Nations Unies A/CN.9/WG.IV/WP.86

Assemblée générale

Distr.: Limitée
18 août 2000

Français
Original: Anglais

**Commission des Nations Unies
pour le droit commercial international
Groupe de travail sur le commerce électronique**
Trente-septième session
Vienne, 18-29 septembre 2000

Signatures électroniques

Projet de Guide pour l'incorporation dans le droit interne des Règles uniformes de la CNUDCI sur les signatures électroniques

Note du Secrétariat

1. Conformément aux décisions prises par la Commission à ses vingt-neuvième (1996)[1] et trentième (1997)[2] sessions, le Groupe de travail sur le commerce électronique a consacré ses trente et unième à trente-sixième sessions à l'élaboration du projet de Règles uniformes de la CNUDCI sur les signatures électroniques (dénommé ci-après "les Règles uniformes"). Les rapports de ces sessions sont publiés sous la cote A/CN.9/437, 446, 454, 457, 465 et 467 respectivement. Lors de l'élaboration des Règles uniformes, le Groupe de travail a noté qu'il serait utile de fournir, dans un commentaire, des informations complémentaires concernant lesdites Règles. S'inspirant de la démarche adoptée pour la préparation de la Loi type de la CNUDCI sur le commerce électronique, une proposition tendant à assortir les Règles uniformes d'un guide afin d'aider les États à incorporer ces dernières dans leur droit interne et à les appliquer a été généralement bien accueillie. Le guide, qui pourrait être établi en grande partie à partir des *travaux préparatoires* des Règles uniformes, constituerait également un outil précieux pour d'autres utilisateurs des Règles.

2. À sa trente-sixième session, le Groupe de travail a examiné la question des signatures électroniques en se fondant sur la note établie par le secrétariat (A/CN.9/WG.IV/WP.84). À l'issue des débats, il a adopté les projets d'articles 1 et 3 à 11 quant au fond et les a renvoyés à un groupe de rédaction chargé d'assurer la cohérence entre les dispositions des Règles uniformes. Le secrétariat a été prié d'établir un projet de guide pour l'incorporation des dispositions adoptées. Sous réserve de l'approbation de la Commission, le Groupe de travail a recommandé que les projets d'articles 2 et 13 des Règles uniformes, ainsi que le guide pour leur incorporation, soient revus par lui à une session ultérieure.[3]

3. À sa trente-troisième session (juin-juillet 2000), la Commission a noté que le Groupe de travail avait, à sa trente-sixième session, adopté le texte des projets d'articles 1 et 3 à 11 des Règles uniformes. Il restait, a-t-on dit, à clarifier certains points suite à la décision du Groupe de travail de supprimer dans le projet de Règles uniformes la notion de "signature électronique renforcée". On a exprimé la crainte qu'il soit nécessaire, en fonction des décisions que prendrait le Groupe de travail concernant les projets d'articles 2 et 13, de réexaminer les autres projets de dispositions pour éviter que la norme établie dans les règles uniformes ne s'applique de la même façon aux signatures électroniques garantissant un niveau de sécurité élevé et aux certificats de moindre valeur susceptibles d'être utilisés dans les communications électroniques n'étant pas destinées à produire d'effet juridique important.

4. À l'issue des débats, la Commission a félicité le Groupe de travail pour les efforts qu'il avait fournis et les progrès qu'il avait accomplis dans l'élaboration des Règles uniformes. Elle l'a instamment prié de terminer ses travaux sur ce texte à sa trente-septième session et d'examiner le projet de guide que devait établir le secrétariat.[4]

5. L'annexe de la présente note renferme la première partie et le chapitre premier de la deuxième partie du projet de Guide établi par le secrétariat. Le chapitre II de la deuxième partie est publié sous la cote A/CN.9/WG.IV/WP.86/Add.1.

Annexe

CNUDCI
RÈGLES UNIFORMES SUR LES SIGNATURES ÉLECTRONIQUES

ET

GUIDE POUR LEUR INCORPORATION

2001

TABLE DES MATIÈRES

Première partie

RÈGLES UNIFORMES DE LA CNUDCI SUR LES SIGNATURES ÉLECTRONIQUES (2001)

Projets d'articles 1 et 3 à 11 des Règles uniformes de la CNUDCI sur les signatures électroniques (2001)

(Texte adopté par le Groupe de travail de la CNUDCI sur le commerce électronique à sa trente-sixième session, tenue à New York du 14 au 25 février 2000)

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 le consommateur.

*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 suivante: [...]."

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

Article 3. Égalité de traitement des techniques de signature

Aucune disposition des présentes Règles, à l'exception de l'article 5, n'est appliquée de manière à exclure, restreindre ou priver d'effets juridiques une quelconque méthode de création de signatures électroniques satisfaisant aux exigences mentionnées au paragraphe 1 de l'article 6 des présentes Règles ou autrement satisfaisant aux exigences de la loi applicable.

Article 4. Interprétation

1. Pour l'interprétation des présentes Règles, 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 qui ne sont pas expressément réglées par elles sont tranchées selon les principes généraux dont elles s'inspirent.

Article 5. Dérogation conventionnelle

Il est possible de déroger aux présentes Règles ou d'en modifier les effets par convention, à moins que cette convention soit invalide ou sans effets juridiques aux termes de la loi de l'État adoptant [ou à moins que lesdites Règles n'en disposent autrement].

Article 6. Satisfaction de l'exigence 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 signature électronique dont la fiabilité est suffisante au regard de l'objet pour lequel le message de données a été créé ou communiqué, compte tenu de toutes les circonstances, y compris toute convention en la matière.

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 en l'absence de signature.

3. Une signature électronique est considérée fiable en ce qu'elle satisfait à l'exigence indiquée au paragraphe 1 si:

a) Les moyens utilisés pour la création d'une signature électronique sont, dans le contexte dans lequel ils sont utilisés, liés exclusivement au signataire;

b) Les moyens utilisés pour la création d'une signature électronique sont, au moment de la signature, sous le contrôle exclusif du signataire;

c) Toute modification apportée à la signature électronique après le moment de la signature est décelable; et,

d) Dans le cas où l'exigence légale de signature a pour but de garantir l'intégrité de l'information à laquelle elle se rapporte, toute modification apportée à l'information après le moment de la signature est décelable.

4. Le paragraphe 3 ne restreint pas la possibilité pour toute personne concernée:

a) D'établir de toute autre manière, aux fins de satisfaire l'exigence visée au paragraphe 1, la fiabilité de la signature électronique; ni

b) D'apporter des preuves de la non-fiabilité de la signature électronique.

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

Article 7. Satisfaction des dispositions de l'article 6

1. [Toute personne, tout organe ou autorité, de droit public ou privé, indiqué par l'État adoptant comme compétent en la matière] peut déterminer quelles signatures électroniques satisfont aux exigences de l'article 6.

2. Toute détermination arrêtée en vertu du paragraphe 1 doit être conforme aux normes internationales reconnues.

3. Aucune disposition du présent article n'affecte le fonctionnement des règles du droit international privé.

Article 8. Normes de conduite du signataire

1. Chaque signataire:

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

b) Avertit, sans délai, toute personne dont il peut raisonnablement penser qu'elle se fie à la signature électronique ou qu'elle prête des services à l'appui de la signature électronique si:

i) Il sait que le dispositif de signature est compromis; ou

ii) Il estime, au regard de circonstances connues de lui, qu'il y a un risque important que le dispositif de signature ait été compromis;

c) Prend, lorsqu'un certificat est utilisé à l'appui de la signature électronique, des précautions raisonnables pour assurer que tous les renseignements qu'il donne concernant le certificat durant tout son cycle de vie ou devant figurer dans le certificat sont exacts et complets.

