer si les États souhaitent adopter une telle approche. Il conviendrait peut-être d'expliquer clairement ces points, éventuellement dans un guide accompagnant les Règles uniformes (voir A/CN.9/465, par. 93).

50. Les variantes A et B ont pour objet d'encourager les États à veiller à ce que les déterminations en vertu du paragraphe 1 soient conformes 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. La variante A mentionne l'intervention possible de l'État dans la désignation d'un organe ou d'une autorité compétent pour évaluer la fiabilité technique des techniques de signature (que cet organe soit une entité publique ou privée). La variante B, pour ne pas trop insister sur le rôle de l'État dans les déterminations visées au paragraphe 1, laisse ouverte la question de savoir si un organe ou une autorité habilitée à évaluer la fiabilité technique des techniques de signature doit être établi par l'État (soit en tant qu'organe public, soit en tant qu'entité privée), ou relever uniquement du secteur privé.

51. Il n'a pas été tenu compte dans la version révisée du projet d'article 8 d'une proposition formulée à la trente-cinquième session du Groupe de travail (à savoir que "toute détermination devrait porter non seulement sur la question de savoir si certaines méthodes satisfaisaient aux exigences énoncées aux projets d'articles 6 et 7, mais également sur la mesure dans laquelle ces exigences étaient satisfaites"). Le Groupe de travail souhaitera peut-être préciser s'il pourrait n'être satisfait que partiellement à une exigence telle que l'utilisation d'une signature manuscrite (ou la production d'un document original) dans le cas d'un document traité dans un environnement électronique, ce qui semblerait s'écarter de l'approche d'équivalence fonctionnelle adoptée lors de l'établissement de la Loi type et des Règles uniformes. Si l'intention du Groupe de travail est simplement d'indiquer qu'une signature électronique (ou une méthode garantissant l'intégrité) ne s'applique pas nécessairement à la totalité du contenu d'un message de données mais doit pouvoir s'appliquer uniquement à une partie déterminée des informations contenues dans ce message, il peut aisément le faire dans le guide accompagnant les Règles uniformes.

Article 9. Responsabilités du détenteur du dispositif de signature

1. Chaque détenteur d'un dispositif de signature:

   a) Prend des dispositions raisonnables pour éviter toute utilisation non autorisée de son dispositif de signature;

   b) Avise les personnes voulues sans retard excessif si:

      i) il sait que le dispositif de signature a été compromis; ou si

ii) au vu des circonstances connues de lui, il y a un risque important que le dispositif de signature ait été compromis;

c) [Lorsqu'un certificat est utilisé pour étayer le dispositif de signature,] [Lorsque le dispositif de signature implique l'utilisation d'un certificat,] prend des dispositions raisonnables pour veiller à ce que toutes les déclarations faites par lui qui concernent le [cycle de vie du] certificat ou qui doivent figurer dans le certificat soient exactes et complètes.

2. Le détenteur d'un dispositif de signature est responsable de la non-satisfaction des exigences énoncées au paragraphe 1.

Références aux documents de la CNUDCI

A/CN.9/465, par. 99 à 108;
A/CN.9/WG.IV/WP.82, par. 50 à 55
A/CN.9/457, par. 65 à 98
A/CN.9/WG.IV/WP.80, par. 18 et 19

Remarques

52. Le projet d'article 9 a été largement approuvé, quant au fond, par le Groupe de travail à sa trente-cinquième session. Au paragraphe 1, le terme "chaque" a été ajouté avant le terme "détenteur" pour tenir compte de l'avis général selon lequel, dans certains cas, il pourrait ne pas être équitable de prévoir que chaque détenteur du dispositif est responsable de la totalité du préjudice auquel peut donner lieu l'utilisation non autorisée du dispositif (par exemple, si le dispositif de signature d'une société a été utilisé sans autorisation par un certain nombre de ses employés). En conséquence, chaque détenteur ne devrait être tenu responsable que dans la mesure où il a personnellement manqué aux obligations énoncées au paragraphe 1 (voir A/CN.9/465, par. 105).

53. Le paragraphe 2 est basé sur la conclusion à laquelle est parvenu le Groupe de travail à sa trente-cinquième session, à savoir qu'il pourrait être difficile d'arriver à un consensus sur les conséquences pouvant découler de la responsabilité du détenteur d'un dispositif de signature. Selon le contexte dans lequel la signature électronique est utilisée, le détenteur du dispositif de signature pourrait, par exemple, en vertu de la loi en vigueur, être lié par le contenu du message ou être tenu de verser des dommages-intérêts. En conséquence, le paragraphe 2 pose simplement le principe selon lequel le détenteur d'un dispositif de signature doit être tenu responsable de la non-satisfaction des exigences énoncées au paragraphe 1 en laissant à la loi applicable en dehors des Règles uniformes dans chaque État adoptant le soin de prévoir les conséquences juridiques découlant d'une telle responsabilité (ibid., par. 108). Selon une autre opinion exprimée à la même session, il aurait fallu insérer dans le projet d'article 9 (ibid., par. 107) une règle fondée sur un critère de prévisibilité du préjudice (inspirée de l'article 74 de la Convention sur les ventes, et réénonçant une règle fondamentale qui s'appliquerait en vertu du droit normalement applicable dans de nombreux pays).