2. Le signataire est responsable de tout manquement aux exigences visées au paragraphe 1.

Article 9. Normes de conduite du prestataire de services de certification

1. Le prestataire de services de certification:

a) Agit en conformité de ses déclarations de principe et des renseignements qu'il donne concernant ses pratiques;

b) Prend des précautions raisonnables pour assurer que tous les renseignements qu'il donne concernant le certificat durant tout son cycle de vie ou figurant dans le certificat sont exacts et complets;

c) Fournit à toute partie se fiant au certificat des moyens raisonnablement accessibles lui permettant de s'assurer à partir du certificat:

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

ii) De ce que la personne identifiée dans le certificat avait au moment de la signature le contrôle du dispositif de signature;

iii) De ce que le dispositif de signature était valide à la date ou précédemment à la date à laquelle le certificat a été émis;

d) Fournit à toute partie se fiant au certificat des moyens raisonnablement accessibles lui permettant de s'assurer, s'il y a lieu, à partir du certificat ou de toute autre manière:

i) De la méthode utilisée pour identifier le signataire;

ii) De toute restriction quant aux fins ou à la valeur pour lesquelles la signature ou le certificat peuvent être utilisés;

iii) De ce que le dispositif de signature fonctionne et n'a pas été compromis;

iv) De toute restriction quant à la nature ou à l'étendue de la responsabilité stipulée par le prestataire de services de certification;

v) De l'existence de moyens accessibles au signataire permettant à celui-ci de l'avertir que le dispositif de signature a été compromis;

vi) De la disponibilité d'un service d'annulation en temps utile;

e) Fournit au signataire le moyen de l'avertir que le dispositif de signature a été compromis, et assure en temps utile un service d'annulation;

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

2. Un prestataire de services de certification est responsable pour tout manquement aux exigences visées au paragraphe 1.

[Article 10. Fiabilité

Pour déterminer si et dans quelle mesure tous systèmes, procédures et ressources humaines utilisées par le prestataire de services de certification sont fiables, il est tenu compte des facteurs suivants:

a) Ressources humaines et financières, y compris l'existence d'avoirs;

b) Qualité du matériel et des logiciels;

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

d) Possibilité d'accès à l'information pour les signataires 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; et

g) Tous autres facteurs pertinents.]

Article 11. Normes de conduite de la partie se fiant à la signature ou au certificat

La partie se fiant à la signature ou au certificat assume les conséquences juridiques découlant du fait qu'elle s'est abstenue de:

a) Prendre des mesures raisonnables pour vérifier la fiabilité d'une signature électronique; ou,

b) Si une signature électronique est appuyée par un certificat, de prendre des mesures raisonnables pour:

i) Vérifier que le certificat est valide ou qu'il n'a pas été suspendu ni annulé; et

ii) Tenir compte de toute restriction dont le certificat ferait l'objet.

Deuxième partie

GUIDE POUR L'INCORPORATION DES RÈGLES UNIFORMES DE LA CNUDCI SUR LES SIGNATURES ÉLECTRONIQUES (2001)

Objet du présent Guide

1. Lorsqu'elle a élaboré et adopté les Règles uniformes de la CNUDCI sur les signatures électroniques (également dénommées dans la présente publication "les Règles uniformes"), la Commission des Nations Unies pour le droit commercial international (CNUDCI) était consciente du fait que, pour les États qui modernisent leur législation, ces Règles seraient un outil plus efficace si des informations de base et des explications étaient données aux gouvernements et aux parlements pour les aider à les utiliser. Elle a aussi tenu compte du fait que les Règles uniformes seraient probablement utilisées par des pays peu familiarisés avec le type de techniques de communication qui y sont envisagées. Le présent Guide, qui a été établi en grande partie sur la base des travaux préparatoires, se veut par ailleurs un instrument utile pour d'autres utilisateurs du texte, tels que juges, arbitres, praticiens et universitaires. Ces informations pourraient aussi aider les États à examiner, le cas échéant, les dispositions qu'il conviendrait de modifier pour tenir compte de conditions particulières. Durant l'élaboration des Règles uniformes, il a été présumé que le projet de Règles uniformes serait accompagné d'un tel guide. Il a été décidé, par exemple, de ne pas régler un certain nombre de points dans le texte des Règles uniformes, mais de s'y référer dans le Guide afin d'aider les États Membres à appliquer les Règles uniformes le moment venu. Les informations présentées dans le présent Guide visent à expliquer pourquoi les dispositions des Règles uniformes ont été retenues à titre de caractéristiques minimales essentielles d'une législation destinée à atteindre les objectifs des Règles uniformes.

2. Le présent Guide pour l'incorporation a été élaboré par le secrétariat conformément à la demande faite par la CNUDCI à la clôture de sa trente-quatrième session, en 2001. Il est fondé sur les délibérations et décisions de la Commission à cette session,[8] à laquelle les Règles uniformes ont été adoptées, ainsi que sur les considérations du Groupe de travail sur le commerce électronique, qui a mené les travaux préparatoires.

Chapitre premier. Présentation générale des Règles uniformes

I. OBJECTIFS ET ORIGINE DES RÈGLES UNIFORMES

A. Objectifs

3. Le recours accru à des techniques d'authentification électroniques au lieu de signatures manuscrites et d'autres méthodes traditionnelles d'authentification a conduit à penser qu'il serait utile d'avoir un cadre juridique spécifique afin de réduire l'incertitude quant à l'effet juridique pouvant résulter de l'utilisation de telles techniques modernes (qui peuvent être désignées d'une façon générale par le terme "signatures électroniques"). Le risque que divers pays adoptent des approches législatives divergentes à l'égard des signatures électroniques demande des dispositions législatives uniformes afin d'établir les règles de base de ce qui est intrinsèquement un phénomène international dans lequel l'interopérabilité juridique (ainsi que technique) est essentielle.

4. Se fondant sur les principes fondamentaux sur lesquels repose l'article 7 de la Loi type de la CNUDCI sur le commerce électronique (également dénommée ci-après "la Loi type") pour ce qui est de la réalisation de la fonction de signature dans un environnement

électronique, les Règles uniformes visent à aider les États à mettre en place un cadre législatif moderne, harmonisé et équitable permettant d'aborder de façon plus efficace les questions des signatures électroniques. Supplément modeste mais important de la Loi type, les Règles uniformes proposent des normes concrètes par rapport auxquelles la fiabilité technique des signatures électroniques peut être mesurée. Elles établissent en outre un lien entre cette fiabilité technique et l'efficacité juridique que l'on peut attendre d'une signature électronique particulière. Elles ajoutent un élément important à la Loi type en adoptant une approche qui permet de déterminer à l'avance (ou d'évaluer avant utilisation effective) l'efficacité juridique d'une technique de signature électronique particulière. Elles visent donc à faire mieux comprendre les signatures électroniques et à donner confiance dans l'utilisation de certaines techniques de signatures électroniques dans des opérations ayant une valeur juridique. En outre, en définissant avec la souplesse requise un ensemble de normes de conduite pour les diverses parties pouvant être amenées à utiliser des signatures électroniques (à savoir signataires, parties se fiant à la signature et tiers prestataires de services), les Règles uniformes peuvent aider à la mise en place de pratiques commerciales plus harmonieuses dans le cyberespace.

5. Les objectifs des Règles uniformes, qui consistent notamment à permettre ou à faciliter le recours aux signatures électroniques et à accorder le même traitement aux utilisateurs de la documentation sur papier et aux utilisateurs d'informations informatisées, contribuent de manière décisive à favoriser l'économie et l'efficacité du commerce international. En incorporant dans sa législation nationale les procédures prescrites dans les Règles uniformes (et la Loi type) pour les cas où les parties décident d'utiliser des moyens de communication électroniques, un État adopterait une approche neutre quant à la technique d'information.

B. Origine

6. Les Règles uniformes constituent une nouvelle étape dans une série d'instruments internationaux adoptés par la CNUDCI, qui ou bien portent spécifiquement sur les besoins du commerce électronique ou bien ont été élaborés compte tenu des besoins des moyens modernes de communication. Dans la première catégorie figurent le Guide juridique de la CNUDCI sur les transferts électroniques de fonds (1987), la Loi type de la CNUDCI sur les virements internationaux (1992) et la Loi type de la CNUDCI sur le commerce électronique (1996 et 1998). La deuxième catégorie comprend toutes les conventions internationales et autres instruments législatifs adoptés par la CNUDCI depuis 1978, qui promeuvent tous un formalisme réduit et contiennent des définitions de "l'écrit" destinés à englober les communications dématérialisées.

7. L'instrument le plus spécifique (et peut-être le mieux connu) de la CNUDCI dans le domaine du commerce électronique est la Loi type de la CNUDCI sur le commerce électronique. Son élaboration, au début des années 90 a pour origine le recours accru à des moyens modernes de communication tels que le courrier électronique et l'échange de données informatisées (EDI) pour la conduite des opérations commerciales internationales. On s'est rendu compte que de nouvelles techniques s'étaient répandues rapidement et continueraient de se développer à mesure que des supports techniques tels que les autoroutes de l'information et l'Internet devenaient plus largement accessibles. Toutefois, la communication d'informations ayant une valeur juridique sous forme de messages sans support papier était entravée par des obstacles juridiques à l'utilisation de tels messages ou par l'incertitude quant à leur effet ou leur validité juridiques. Afin de faciliter le recours accru aux moyens modernes de communication, la CNUDCI a élaboré la Loi type, dont l'objectif est d'offrir aux législateurs nationaux un ensemble de règles internationalement acceptables sur la manière de surmonter un certain nombre de ces obstacles et de créer un

environnement juridique plus sûr pour ce que l'on appelle aujourd'hui le "commerce électronique".

8. La décision prise par la CNUDCI d'élaborer une législation type sur le commerce électronique a tenu au fait que, dans un certain nombre de pays, la législation régissant les communications et l'archivage de l'information était inadaptée ou dépassée car elle n'envisageait pas le recours au commerce électronique. Dans certains cas, la législation impose encore directement ou indirectement des restrictions à l'utilisation des moyens modernes de communication, par exemple en prescrivant l'emploi de documents "écrits", "signés" ou "originaux". Pour les notions de documents "écrits", "signés" et "originaux", la Loi type a adopté des approches fondées sur l'équivalent multifonctionnel.

9. Lorsque la Loi type était en cours d'élaboration, quelques pays avaient adopté des dispositions particulières pour traiter de certains aspects du commerce électronique, mais il n'y avait pas de législation traitant de ce commerce dans son ensemble. Cela pouvait être source d'incertitudes quant à la nature juridique et à la validité d'informations présentées sous une forme autre que celle de documents traditionnels sur papier. En outre, des lois et des pratiques saines étaient nécessaires dans tous les pays où l'utilisation de l'EDI et de la messagerie électronique se généralisait, mais ce besoin se faisait aussi sentir dans de nombreux pays pour des techniques de communication telles que la télécopie et le télex.

10. La Loi type aidait aussi à pallier les désavantages tenant au fait qu'une législation nationale inappropriée entravait le commerce international, dont une proportion importante est liée à l'utilisation des techniques modernes de communication. Les disparités entre les régimes juridiques nationaux régissant l'utilisation de ces techniques de communication et les incertitudes qu'elles entraînent peuvent encore contribuer dans une large mesure à limiter les possibilités qu'ont les entreprises d'accéder aux marchés internationaux.

11. En outre, au niveau international, la Loi type peut servir, dans certains cas, d'outil pour interpréter les conventions internationales et autres instruments internationaux existants qui créent des obstacles juridiques au recours au commerce électronique, par exemple en prescrivant la forme écrite pour certains documents ou certaines clauses contractuelles. Entre les États Parties à de tels instruments internationaux, l'adoption de la Loi type comme règle d'interprétation pourrait être le moyen de reconnaître le commerce électronique et d'éviter de devoir négocier un protocole à l'instrument international concerné.

C. Historique

12. Après avoir adopté la Loi type de la CNUDCI sur le commerce électronique, la Commission a, à sa vingt-neuvième session (1996), décidé d'inscrire à son ordre du jour la question des signatures numériques et des autorités de certification. Le Groupe de travail sur le commerce électronique a été prié d'examiner l'opportunité et la faisabilité de l'élaboration de règles uniformes sur ces sujets. Il a été convenu que les règles uniformes à élaborer devraient être consacrées notamment aux questions telles que le fondement juridique des opérations de certification, y compris les nouvelles techniques d'authentification et de certification numériques; l'applicabilité de la certification; la répartition des risques et des responsabilités entre utilisateurs, 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 l'incorporation par référence.[5]

13. 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. Il 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). 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.

14. S'agissant du champ d'application et de la forme exacts des Règles uniformes, la Commission a généralement convenu qu'aucune décision ne pouvait être prise à un stade aussi précoce. Elle a estimé qu'il était justifié que le Groupe de travail axe son attention sur les questions relatives aux signatures numériques, étant donné le rôle apparemment prédominant joué par la cryptographie à clef publique dans la nouvelle pratique du commerce électronique, mais les Règles uniformes à élaborer devraient être compatibles avec l'approche techniquement neutre adoptée dans la Loi type. Ainsi, les Règles uniformes ne devraient pas décourager l'utilisation d'autres techniques d'authentification. En outre, lorsqu'il s'agirait de la cryptographie à clef publique, il pourrait être nécessaire de prendre en considération, dans ces Règles uniformes, divers niveaux de sécurité et de reconnaître les divers effets juridiques et niveaux de responsabilité correspondant aux différents types de services fournis dans le contexte des signatures numériques. S'agissant des autorités de certification, la Commission a certes reconnu la valeur des normes issues du marché, mais il a été largement considéré que le Groupe de travail pourrait utilement envisager l'établissement d'un ensemble minimum de normes que les autorités de certification devraient strictement respecter, en particulier dans les cas de certification internationale.[6]

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

16. À sa trente et unième session (1998), la Commission était saisie du rapport du Groupe de travail sur les travaux de sa trente-deuxième session (A/CN.9/446). Il a été noté que le Groupe de travail avait eu des difficultés manifestes, à ses trente et unième et trente-deuxième sessions, 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 été également 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.

17. 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 progresserait 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 considéré comme un forum international particulièrement important pour les échanges de

vues sur les problèmes juridiques du commerce électronique et la recherche des solutions correspondantes.[7]

18. Le Groupe de travail a poursuivi la révision des Règles uniformes à ses trente-troisième (1998) et trente-quatrième (1999) sessions sur la base des notes établies par le secrétariat (A/CN.9/WG.IV/WP.76 et A/CN.9/WG.IV/WP.79 et 80). Les rapports des sessions sont publiés sous les cotes A/CN.9/454 et 457.

19. À sa trente-deuxième session (1999), la Commission était saisie du rapport du Groupe de travail sur les travaux de ses trente-troisième (juin-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. 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 estimé 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.

20. Selon une opinion, l'approche qu'avait adoptée jusqu'ici le Groupe de travail ne tenait suffisamment compte de la nécessité, dans le monde des affaires, d'une souplesse dans l'utilisation des signatures électroniques ou autres techniques d'authentification. Les Règles uniformes, telles qu'actuellement envisagées, mettaient trop l'accent sur les signatures numériques et, dans cette optique même, sur une application particulière 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. Une réglementation de certaines utilisations des signatures électroniques était peut-être nécessaire en dehors du droit commercial, mais le Groupe de travail ne devrait participer à aucune activité de ce type.