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.

Paragraphe 2: 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. Responsabilités d'un prestataire de services de certification

1. Un prestataire de services de certification:

a) Agit conformément aux déclarations qu'il fait concernant ses pratiques;

b) Fait preuve de la diligence voulue afin de veiller à ce que toutes les déclarations faites par lui qui concernent le cycle de vie du certificat ou qui figurent dans le certificat soient exactes et complètes;

c) Fournit des moyens raisonnablement accessibles qui permettent à une partie se fiant au certificat de s'assurer:

i) de l'identité du prestataire de services de certification;

ii) du fait que la personne qui est identifiée dans le certificat détient au moment pertinent le dispositif de signature indiqué dans le certificat;

iii) de la méthode employée pour identifier le détenteur du dispositif de signature;

iv) de toute restriction quant aux fins ou à la valeur pour lesquelles la signature peut être utilisée; et

v) du fait que le dispositif de signature est valable et n'a pas été compromis;

d) Fournit un moyen permettant au détenteur du dispositif de signature d'avertir qu'un dispositif de signature a été compromis et assure un service prompt d'annulation;

e) Utilise des systèmes, des procédures et des ressources humaines fiables pour la prestation de ses services.

2. Pour déterminer si, et dans quelle mesure, tous systèmes, procédures et ressources humaines sont fiables aux fins de l'alinéa e) du paragraphe 1, il est tenu compte des facteurs 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 du prestataire de services 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 du prestataire de services de certification et la loi de l'État adoptant.

3. Un certificat énonce les éléments suivants:

a) l'identité du prestataire de services de certification;

b) le fait que la personne qui est identifiée dans le certificat détient, au moment pertinent, le dispositif de signature indiqué dans le certificat;

c) le fait que le dispositif de signature était valide à la date ou avant la date à laquelle le certificat a été émis;

d) toute restriction quant aux fins ou à la valeur pour lesquelles le certificat peut être utilisé; et

e) toute restriction quant à la portée ou à l'étendue de la responsabilité que le certificateur accepte envers toute personne.

Variante X

4. Un prestataire de services de certification est responsable de la non-satisfaction des exigences énoncées au paragraphe 1.

5. La responsabilité du prestataire de services de certification 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] [exigences] énoncé[e]s au paragraphe 1.

Variante Y

4. Un prestataire de services de certification est responsable de la non-satisfaction des exigences énoncées au paragraphe 1.

5. Pour l'évaluation du préjudice, il est tenu compte des facteurs suivants:

a) coût de l'obtention du certificat;

b) nature de l'information certifiée;

c) existence et portée de toute restriction quant à l'objet pour lequel le certificat peut être utilisé;

d) existence de toute déclaration limitant la portée ou l'étendue de la responsabilité du prestataire de services de certification; et

e) toute faute concurrente de la partie se fiant au certificat.

Variante Z

4. Si le préjudice a été causé parce que le certificat était incorrect ou défectueux, un prestataire de services de certification est tenu responsable du préjudice subi:

a) soit par une partie qui a passé un contrat avec le prestataire de services de certification pour la délivrance d'un certificat; ou

b) soit par une personne qui se fie raisonnablement à un certificat émis par le prestataire de services de certification.

5. Un prestataire de services de certification 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 pertinente; ou

b) s'il prouve qu'il [n'a pas été négligeant] [a pris toutes les mesures raisonnables pour prévenir le préjudice].

Références aux documents de la CNUDCI

A/CN.9/465, par. 123 à 142 (projet d'article 12);
A/CN.9/WG.IV/WP.82, par. 59 à 68 (projet d'article 12);
A/CN.9/457, par. 108 à 119;
A/CN.9/WG.IV/WP.80, par. 22 à 24.

Remarques

54. Le projet d'article 10 (anciennement projet d'article 12) a été révisé conformément aux décisions prises par le Groupe de travail à sa trente-cinquième session.

55. Les membres du Groupe de travail avaient, à la session précédente, jugé généralement acceptable le paragraphe 1 quant au fond, mais demandé quelques légères modifications de forme. Le paragraphe 2 résulte d'une proposition formulée à cette session, selon laquelle les caractéristiques d'un prestataire de services de certification décrites au projet d'article 13 devraient être retenues non seulement pour les entités étrangères mais aussi pour les prestataires nationaux (A/CN.9/465, par. 136).

56. Le paragraphe 3 découle d'une proposition qui a également suscité un intérêt considérable au sein du Groupe de travail à sa session précédente, selon laquelle le projet d'article 12 devrait établir une règle supplémentaire énonçant le contenu minimum d'un certificat (ibid., par. 135). Les éléments devant figurer dans un certificat sont énumérés dans un paragraphe séparé, mais on conçoit mal que l'alinéa c) du paragraphe 1 et le paragraphe 3 demeurent des dispositions distinctes. Le Groupe de travail souhaitera peut-être préciser si ces deux listes doivent être combinées, probablement à l'alinéa c) du paragraphe 1, qui pourrait commencer par les mots: "indique dans chaque certificat...".

57. Les paragraphes 4 et 5 portent sur la responsabilité du prestataire de services de certification.

58. Dans les variantes X et Y, le paragraphe 4 établit une règle selon laquelle le prestataire de services de certification est responsable du non-respect des obligations ou devoirs énoncés au paragraphe 1, mais laisse à la législation nationale le soin de déterminer les conséquences de ce manquement.

59. Le paragraphe 5 de la variante X établit une règle de prévisibilité du préjudice fondée sur l'article 74 de la Convention sur les ventes. Ce paragraphe vise à limiter toute responsabilité du prestataire de services de certification pouvant découler des paragraphes 1 et 2. Dans la variante Y, le paragraphe 5 est basé sur une proposition formulée à la trente-cinquième session du Groupe de travail (A/CN.9/465, par. 140), selon laquelle

les Règles uniformes pourraient, sans empiéter sur le droit interne, énoncer une liste de facteurs à prendre en considération pour l'application du droit interne aux prestataires de services de certification.

60. La variante Z n'a pas été examinée à la trente-cinquième session du Groupe de travail. Elle découle du sentiment, largement exprimé à la trente-quatrième session (A/CN.9/457, par. 115), qu'il conviendrait de créer une règle uniforme qui ne se limiterait pas à renvoyer à la loi applicable et énoncerait une règle générale de responsabilité pour négligence, sous réserve d'exonérations contractuelles éventuelles (à condition que cette limitation ne soit pas manifestement injuste) et sous réserve que le prestataire de services de certification puisse s'exonérer en démontrant qu'il s'était acquitté des obligations énoncées au paragraphe 1. Le paragraphe 4 de la variante Z traite de la question de savoir envers qui le prestataire de services de certification est responsable. Le paragraphe 5 établit une règle permettant à ce prestataire de se fonder sur toute limitation de la responsabilité énoncée dans le certificat ou de démontrer qu'il n'a pas fait preuve de négligence ou a pris des mesures raisonnables pour prévenir le préjudice (A/CN.9/WG.4/WP.82, par.67).

Références à des lois nationales et à d'autres textes

Paragraphes 1, 2 et 3 – 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 Divulgation
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.

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) faire la preuve qu'ils sont suffisamment fiables pour fournir 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;
c) veiller à ce que la date et l'heure d'émission et de révocation d'un certificat puissent être déterminées avec précision;
d) vérifier, par des moyens appropriés et conformes au droit national, l'identité et, le cas échéant, les qualités spécifiques de la personne à laquelle un certificat qualifié est délivré;
e) 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, des connaissances spécialisées en technologie des signatures électroniques et une bonne pratique des procédures de sécurité appropriées; ils doivent également appliquer des procédures et méthodes administratives et de gestion qui soient adaptées et conformes à des normes reconnues;
f) utiliser des systèmes et des produits fiables qui soient protégés contre les modifications et qui assurent la sécurité technique et cryptographique des fonctions qu'ils assument;
g) prendre des mesures contre la contrefaçon des certificats et, dans les cas où le prestataire de service de certification génère des données afférentes à la création de signature, garantir la confidentialité au cours du processus de génération de ces données;
h) 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;
i) enregistrer toutes les informations pertinentes concernant un certificat qualifié pendant le délai utile, en particulier, pour pouvoir fournir une preuve de la certification en justice. Ces enregistrements peuvent être effectués par des moyens électroniques;
j) ne pas stocker ni copier les données afférentes à la création de signature de la personne à laquelle le prestataire de service de certification a fourni des services de gestion de clés;
k) avant d'établir une relation contractuelle avec une personne demandant un certificat à l'appui de sa signature électronique, informer cette personne par un moyen de communication durable des modalités et 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, qui peut être transmise par voie électronique, doit être faite par écrit 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 prévalent du certificat;
l) 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'information puisse être contrôlée quant à son authenticité,
   - les certificats ne soient disponibles au public pour des recherches que 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 a 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.

Divulgation

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.

Paragraphes 4 et 5 – 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.