21. Selon l'avis qui a largement prévalu, le Groupe de travail devrait poursuivre sa tâche sur la base de son mandat original. 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 l'élaboration d'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 aux clefs) correspondait 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 abonné), 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, 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, il a été 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 sur le plan technique (ibid., par. 68).

22. À l'issue du débat, la Commission a réaffirmé ses décisions précédentes quant à la faisabilité de la rédaction de règles uniformes et s'est déclarée certaine que le Groupe de travail pourrait progresser encore à ses prochaines sessions.[8]

23. Le Groupe de travail a poursuivi ses travaux à ses trente-cinquième (septembre 1999) et trente-sixième (février 2000) sessions en se fondant sur des notes établies par le secrétariat (A/CN.9/WG.IV/WP.82 et 84). À sa trente-troisième session (2000), la Commission était saisie du rapport du Groupe de travail sur les travaux de ces deux sessions (A/CN.9/465 et 467). Il a été noté que le Groupe de travail, à sa trente-sixième session, avait adopté le texte des projets d'articles 1 et 3 à 12 des Règles uniformes. Il restait, a-t-on dit, à clarifier certains points suite à la décision du Groupe de travail de supprimer dans le projet de Règles uniformes la notion de "signature électronique renforcée". On a exprimé la crainte qu'il soit nécessaire, en fonction des décisions que prendrait le Groupe de travail concernant les projets d'articles 2 et 13, de réexaminer les autres projets de dispositions pour éviter que la norme établie dans les Règles uniformes ne s'applique de la même façon aux signatures électroniques garantissant un niveau de sécurité élevé et aux certificats de moindre valeur susceptibles d'être utilisés dans les communications électroniques n'étant pas destinées à produire d'effet juridique important.

24. A l'issue des débats, la Commission a félicité le Groupe de travail pour les efforts qu'il avait fournis et les progrès qu'il avait accomplis dans l'élaboration des Règles uniformes. Elle l'a instamment prié de terminer ses travaux sur ce texte à sa trente-septième session et d'examiner le projet de guide que devait établir le Secrétariat.[9] [*Note du secrétariat: cette section relative à l'historique des Règles uniformes doit être complétée, et éventuellement rédigée de façon plus concise, après examen final et adoption des Règles uniformes par la Commission.]*

II. LES RÈGLES UNIFORMES COMME OUTIL D'HARMONISATION DES DROITS

25. Comme la Loi type, les Règles uniformes se présentent sous la forme d'un texte législatif qu'il est recommandé aux États d'incorporer dans leur droit national. Contrairement à ce qui se passe dans le cas d'une convention internationale, l'État qui adopte une législation type n'est pas tenu d'en aviser l'Organisation des Nations Unies ou les autres États qui ont pu eux aussi l'adopter. Les États sont toutefois vivement encouragés à informer le secrétariat de la CNUDCI de toute adoption des Règles uniformes (ou de toute autre loi type résultant des travaux de la CNUDCI).

26. En incorporant le texte de la législation type dans son système juridique, un État peut modifier ou exclure certaines de ses dispositions. Dans le cas d'une convention, la possibilité pour les États Parties d'apporter des changements (habituellement appelés "réserves") au texte uniforme est beaucoup plus limitée; en particulier, les conventions de droit commercial, le plus souvent, ou bien interdisent toute réserve, ou bien n'en autorisent que quelques-unes, qui sont spécifiées. La souplesse inhérente à une législation type est particulièrement souhaitable dans les cas où il est probable que l'État souhaitera apporter diverses modifications au texte uniforme avant d'être prêt à l'adopter dans son droit national. On peut s'attendre à certaines modifications, en particulier lorsque le texte uniforme a un lien étroit avec le système judiciaire et procédural national. Cela signifie cependant aussi que le degré d'harmonisation et de certitude quant à l'harmonisation,

atteint par une législation type, sera probablement moins élevé que dans le cas d'une convention. Cet inconvénient relatif peut néanmoins être compensé par le fait qu'il y a probablement plus d'États adoptant une législation type que d'États adhérant à une convention. Pour atteindre un degré satisfaisant d'harmonisation et de certitude, il est recommandé que les États apportent aussi peu de modifications que possible lors de l'incorporation des Règles uniformes dans leur système juridique. D'une façon générale, lors de l'adoption des Règles uniformes (ou de la Loi type), il est souhaitable d'adhérer autant que possible au texte uniforme de manière à rendre le droit national aussi transparent que possible pour les étrangers qui l'utiliseront.

III. OBSERVATIONS GÉNÉRALES SUR LES SIGNATURES ÉLECTRONIQUES[10]

A. Fonctions de la signature

27. L'article 7 de la Loi type de la CNUDCI sur le commerce électronique se fonde sur la reconnaissance des fonctions remplies par la signature dans les échanges sur papier. Lors des travaux préparatoires ayant trait à la Loi type, le Groupe de travail a examiné les fonctions suivantes traditionnellement remplies par les signatures manuscrites: identification d'une personne; certitude quant à la participation en personne de l'intéressé dans l'acte de signature; association de cette personne avec la teneur d'un document. Il a été noté qu'en outre la signature pouvait remplir diverses fonctions, selon la nature du document signé. Par exemple, une signature peut témoigner de l'intention d'une partie d'être liée par la teneur d'un contrat signé; de l'intention d'une personne de revendiquer la paternité d'un texte (montrant ainsi qu'elle a conscience du fait que l'acte de signature peut avoir éventuellement des conséquences juridiques); de l'intention d'une personne de s'associer au contenu d'un document rédigé par quelqu'un d'autre; du fait que et du moment où une personne se trouvait en un lieu donné. La relation entre les Règles uniformes et l'article 7 de la Loi type est examinée plus avant aux paragraphes 67 et 70 à 75 du présent Guide.

28. Dans un environnement électronique, l'original d'un message ne se distingue pas d'une copie, ne comporte aucune signature manuscrite et ne figure pas sur papier. Les possibilités de fraude sont énormes, du fait de la facilité qu'il y a à intercepter et modifier l'information sous forme électronique sans risque d'être détecté, ainsi que de la rapidité avec laquelle on peut traiter de multiples transactions. La finalité des diverses techniques actuellement disponibles sur le marché ou en cours de mise au point consiste à créer les possibilités techniques au moyen desquelles un certain nombre ou la totalité des fonctions perçues comme caractéristiques d'une signature manuscrite peuvent être remplies dans un contexte électronique. De manière générale, ces techniques sont qualifiées de "signatures numériques".

B. Signatures numériques et autres signatures électroniques

29. Lorsqu'elle a examiné s'il était opportun et possible d'élaborer des Règles uniformes, et défini leur champ d'application, la CNUDCI a examiné les diverses techniques de signatures électroniques qui étaient utilisées ou en cours de mise au point. L'objectif commun à ces techniques est de fournir des équivalents fonctionnels à 1) la signature manuscrite et 2) aux autres types de mécanismes d'authentification utilisés dans le cas des documents sur papier (par exemple, sceaux ou cachets). Les mêmes techniques peuvent remplir des fonctions supplémentaires dans le domaine du commerce électronique, qui découlent des fonctions d'une signature mais où elles n'ont aucun équivalent strict dans le cas des documents papiers.