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 à l'intention du public un certificat présenté comme agréé ou qui garantit au public un tel certificat soit responsable du préjudice causé à toute entité ou personne physique ou morale qui se fie raisonnablement à ce certificat pour ce qui est de:

a) l'exactitude de toutes informations contenues dans le certificat qualifié à la date où il a été délivré;

b) l'assurance que, au moment de la délivrance du certificat, le signataire identifié dans le certificat qualifié détenait les données afférentes à la création de signature correspondant aux données afférentes à la vérification de signature fournies ou identifiées dans le certificat;

c) l'assurance que les données afférentes à la création de signature et celles afférentes à la vérification de signature puissent être utilisées de façon complémentaire, dans le cas où le prestataire de service de certification génère ces deux types de données,

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

2. Les États membres veillent au moins à ce qu'un prestataire de service de certification qui a délivré à l'intention du public un certificat présenté comme agréé soit responsable du préjudice causé à une entité ou personne physique ou morale qui se prévaut raisonnablement du certificat, pour avoir omis de faire 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 qualifié, les limites fixées à son utilisation, à condition que ces limites soient discernables par des tiers. Le prestataire de service de certification ne doit pas être tenu responsable du préjudice résultant de l'usage abusif d'un certificat qualifié qui dépasse les limites fixées à son utilisation.

4. Les États membres veillent à ce qu'un prestataire de service de certification puisse indiquer, dans un certificat qualifié, la valeur limite des transactions pour lesquelles le certificat peut être utilisé, à condition que cette limite soit discernable par des tiers.

5. Les dispositions des paragraphes 1 à 4 s'appliquent sans préjudice de la directive 93/13/CEE du Conseil du 5 avril 1993 concernant les clauses abusives dans les contrats conclus avec les consommateurs.

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 fausse ou falsifiée d'un titulaire, si, s'agissant de la signature numérique fausse 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 fausse ou falsifiée d'un titulaire, si, s'agissant de la signature numérique fausse 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 11. Foi accordée aux signatures électroniques

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

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

a) nature de l'opération sous-jacente que la signature électronique est censée étayer;

b) adoption ou non par la partie se fiant à la signature électronique de mesures appropriées pour en déterminer la fiabilité;

c) adoption ou non par la partie se fiant à la signature électronique de mesures visant à vérifier que celle-ci était étayée par un certificat;

d) fait que la partie se fiant à la signature savait ou aurait dû savoir que le dispositif de signature électronique avait été compromis ou annulé;

e) toute convention ou toute pratique existant entre la partie se fiant à la signature et le titulaire ou tout usage commercial pouvant s'appliquer;

f) tout autre facteur pertinent.

Article 12. Foi accordée aux certificats

1. Une personne n'est pas fondée à se fier aux informations contenues dans un certificat dans la mesure où il n'est pas raisonnable de le faire.

2. Pour déterminer s'il n'est pas raisonnable de se fier aux informations contenues dans le certificat [Pour déterminer s'il était raisonnable qu'une personne se soit fiée aux informations contenues dans le certificat], il est tenu compte, s'il y a lieu, des facteurs suivants:

a) toutes restrictions dont le certificat peut faire l'objet:

b) 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 ou de suspensions de certificats, le cas échéant;

c) toute convention ou toute pratique existant ou ayant existé au moment pertinent entre la partie se fiant au certificat et le prestataire de services de certification ou le titulaire ou tout usage commercial pouvant s'appliquer;

d) tout autre facteur pertinent.

Variante A

3. S'il n'est pas raisonnable de se fier à la signature électronique au vu des circonstances compte tenu des facteurs énoncés au paragraphe 1, une partie se fiant au certificat assume le risque que la signature ne soit pas une signature valable.

Variante B

3. S'il n'est pas raisonnable de se fier à la signature au vu des circonstances compte tenu des facteurs énoncés au paragraphe 1, une partie se fiant au certificat ne peut se retourner contre le détenteur du dispositif de signature ou le prestataire de services de certification.

Références aux documents de la CNUDCI

A/CN.9/465, par. 109 à 122 (projets d'articles 10 et 11);
A/CN.9/WG.IV/WP.82, par. 56 à 58 (projets d'articles 10 et 11);
A/CN.9/457, par. 99 à 107;
A/CN.9/WG.IV/WP.80, par. 20 et 21.

Remarques

61. Les projets d'articles 11 et 12, qui traitent respectivement du caractère raisonnable de la foi accordée aux signatures électroniques et aux certificats, ont fait l'objet de légères modifications de forme compte tenu des délibérations du Groupe de travail à sa trente-cinquième session. Selon l'avis qui avait prévalu au sein du Groupe de travail à la trente-quatrième session, les Règles uniformes devraient contenir des dispositions relatives aux obligations de la partie qui entend se fier à un certificat, mais des doutes ont été émis à la trente-cinquième session quant à l'utilité de la notion de confiance, se rapportant à la fois au message et à la signature et qui pourrait soulever des difficultés au regard du droit des obligations et de la répartition nécessaire des risques (voir A/CN.9/465, par. 111). Le Groupe de travail souhaitera peut-être déterminer, à titre de principe général, si les Règles uniformes devraient imposer expressément des obligations aux parties se fiant aux signatures. Si l'on estime que les articles 11 et 12 énoncent de telles obligations, il pourrait être nécessaire d'examiner de façon plus approfondie les conséquences de l'inexécution de ces obligations. Si l'on estime, par contre, que les articles 11 et 12 établissent uniquement un "code de conduite", sans traiter les conséquences de la non-application dudit code (voir A/CN.9/465, par. 113), il serait peut-être plus approprié d'inclure un tel texte dans un document explicatif tel qu'un guide pour l'incorporation des Règles uniformes.

62. Les variantes A et B, qui sont toutes deux fondées sur le principe que les Règles uniformes devraient traiter les conséquences juridiques pouvant découler du non-exercice, par une partie se fiant à la signature, de la diligence voulue pour évaluer la fiabilité d'une signature électronique (que celle-ci soit ou non étayée par un certificat), visent à tenir compte des deux propositions formulées à cet égard à la trente-cinquième session du Groupe de travail (voir A/CN.9/465, par. 117).

63. Le Groupe de travail souhaitera peut-être examiner plus avant la relation entre les projets d'articles 11 et 12, d'une part, et le projet d'article 6, d'autre part.

Référence 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 13. Reconnaissance des certificats et signatures électroniques étrangers

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

2. Les certificats émis par un prestataire de services de certification sont reconnus comme équivalant juridiquement aux certificats émis par les prestataires de services de certification soumis à ... *[la loi de l'État*

adoptant] si les pratiques des prestataires de services de certification étrangers offrent un niveau de fiabilité au moins équivalant à celui qui est requis des prestataires de services de certification 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 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 ces 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. Pour déterminer l'équivalence, il est tenu compte, s'il y a lieu, [des facteurs énoncés au paragraphe 2 de l'article 10] [des facteurs 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].

5. Nonobstant les paragraphes 2 et 3, les parties à des transactions commerciales et autres peuvent spécifier qu'il est nécessaire de recourir à un prestataire de services de certification, une catégorie de prestataires de services de certification ou une catégorie de certificats particuliers pour les messages ou signatures qui leur sont soumis.

6. Lorsque, nonobstant les paragraphes 2 et 3, les parties conviennent, s'agissant de leurs relations, d'utiliser certains types de signatures électroniques et de certificats, [cette convention est jugée suffisante aux fins de la reconnaissance internationale]. [Pour déterminer si, ou dans quelle mesure, une signature électronique ou un certificat produit légalement ses effets, il est tenu compte de toute convention entre les parties à la transaction dans laquelle cette signature ou ce certificat est utilisé.]

Références aux documents de la CNUDCI

A/CN.9/465, par. 21 à 35;
A/CN.9/WG.IV/WP.82, par. 69 à 71;
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 I); et
A/CN.9/WG.IV/WP.71, par.73 à 75;

Remarques

64. Le principe de non-discrimination énoncé au paragraphe 1 a bénéficié d'un appui général à la trente-cinquième session du Groupe de travail, mais on s'est demandé s'il était approprié de faire référence au pays d'origine. Selon un avis, cette référence rendait la disposition sur la non-discrimination trop étroite et laissait la porte ouverte à des discriminations fondées sur un certain nombre d'autres motifs, ce qui n'était pas souhaitable. Selon une autre opinion, il pourrait en fait y avoir des cas où le pays d'origine de la signature ou du certificat était essentiel pour la question de la reconnaissance. Toutefois, aucun appui n'a été exprimé en faveur d'une proposition tendant à remplacer le libellé actuel, selon lequel "il n'est pas tenu compte" du pays d'origine, par un libellé selon lequel la détermination de l'effet juridique d'une signature électronique ne devrait pas être basée "uniquement" sur le pays d'origine (voir A/CN.9/465, par. 23 et 24). Le Groupe de travail voudra peut-être déterminer, à titre de principe général, si un énoncé précis incorporant le principe de non-discrimination devrait être inclus au projet d'article 13 ou si ce principe devrait être exprimé de manière plus générale dans un préambule ou dans un guide pour l'incorporation des Règles uniformes.

65. Les membres du Groupe de travail se sont largement accordés, à la précédente session, sur les paragraphes 2, 3, 4 et 5, qui énoncent une règle appropriée sur la reconnaissance des certificats et signatures étrangers (ibid., par. 34). S'agissant des facteurs énumérés au paragraphe 4, un renvoi au projet d'article 10 pourrait être suffisant si l'on retient les mêmes facteurs pour déterminer la fiabilité des systèmes utilisés par les prestataires nationaux de services de certification. Le paragraphe 5 reflète un avis généralement exprimé dans le Groupe de travail, selon lequel les parties à des transactions commerciales et autres devraient avoir le droit de choisir le prestataire de services de certification, la catégorie de prestataires de services de certification ou la catégorie de certificats qu'ils souhaitent utiliser pour les messages ou les signatures qu'ils reçoivent. La référence aux parties à des transactions commerciales et autres vise à englober les organismes publics agissant en leur qualité d'entité commerciale.