30. Ainsi qu'il a été indiqué plus haut, les gouvernements et parlements de nombreux pays qui sont en train d'élaborer une législation sur les questions relatives aux signatures électroniques, y compris la mise en place d'infrastructures à clef publique ou autres projets sur des questions étroitement liées (voir A/CN.9/457, par. 16) attendent des orientations de la CNUDCI. Quant à la décision prise par la CNUDCI de se concentrer sur les questions et sur la terminologie de la cryptographie à clef publique, il convient de noter que le jeu des relations entre trois types distincts de parties (les signataires, les prestataires de services de certification et les parties se fiant aux clefs) correspond à un modèle possible de cryptographie à clef publique, mais que d'autres modèles sont concevables (sans intervention d'une autorité de certification indépendante, par exemple). L'un des principaux avantages qu'il y a à se concentrer sur les questions relatives à la cryptographie à clef publique est que l'on peut ainsi structurer plus facilement les Règles uniformes par référence à trois fonctions (ou rôles) associées aux signatures électroniques, à savoir, la fonction de signataire (émetteur de la clef ou abonné) la fonction de certification, et la fonction de confiance. Ces trois fonctions sont communes dans tous les modèles de cryptographie à clef publique et il faudrait les traiter, qu'elles soient exercées par trois entités séparées ou que deux d'entre elles soient assurées par la même personne (par exemple, lorsque le prestataire de services de certification est également une partie se fiant à la clef). En outre, en se concentrant sur les fonctions typiques de la cryptographie à clef publique et non sur un modèle particulier, on parvient plus facilement à élaborer une règle tout à fait neutre sur le plan technique dans la mesure où des fonctions similaires sont remplies dans le cas d'une technique de signature électronique autre qu'une infrastructure à clef publique.

1. Signatures électroniques faisant appel à des techniques autres que la cryptographie à clef publique

31. Parallèlement aux "signatures numériques" s'appuyant sur la cryptographie fonctionnant par création d'une clef publique, il existe divers autres mécanismes, recouverts eux aussi par la notion plus large de "signatures électroniques" qui peuvent être en usage ou dont on envisage l'utilisation dans l'avenir, en vue de remplir une ou plusieurs des fonctions susmentionnées des signatures manuscrites. Par exemple, certaines techniques, pour garantir l'authentification, utiliseraient un dispositif biométrique s'appuyant sur les signatures manuscrites. Avec un tel dispositif, le signataire apposerait sa signature manuscrite à l'aide d'un stylo spécial, soit sur un écran d'ordinateur, soit sur un bloc numérique. La signature manuscrite serait alors analysée par ordinateur et mise en mémoire sous forme d'un ensemble de valeurs numériques, qui pourrait être ajouté, à un message de données et affiché par le destinataire aux fins d'authentification. Ce système d'authentification présupposerait que des échantillons de la signature manuscrite ont été préalablement analysés et mis en mémoire par le dispositif biométrique.

32. Peu d'informations sur les incidences techniques et juridiques de l'utilisation de dispositifs de "signatures" fondés sur des techniques autres que la cryptographie à clef publique ont été fournies au Groupe de travail de la CNUDCI sur le commerce électronique lors de l'élaboration des Règles uniformes. Étant donné qu'il existe des informations préliminaires suffisantes sur les conséquences juridiques des signatures numériques, et que des projets de loi sur le sujet ont été élaborés dans un certain nombre de pays, la CNUDCI a axé ses travaux sur les questions des signatures numériques faisant appel à la cryptographie à clef publique.

33. La CNUDCI a toutefois souhaité élaborer des Règles uniformes de nature à faciliter l'utilisation aussi bien de signatures numériques que d'autres formes de signatures électroniques. À cet effet, elle a essayé de traiter les questions juridiques liées aux

signatures électroniques à un niveau intermédiaire entre le caractère très général de la Loi type et le degré de détail qui peut être nécessaire dans le cas d'une signature particulière. En tout état de cause, conformément au principe de neutralité technique énoncé dans la Loi type, les Règles uniformes ne doivent pas être interprétées comme décourageant l'utilisation d'une méthode quelle qu'elle soit de signature électronique, que celle-ci existe déjà ou doive être mise en œuvre dans l'avenir.

2. Signatures numériques utilisant la cryptographie à clef publique[11]

34. Étant donné l'usage croissant des techniques de signature numérique dans un certain nombre de pays, l'introduction ci-après pourra être utile à ceux qui élaborent des lois sur les signatures électroniques.

a) Notions et terminologie techniques

i) Cryptographie

35. Les signatures numériques sont créées et vérifiées grâce à la cryptographie, branche des mathématiques appliquées qui s'occupe de la transformation de messages en des formes apparemment inintelligibles et de leur restitution dans leur forme initiale. Les signatures numériques utilisent ce que l'on appelle la "cryptographie à clef publique", qui est souvent basée sur l'utilisation de fonctions algorithmiques pour créer deux "clefs" (c'est-à-dire des nombres de plusieurs chiffres générés à l'aide d'une série de formules mathématiques appliquées aux nombres premiers) différentes mais mathématiquement liées entre elles. L'une de ces clefs est utilisée pour créer une signature numérique ou pour transformer des données en une forme apparemment inintelligible, et l'autre pour vérifier une signature numérique ou restituer le message dans sa forme initiale. Le matériel et le logiciel informatiques utilisant deux clefs de ce type sont souvent appelés collectivement "cryptosystèmes" ou, plus précisément "cryptosystèmes asymétriques" lorsqu'ils utilisent des algorithmes asymétriques.

36. Bien que le recours à la cryptographie soit l'une des principales caractéristiques des signatures numériques, le simple fait qu'une signature numérique soit utilisée pour authentifier un message contenant des données sous forme numérique ne doit pas être assimilé à l'utilisation plus générale de la cryptographie à des fins de confidentialité. Le codage pour raison de confidentialité est une méthode utilisée pour coder une communication électronique de manière que seuls l'initiateur et le destinataire du message seront en mesure de le lire. Dans un certain nombre de pays, la loi restreint l'utilisation de la cryptographie à cette fin pour des raisons d'ordre public qui peuvent comporter des considérations de défense nationale. Cependant, l'utilisation de la cryptographie aux fins d'authentification par la création d'une signature numérique n'implique pas nécessairement le recours au codage pour garantir le caractère confidentiel d'une communication, étant donné que la signature numérique codée peut être tout simplement jointe à un message non codé.

ii) Clefs publiques et privées

37. Les clefs complémentaires utilisées pour les signatures numériques sont appelées la "clef privée", qui n'est utilisée que par le signataire pour créer la signature numérique, et la "clef publique", qui est d'ordinaire plus largement connue et est utilisée par une partie se fiant à la signature pour vérifier la signature numérique. Il appartient à l'utilisateur d'une clef privée de maintenir la clef privée secrète. On notera que l'utilisateur individuel n'a pas besoin de connaître la clef privée. Une telle clef privée est normalement conservée

sur une carte à mémoire, ou est normalement accessible grâce à un numéro d'identification personnel ou, dans l'idéal, grâce à un dispositif d'identification biométrique, par exemple un dispositif de reconnaissance d'empreinte de pouce. Si plusieurs personnes ont besoin de vérifier les signatures numériques du signataire, la clef publique doit être rendue accessible ou distribuée à l'ensemble de ces personnes en la publiant, par exemple, dans un répertoire en ligne ou dans toute autre forme de répertoire public où elle est facilement accessible. Bien que les clefs de la paire soient mathématiquement liées, si un système de cryptographie asymétrique a été conçu et mis en œuvre de façon sécurisée, il est pratiquement impossible, connaissant la clef publique, de déduire la clef privée. Les algorithmes les plus courants de chiffrement par utilisation de clefs publiques et privées reposent sur une caractéristique importante des grands nombres premiers: une fois multipliés ensemble pour produire un nouveau nombre, il est particulièrement difficile et long de déterminer les deux nombres premiers qui ont créé ce nouveau nombre plus important.[12] Ainsi, bien que de nombreuses personnes connaissent la clef publique d'un signataire donné et l'utilisent pour vérifier les signatures de ce signataire, elles ne peuvent découvrir la clef privée de ce signataire et l'utiliser pour falsifier des signatures numériques.