66. Le libellé du paragraphe 6 vise à traduire la décision prise par le Groupe de travail à sa trente-cinquième session selon laquelle le projet d'article 13 devrait prévoir que la reconnaissance des conventions entre les parties intéressées concernant l'utilisation de certains types de signatures électroniques ou de certificats est un motif suffisant pour la reconnaissance nationale (entre ces parties) de telles signatures ou certificats convenus (A/CN.9/465, par. 34).

67. Le Groupe de travail pourrait souhaiter déterminer, à titre de principe général, si le projet d'article 13 devrait porter à la fois sur les certificats et sur les signatures.

Références à des lois nationales et à d'autres textes

Directive de la Communauté européenne

Article 7 Aspects internationaux

1. Les États membres veillent à ce que les certificats délivrés à titre de certificats agréés à l'intention du public par un prestataire de service de certification établi dans un pays tiers soient reconnus équivalents, sur le plan juridique, aux certificats délivrés par un prestataire de service de certification établi dans la Communauté:

a) si le prestataire de service de certification remplit les conditions visées dans la présente directive et a été accrédité dans le cadre d'un régime volontaire d'accréditation établi dans un État membre; 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 en application d'un accord bilatéral ou multilatéral entre la Communauté et des pays tiers ou des organisations internationales.

2. Afin de faciliter les services de certification internationaux avec des pays tiers et la reconnaissance juridique des signatures électroniques avancées émanant de pays tiers, la Commission fait, le cas échéant, des propositions visant à la mise en œuvre effective de normes et d'accords internationaux applicables aux services de certification. En particulier et si besoin est, elle soumet des propositions au Conseil concernant des mandats appropriés 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].

Annexe I. PROJET DE RÈGLES UNIFORMES SUR LES SIGNATURES ÉLECTRONIQUES

(Récapitulatif des projets d'articles 1 à 13, tels qu'examinés dans la deuxième partie de la présente note)

Article premier. Champ d'application

Les présentes Règles s'appliquent lorsque des signatures électroniques sont utilisées dans le contexte* d'activités commerciales**. Elles ne se substituent à aucune règle de droit visant à protéger les consommateurs.

* La Commission propose le texte suivant aux États qui souhaiteraient étendre l'applicabilité des présentes Règles:

"Les présentes Règles s'appliquent lorsque des signatures électroniques sont utilisées, sauf dans les situations suivantes: [...]."

** Le terme "commercial" 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.

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 audit 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].”

Article 3. [Neutralité technique] [Égalité de traitement des signatures]

Aucune des dispositions des présentes Règles n’est appliquée de manière à exclure, restreindre ou priver d’effet juridique toute méthode [de signature électronique] [satisfaisant aux exigences mentionnées au paragraphe 1 de l’article 6 des présentes Règles] [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] [ou satisfaisant autrement aux exigences de la loi applicable].

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.

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.

Article 5. [Dérogation conventionnelle] [Autonomie des parties] [Liberté contractuelle]

Il est possible de déroger aux présentes Règles ou [de les modifier] [d’en modifier l’effet] par convention, à moins que lesdites Règles ou la loi de l’État adoptant en disposent autrement.

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

1. 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 méthode] [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.

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

Variante A

3. [Une méthode] [Une signature électronique] est présumée fiable en ce qu’elle satisfait à l’exigence indiquée au paragraphe 1 lorsqu’elle garantit:

a) que les données utilisées pour la création d’une signature électronique sont particulières au détenteur du dispositif de [création de] signature dans le contexte dans lequel elles sont utilisées;

b) que le détenteur du dispositif de [création de] signature [a] [a eu au moment pertinent] seul le contrôle de ce dispositif;

c) que la signature électronique est liée [aux informations] [au message de données ou à la partie de ce message] [auxquelles] [auquel] elle se rapporte [d'une manière qui garantit l'intégrité de ces informations];

d) que le détenteur du dispositif de [création de] signature est objectivement identifié dans le contexte [dans lequel le dispositif est utilisé] [du message de données].

Variante B

3. En l'absence de preuve du contraire, il est présumé que l'utilisation d'une signature électronique prouve:

a) la conformité de la signature électronique à la norme de fiabilité énoncée au paragraphe 1;

b) l'identité du signataire présumé; et

c) l'approbation par le signataire présumé des informations auxquelles se rapporte la signature électronique.

4. La présomption établie au paragraphe 3 s'applique uniquement si:

a) la personne qui entend se fier à la signature électronique avise le signataire présumé qu'il se fie à cette signature [en tant qu'équivalent de la signature manuscrite du signataire présumé] [comme preuve des éléments énumérés au paragraphe 3)]; et

b) le signataire présumé n'avise pas promptement la personne qui adresse une notification en vertu de l'alinéa a) des raisons pour lesquelles il ne faut pas se fier à la signature électronique [comme équivalent de sa signature manuscrite] [comme preuve des éléments énumérés au paragraphe 3].

Variante C

3. En l'absence de preuve du contraire, il est résumé que l'utilisation d'une signature électronique prouve:

a) la conformité de la signature électronique à la norme de fiabilité énoncée au paragraphe 1;

b) l'identité du signataire présumé; et

c) l'approbation par le signataire présumé des informations auxquelles se rapporte la signature électronique.

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

[Article 7. Présomption d'original

1. Un message de données est présumé être sous sa forme originale lorsqu'il est fait usage, pour ce message de données, [d'une méthode] [d'une signature électronique] [dans le contexte de l'article 6] qui:

a) 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; et

b) lorsqu'il est exigé qu'une information soit présentée, cette information peut être montrée à la personne à laquelle elle doit être présentée;

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

Article 8. Satisfaction des exigences des articles 6 et 7

Variante A

1. *[L'Organe ou l'autorité indiqué par l'État adoptant comme compétent en la matière]* peut déterminer quelles méthodes satisfont aux exigences des articles 6 et 7.

2. Toute détermination en vertu du paragraphe 1 est conforme aux normes internationales reconnues.

Variante B

1. Il peut être déterminé qu'une ou plusieurs méthodes de signature électronique satisfont aux exigences des articles 6 et 7.

2. Toute détermination en vertu du paragraphe 1 est conforme aux normes internationales reconnues.

Article 9. Responsabilités du détenteur du dispositif de signature

1. Chaque détenteur d'un dispositif de signature:

a) Prend des dispositions raisonnables pour éviter toute utilisation non autorisée de son dispositif de signature;

b) Avise les personnes voulues sans retard excessif si:

i) il sait que le dispositif de signature a été compromis; ou si

ii) au vu des circonstances connues de lui, il y a un risque important que le dispositif de signature ait été compromis;

c) [Lorsqu'un certificat est utilisé pour étayer le dispositif de signature,] [Lorsque le dispositif de signature implique l'utilisation d'un certificat,] prend des dispositions raisonnables pour veiller à ce que toutes les déclarations faites par lui qui concernent le [cycle de vie du] certificat ou qui doivent figurer dans le certificat soient exactes et complètes.

2. Le détenteur d'un dispositif de signature est responsable de la non-satisfaction des exigences énoncées au paragraphe 1.

Article 10. Responsabilités d'un prestataire de services de certification

1. Un prestataire de services de certification:

a) agit conformément aux déclarations qu'il fait concernant ses pratiques;

b) fait preuve de la diligence voulue afin de veiller à ce que toutes les déclarations faites par lui qui concernent le cycle de vie du certificat ou qui figurent dans le certificat soient exactes et complètes;

c) fournit des moyens raisonnablement accessibles qui permettent à une partie se fiant au certificat de s'assurer:

i) de l'identité du prestataire de services de certification;

ii) du fait que la personne qui est identifiée dans le certificat détient au moment pertinent le dispositif de signature indiqué dans le certificat;

iii) de la méthode employée pour identifier le détenteur du dispositif de signature;

iv) de toute restriction quant aux fins ou à la valeur pour lesquelles la signature peut être utilisée; et

v) du fait que le dispositif de signature est valable et n'a pas été compromis;

d) Fournit un moyen permettant au détenteur du dispositif de signature d'avertir qu'un dispositif de signature a été compromis et assure un service prompt d'annulation;

e) Utilise des systèmes, des procédures et des ressources humaines fiables pour la prestation de ses services.

2. Pour déterminer si, et dans quelle mesure, tous systèmes, procédures et ressources humaines sont fiables aux fins de l'alinéa e) du paragraphe 1, il est tenu compte des facteurs 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 du prestataire de services 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 du prestataire de services de certification et la loi de l'État adoptant.

3. Un certificat énonce les éléments suivants:

a) l'identité du prestataire de services de certification;

b) le fait que la personne qui est identifiée dans le certificat détient, au moment pertinent, le dispositif de signature indiqué dans le certificat;

c) le fait que le dispositif de signature était valide à la date ou avant la date à laquelle le certificat a été émis;

d) toute restriction quant aux fins ou à la valeur pour lesquelles le certificat peut être utilisé; et

e) toute restriction quant à la portée ou à l'étendue de la responsabilité que le certificateur accepte envers toute personne.