38. On notera, cependant, que le concept de cryptographie à clef publique ne nécessite pas forcément l'utilisation des algorithmes susmentionnés, fondés sur des nombres premiers. On utilise ou l'on met au point actuellement d'autres techniques mathématiques telles que des systèmes de cryptographie fondés sur des courbes elliptiques, souvent décrits comme offrant un niveau élevé de sécurité grâce à l'utilisation de longueurs de clefs considérablement réduites.

iii) Fonction de hachage

39. Outre la production de paires de clefs, un autre processus fondamental, généralement appelé "fonction de hachage", est utilisé à la fois pour créer et pour vérifier une signature numérique. Une fonction de hachage est un processus mathématique fondé sur un algorithme, qui crée une représentation numérique - ou forme comprimée du message souvent appelée "abrégé" ou "empreinte digitale", et qui prend la forme d'une "valeur de hachage" ou d'un "résultat de hachage" d'une longueur normalisée généralement bien plus courte que le message lui-même mais qui lui est néanmoins unique. Toute modification apportée au message produit inévitablement un résultat de hachage différent lorsqu'on utilise la même fonction de hachage. Dans le cas d'une fonction de hachage sécurisée, parfois appelée "fonction de hachage unidirectionnelle", il est pratiquement impossible, connaissant la valeur de hachage, de déduire le message initial. Les fonctions de hachage permettent donc au programme de création de signatures numériques d'opérer sur des volumes de données limités et prévisibles tout en établissant une solide corrélation avec la teneur du message initial, ce qui lui permet d'assurer qu'aucune modification n'a été apportée au message depuis que ce dernier a été signé sous forme numérique.

iv) Signature numérique

40. Pour signer un document ou toute autre information, le signataire commence par définir précisément les limites de ce qu'il doit signer. Ensuite, une fonction de hachage opérant dans le programme du signataire calcule un résultat de hachage propre (à toutes fins pratiques) à l'information qui doit être signée. Le programme du signataire transforme ensuite le résultat de hachage en une signature numérique à l'aide de la clef privée du signataire. La signature numérique résultante est par conséquent propre à la fois à l'information signée et à la clef privée utilisée pour créer la signature numérique.

41. Généralement, une signature numérique (un résultat de hachage signé numériquement) est attachée au message et stockée ou transmise avec ce message. Cependant, elle peut également être envoyée ou stockée comme élément de données distinct, aussi longtemps qu'elle maintient une association fiable avec le message correspondant. Étant donné qu'une signature numérique est propre à son message, elle est inutile si on la dissocie de façon permanente dudit message.

v) Vérification de la signature numérique

42. La vérification de la signature numérique consiste à vérifier la signature numérique par rapport au message initial et à une clef publique donnée, et à déterminer de cette façon si la signature numérique a été créée pour ce même message à l'aide de la clef privée correspondant à la clef publique référencée. La vérification d'une signature numérique s'effectue en calculant un nouveau résultat de hachage du message initial au moyen de la fonction de hachage utilisée pour créer la signature numérique. Ensuite, à l'aide de la clef publique et du nouveau résultat de hachage, le contrôleur vérifie si la signature numérique a été créée à l'aide de la clef privée correspondante, et si le résultat de hachage nouvellement calculé correspond au résultat de hachage initial qui a été transformé en signature numérique au cours du processus de signature.

43. Le programme de vérification confirmera la signature numérique comme étant "vérifiée": 1) si la clef privée du signataire a été utilisée pour signer numériquement le message, ce qui est avéré si la clef publique du signataire a été utilisée pour vérifier la signature étant donné que la clef publique du signataire permettra de vérifier uniquement une signature numérique créée à l'aide de la clef privée du signataire; et 2) si le message ne subit aucune modification, ce qui est avéré si le résultat de hachage calculé par la personne chargée de la vérification est identique au résultat de hachage extrait de la signature numérique lors du processus de vérification.

b) Infrastructure à clef publique et prestataires de services de certification

44. Pour vérifier une signature numérique, le vérificateur doit avoir accès à la clef publique du signataire et s'assurer que celle-ci correspond bien à la clef privée du signataire. Cependant, une paire de clefs publique et privée n'a aucune association intrinsèque avec une personne quelconque; il s'agit simplement d'une paire de nombres. Un mécanisme supplémentaire est nécessaire pour associer de manière fiable une personne ou une entité particulière à la paire de clefs. Si l'on veut que le chiffrement à clef publique remplisse sa fonction, il faut trouver un moyen d'envoyer les clefs à un grand nombre de personnes, dont beaucoup sont inconnues de l'expéditeur, et alors même qu'aucune relation de confiance ne s'est forgée entre les parties. Pour ce faire, les parties concernées doivent avoir une très grande confiance dans les clefs publiques et privées émises.

45. Le degré requis de confiance peut exister entre deux parties qui se font confiance, qui ont traité l'une avec l'autre sur une certaine durée, qui communiquent sur des systèmes fermés, qui fonctionnent à l'intérieur d'un groupe fermé, ou dont les relations sont régies par contrat - par exemple dans le cadre d'un accord entre partenaires commerciaux. Si une transaction ne fait intervenir que deux parties, chaque partie peut simplement communiquer (par un moyen relativement sûr tel qu'un coursier ou un téléphone, qui permet la reconnaissance de voix) la clef publique de la paire de clefs que chaque partie va utiliser. Cependant, il se peut que le même degré de confiance soit absent lorsque les parties ont peu affaire l'une à l'autre, communiquent sur des systèmes ouverts (par exemple Internet), ne font pas partie d'un groupe fermé, n'ont pas conclu d'accord entre partenaires commerciaux ou lorsque leur relation n'est pas régie par un droit particulier.

46. En outre, étant donné que le chiffrement à clef publique est une technique hautement mathématique, tous les utilisateurs doivent avoir confiance dans les compétences, les connaissances et les dispositifs de sécurité des parties émettant les clefs publiques et privées.[13]

47. Un signataire éventuel pourrait faire une déclaration publique indiquant que les signatures vérifiables au moyen d'une clef publique donnée devraient être considérées comme provenant de lui. Cependant, d'autres parties pourraient refuser d'accepter cette déclaration, en particulier lorsqu'il n'existe aucun contrat préalable établissant avec certitude l'effet juridique de ladite déclaration. Une partie se fiant à une telle déclaration non étayée publiée dans un système ouvert courrait alors un risque important de faire confiance, à son insu, à un imposteur ou d'avoir à établir qu'il n'y a pas eu refus de signature numérique (point souvent appelé "non-répudiation") dans les cas où une transaction s'avérerait défavorable pour le signataire supposé.