Variante X

4. Un prestataire de services de certification est responsable de la non-satisfaction des exigences énoncées au paragraphe 1.

5. La responsabilité du prestataire de services de certification 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] [exigences] énoncé[e]s au paragraphe 1.

Variante Y

4. Un prestataire de services de certification est responsable de la non-satisfaction des exigences énoncées au paragraphe 1.

5. Pour l'évaluation du préjudice, il est tenu compte des facteurs suivants:

a) coût de l'obtention du certificat;

b) nature de l'information certifiée;

c) existence et portée de toute restriction quant à l'objet pour lequel le certificat peut être utilisé;

d) existence de toute déclaration limitant la portée ou l'étendue de la responsabilité du prestataire de services de certification; et

e) toute faute concurrente de la partie se fiant au certificat.

Variante Z

4. Si le préjudice a été causé parce que le certificat était incorrect ou défectueux, un prestataire de services de certification est tenu responsable du préjudice subi:

a) soit par une partie qui a passé un contrat avec le prestataire de services de certification pour la délivrance d'un certificat; ou

b) soit par une personne qui se fie raisonnablement à un certificat émis par le prestataire de services de certification.

5. Un prestataire de services de certification 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 pertinente; ou

b) s'il prouve qu'il [n'a pas été négligeant] [a pris toutes les mesures raisonnables pour prévenir le préjudice].

Article 11. Foi accordée aux signatures électroniques

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

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

a) nature de l'opération sous-jacente que la signature électronique est censée étayer;

b) adoption ou non par la partie se fiant à la signature électronique de mesures appropriées pour en déterminer la fiabilité;

c) adoption ou non par la partie se fiant à la signature électronique de mesures visant à vérifier que celle-ci était étayée par un certificat;

d) fait que la partie se fiant à la signature savait ou aurait dû savoir que le dispositif de signature électronique avait été compromis ou annulé;

e) toute convention ou toute pratique existant entre la partie se fiant à la signature et le titulaire ou tout usage commercial pouvant s'appliquer;

f) tout autre facteur pertinent.

Article 12. Foi accordée aux certificats

1. Une personne n'est pas fondée à se fier aux informations contenues dans un certificat dans la mesure où il n'est pas raisonnable de le faire.

2. Pour déterminer s'il n'est pas raisonnable de se fier aux informations contenues dans le certificat [Pour déterminer s'il était raisonnable qu'une personne se soit fiée aux informations contenues dans le certificat], il est tenu compte, s'il y a lieu, des facteurs suivants:

a) toutes restrictions dont le certificat peut faire l'objet:

b) 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 ou de suspensions de certificats, le cas échéant;

c) toute convention ou toute pratique existant ou ayant existé au moment pertinent entre la partie se fiant au certificat et le prestataire de services de certification ou le titulaire ou tout usage commercial pouvant s'appliquer;

d) tout autre facteur pertinent.

Variante A

3. S'il n'est pas raisonnable de se fier à la signature électronique au vu des circonstances compte tenu des facteurs énoncés au paragraphe 1, une partie se fiant au certificat assume le risque que la signature ne soit pas une signature valable.

Variante B

3. S'il n'est pas raisonnable de se fier à la signature au vu des circonstances compte tenu des facteurs énoncés au paragraphe 1, une partie se fiant au certificat ne peut se retourner contre le détenteur du dispositif de signature ou le prestataire de services de certification.

Article 13. Reconnaissance des certificats et signatures électroniques étrangers

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

2. Les certificats émis par un prestataire de services de certification sont reconnus comme équivalant juridiquement aux certificats émis par les prestataires de services de certification soumis à ... *[la loi de l'État adoptant]* si les pratiques des prestataires de services de certification étrangers offrent un niveau de fiabilité au moins équivalant à celui qui est requis des prestataires de services de certification 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 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 ces 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. Pour déterminer l'équivalence, il est tenu compte, s'il y a lieu, [des facteurs énoncés au paragraphe 2 de l'article 10] [des facteurs 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].

5. Nonobstant les paragraphes 2 et 3, les parties à des transactions commerciales et autres peuvent spécifier qu'il est nécessaire de recourir à un prestataire de services de certification, une catégorie de prestataires de services de certification ou une catégorie de certificats particuliers pour les messages ou signatures qui leur sont soumis.

6. Lorsque, nonobstant les paragraphes 2 et 3, les parties conviennent, s'agissant de leurs relations, d'utiliser certains types de signatures électroniques et de certificats, [cette convention est jugée suffisante aux fins de la reconnaissance internationale]. [Pour déterminer si, ou dans quelle mesure, une signature électronique ou un certificat produit légalement ses effets, il est tenu compte de toute convention entre les parties à la transaction dans laquelle cette signature ou ce certificat est utilisé.]

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.

[4]Ibid., cinquante-quatrième session, Supplément N° 17 (A/54/17), par. 308 à 314.