48. L'une des solutions à ce problème consiste à recourir à un ou plusieurs tiers à qui l'on fait toute confiance pour associer un signataire identifié ou le nom de ce signataire à une clef publique spécifique. Cette tierce partie est généralement appelée, dans la plupart des normes et directives techniques, "autorité de certification", "fournisseur de services de certification" ou "prestataire de services de certification" (dans les Règles uniformes, c'est l'expression "prestataire de services de certification" qui a été retenue). Dans plusieurs pays, ces autorités de certification s'organisent de façon hiérarchique en ce que l'on appelle souvent une infrastructure à clef publique.

i) Infrastructure à clef publique

49. La création d'une infrastructure à clef publique est un moyen d'inspirer confiance dans le fait que: 1) la clef publique de l'utilisateur n'a pas été falsifiée et correspond effectivement à la clef privée de l'utilisateur; 2) les techniques de chiffrement utilisées sont bonnes; 3) l'on peut faire confiance aux entités délivrant les clefs cryptographiques pour préserver ou recréer les clefs publiques et privées susceptibles d'être utilisées pour le chiffrement afin d'assurer la confidentialité lorsque le recours à cette technique est autorisé; 4) les différents systèmes de chiffrement sont compatibles. Pour inspirer cette confiance, l'infrastructure à clef publique peut offrir un certain nombre de services, dont les suivants: 1) gestion des clefs cryptographiques utilisées pour les signatures numériques; 2) assurance qu'une clef publique correspond bien à une clef privée; 3) communication des clefs aux utilisateurs finaux; 4) décision selon laquelle tel ou tel utilisateur se verra conférer tel ou tel privilège dans le système; 5) publication d'un répertoire sécurisé des clefs publiques ou des certificats; 6) gestion des jetons personnalisés (par exemple cartes à mémoire) capables d'identifier l'utilisateur au moyen d'éléments d'identification personnels propres à l'intéressé ou capables de créer et de garder en mémoire les clefs privées d'un individu; 7) vérification de l'identité des utilisateurs finaux et offre de services à ces derniers; 8) offre de services de non-répudiation; 9) offre de services de marquage; 10) gestion des clefs de chiffrement utilisées pour le chiffrement de confidentialité lorsque le recours à cette technique est autorisé.

50. L'infrastructure à clef publique s'appuie souvent sur divers niveaux d'autorité. Par exemple, les modèles envisagés dans certains pays pour établir une éventuelle infrastructure se réfèrent notamment aux niveaux d'autorité suivants: 1) une "autorité centrale" unique, qui homologuerait la technologie et les pratiques de toutes les parties autorisées à utiliser les paires de clefs cryptographiques ou de certificats permettant l'utilisation de ces paires de clefs, et qui homologuerait les prestataires de services de certification subordonnés;[14] 2) divers prestataires de services de certification, situés en

dessous de “l’autorité centrale”, qui garantiraient que la clef publique d’un utilisateur correspond effectivement à la clef privée de cet utilisateur (autrement dit, que la clef n’a pas été manipulée); et 3) diverses autorités locales d’enregistrement, placées sous les prestataires de services de certification et chargées de répondre aux demandes des utilisateurs de se voir attribuer des paires de clefs cryptographiques ou un certificat relatif à l’utilisation de ces paires de clefs et chargées d’exiger une preuve d’identité et de vérifier l’identité d’utilisateurs éventuels. Dans certains pays, il est envisagé de confier aux notaires la fonction d’autorité locale d’enregistrement, ou tout au moins d’apporter leur concours à cette fonction.

51. Il se peut que les questions d’infrastructure à clef publique ne se prêtent pas aisément à une harmonisation internationale. En effet, l’organisation d’une infrastructure à clef publique peut faire intervenir diverses questions techniques ainsi que l’action des pouvoirs publics, questions qu’il est peut-être préférable de laisser à la discrétion de chaque État.[15] À cet égard, chaque État devra peut-être prendre des décisions relatives à l’établissement d’une infrastructure à clef publique, concernant notamment les éléments suivants: 1) la modalité et le nombre de niveaux d’autorité devant constituer l’infrastructure à clef publique; 2) la question de savoir si certaines autorités appartenant à l’infrastructure devraient être autorisées à délivrer les paires de clefs cryptographiques ou si ces paires de clefs peuvent être créées par les utilisateurs eux-mêmes; 3) la question de savoir si les prestataires de services de certification garantissant la validité des paires de clefs cryptographiques devraient être des entités publiques ou si des entités privées pourraient agir en cette qualité; 4) la question de savoir si le processus par lequel on autorise une entité donnée à agir en qualité d’autorité de certification devrait se faire sous forme d’autorisation expresse, ou d’octroi d’une “licence” par l’État, ou si d’autres méthodes devraient être utilisées pour veiller à la qualité des prestataires de services de certification si ceux-ci sont autorisés à opérer en l’absence d’une autorisation spécifique; 5) la mesure dans laquelle une utilisation de la cryptographie devrait être autorisée à des fins de confidentialité; et 6) la question de savoir si l’État doit conserver l’accès à l’information chiffrée, au moyen d’un mécanisme de “blocage” de la clef ou autrement. Les Règles uniformes ne traitent pas de ces questions.

ii) Prestataires de services de certification

52. Pour associer une paire de clefs avec un signataire éventuel, le prestataire de services de certification délivre un certificat, enregistrement électronique qui précise la clef publique ainsi que le nom du détenteur du certificat comme “sujet” du certificat et qui peut confirmer que le signataire éventuel identifié dans le certificat détient la clef privée correspondante. La fonction essentielle d’un certificat est d’associer une clef publique à un détenteur précis. Un “destinataire” du certificat souhaitant se fier à une signature numérique créée par le détenteur cité dans le certificat peut utiliser la clef publique figurant dans le certificat pour vérifier que la signature numérique a bel et bien été créée avec la clef privée correspondante. Si cette vérification est positive, le destinataire est assuré que la signature numérique a effectivement été créée par le détenteur de la clef publique citée dans le certificat, et que le message correspondant n’a pas été modifié depuis qu’on y a apposé une signature numérique.

53. Pour assurer l’authenticité du certificat s’agissant tant de sa teneur que de sa source, l’autorité de certification y appose une signature numérique. La signature numérique de l’autorité de certification qui délivre le certificat peut être vérifiée au moyen de la clef publique de l’autorité de certification figurant sur un autre certificat délivré par une autre autorité de certification (qui peut être, mais n’est pas nécessairement, une autorité

hiérarchique supérieure), et cet autre certificat peut à son tour être identifié par la clef publique figurant sur un autre certificat encore, et ainsi de suite, jusqu'à ce que la personne devant s'assurer de la signature numérique soit convaincue de son authenticité. Dans chaque cas, l'autorité de certification délivrant le certificat doit apposer une signature numérique sur son propre certificat pendant la période de validité de l'autre certificat utilisé pour vérifier la signature numérique de l'autorité de certification.

54. Une signature numérique correspondant à un message, qu'elle soit créée par le détenteur de la paire de clefs pour identifier un message ou par l'autorité de certification pour authentifier son certificat, devrait généralement être datée pour permettre au vérificateur de déterminer de manière fiable si la signature numérique a bien été créée pendant la "période de validité" citée dans le certificat, ce qui est l'une des conditions permettant de vérifier une signature numérique.

55. Pour que la clef publique – et son association à un détenteur spécifique – soit aisément disponible pour vérification, le certificat peut être publié dans un répertoire ou mis à disposition par d'autres moyens. Généralement, les répertoires sont des bases de données en ligne regroupant des certificats et d'autres informations disponibles pouvant être appelés et utilisés pour vérifier la signature numérique.

56. Une fois délivré, un certificat peut se révéler sujet à caution, par exemple si le détenteur a donné une fausse identité à l'autorité de certification. Dans d'autres circonstances, un certificat peut être fiable au moment où il est délivré, mais devenir sujet à caution par la suite. Si la clef privée est "compromise", par exemple parce que le détenteur de la clef privée en a perdu le contrôle, le certificat peut perdre sa fiabilité. Alors, l'autorité de certification (à la demande du détenteur ou même sans son consentement, selon les circonstances) peut suspendre (interrompre provisoirement la période de validité) ou révoquer (annuler de manière permanente) le certificat. Dès la suspension ou la révocation d'un certificat, l'autorité de certification doit généralement publier une notification de la révocation ou de la suspension ou notifier les personnes qui l'interrogent ou dont on sait qu'elles ont reçu une signature numérique vérifiable au moyen du certificat douteux.

57. On peut concevoir que les autorités de certification relèvent des pouvoirs publics ou bien de prestataires de services du secteur privé. Dans certains pays, on envisage, pour des raisons d'ordre public, que seuls des organismes d'État soient autorisés à faire office d'autorité de certification. Dans d'autres, on considère que les services de certification doivent faire l'objet d'une libre concurrence sur le marché privé. Indépendamment du fait que les autorités de certification relèvent d'organismes publics ou de prestataires de services privés, et du fait qu'elles aient ou non besoin de se faire délivrer une licence pour fonctionner, il existe, généralement, plus d'une autorité de certification fonctionnant dans l'infrastructure à clef publique. Tout particulièrement importante est la relation qui existe entre les différentes autorités de certification. Les autorités de certification d'une infrastructure à clef publique peuvent être établies en une structure hiérarchique où certaines autorités de certification ne font que vérifier d'autres autorités de certification qui assurent les services directement aux usagers. Dans une telle structure, les autorités de certification sont subordonnées à d'autres. Dans d'autres structures envisageables, certaines autorités de certification peuvent fonctionner sur un pied d'égalité avec d'autres autorités de certification. Dans toute infrastructure importante il y aura vraisemblablement des autorités de certification subordonnées et supérieures. En tout état de cause, en l'absence d'une infrastructure internationale, un certain nombre de questions peuvent se poser s'agissant de la reconnaissance des certificats par les autorités de certification d'autres pays. La reconnaissance de certificats étrangers s'effectue souvent au moyen de

ce que l'on appelle une "certification croisée". En pareil cas, il est indispensable que des autorités de certification pour l'essentiel égales (ou acceptant tout au moins de prendre certains risques s'agissant des certificats délivrés par d'autres autorités de certification) reconnaissent les services assurés par l'une et l'autre, de sorte que leurs usagers respectifs puissent communiquer entre eux de manière plus efficace et en accordant une plus grande confiance aux certificats émis.

58. Des questions juridiques peuvent se poser dans le cadre de la certification croisée ou des certificats en chaîne lorsque des politiques de sécurité multiples entrent en jeu. Il peut s'agir notamment de déterminer quel méfait à causé une perte, ou à qui l'usager s'est fié. On notera que les règles juridiques envisagées dans certains pays disposent que, là où les politiques en vigueur et les questions de sécurité sont connues des usagers, et où n'existe aucune négligence de la part des autorités de certification, aucune responsabilité ne peut être engagée.

59. Il peut incomber à l'autorité de certification ou à l'autorité centrale de veiller à ce que ces prescriptions soient systématiquement respectées. Si la sélection des autorités de certification peut se faire en fonction d'un certain nombre de facteurs, dont la solidité de la clef publique utilisée et l'identité de l'usager, la crédibilité de toute autorité de certification peut également dépendre de son respect des normes de délivrance de certificats et de la justesse de son évaluation des données communiquées par les usagers qui demandent le certificat. D'une importance toute particulière est le régime de responsabilité s'appliquant à l'autorité de certification s'agissant de son respect des prescriptions en matière de politique générale et de sécurité édictées par l'autorité centrale ou par l'autorité de certification supérieure, ou de toute autre prescription applicable, et ce de manière permanente.

60. Lors de l'élaboration des Règles uniformes, il a été considéré qu'il fallait tenir compte, lorsqu'on évalue la fiabilité d'une autorité de certification, des facteurs suivants: 1) indépendance (c'est-à-dire l'absence d'intérêts financiers ou autres dans les transactions en jeu; 2) ressources et moyens financiers permettant d'assumer le risque de voir sa responsabilité mise en cause en cas de perte; 3) maîtrise de la technologie des clefs publiques et familiarité avec les procédures de sécurité concernées; 4) durée (les autorités de certification peuvent en effet être amenées à donner des preuves de certification ou à décrypter des clefs plusieurs années après la fin de la transaction, par exemple dans le cadre d'une action en justice ou d'un litige relatif à la propriété); 5) homologation du matériel et du logiciel; 6) mise en place d'une vérification à rebours et vérification par une entité indépendante; 7) existence d'un plan d'urgence (par exemple logiciel de "récupération catastrophe" ou mécanisme de "blocage" de la clef); 8) sélection et gestion du personnel; 9) dispositif de protection s'agissant de la clef privée de l'autorité de certification; 10) sécurité interne; 11) arrangements pour la fin des opérations, y compris notification aux utilisateurs; 12) garanties et responsabilités (consenties ou exclues); 13) limites de responsabilité; 14) assurance; 15) compatibilité avec d'autres autorités de certification; 16) procédures de révocation (dans les cas où les clefs cryptographiques viendraient à être perdues ou compromises).

c) Résumé du processus de signature numérique

61. L'utilisation d'une signature numérique met habituellement en jeu les processus suivants, effectués soit par le signataire, soit par le destinataire du message signé numériquement:

1) L'utilisateur crée ou se voit attribuer une paire de clefs cryptographiques qui lui est propre;

2) L'expéditeur rédige un message (par exemple sous forme d'un courrier électronique) sur l'ordinateur;

3) L'expéditeur prépare un "abrégé" de son message à l'aide d'un calcul algorithmique sûr. La création de la signature numérique utilise un résultat de hachage calculé à partir à la fois du message signé et d'une clef privée donnée et qui leur est unique. Pour assurer la sûreté du résultat du calcul, il est impératif qu'il n'y ait qu'une possibilité infime que la même signature numérique puisse être créée par la combinaison de tout autre message ou de toute autre clef;

4) L'expéditeur chiffre l'abrégé du message à l'aide de la clef privée. Celle-ci s'applique à l'abrégé du message à l'aide d'un algorithme mathématique. La signature numérique est constituée par l'abrégé du message ainsi chiffré;

5) L'expéditeur appose ou annexe généralement sa signature numérique au message;

6) L'expéditeur envoie sa signature numérique et le message (chiffré ou non) au destinataire par voie électronique;

7) Le destinataire utilise la clef publique de l'émetteur pour vérifier la signature numérique de l'expéditeur. La vérification à l'aide de la clef publique de l'expéditeur prouve que le message provient exclusivement dudit expéditeur;

8) Le destinataire crée lui aussi un "abrégé du message" à l'aide du même algorithme;

9) Le destinataire compare les deux abrégés de message. S'ils sont identiques, le destinataire sait que le message n'a pas été modifié après avoir été signé. Même si le message a subi une très légère modification après avoir reçu une signature numérique, l'abrégé de message créé par le destinataire sera différent de celui créé par l'expéditeur;

10) Le destinataire se voit délivrer par l'autorité de certification (ou par l'intermédiaire de l'expéditeur du message) un certificat qui confirme la signature numérique apposée au message de l'expéditeur. L'autorité de certification est généralement un tiers inspirant toute confiance, qui administre la certification du système de signature numérique. Le certificat comporte la clef publique et le nom de l'expéditeur (éventuellement accompagnés de renseignements complémentaires) signés numériquement par l'autorité de certification.

IV. PRINCIPALES CARACTÉRISTIQUES DES RÈGLES UNIFORMES

A. Nature législative des Règles uniformes

62. Les Règles uniformes ont été préparées en partant du principe qu'elles devraient s'inspirer directement de l'article 7 de la Loi type et devraient être considérées comme un moyen de donner des renseignements précis sur le concept de "méthode fiable" utilisé pour identifier "une personne" et pour indiquer "qu'elle approuve l'information" contenue dans le message de données (voir A/CN.9/WG.IV/WP.71, par. 49).

63. La question de la forme que pourrait prendre le projet de Règles uniformes a été soulevée, et l'on a noté la nécessité d'étudier la relation entre la forme et le contenu. Différentes méthodes ont été proposées quant à ce que pourrait être cette forme, y compris des règles contractuelles, des dispositions législatives ou des principes directeurs destinés aux États envisageant d'adopter une législation sur les signatures électroniques. Il a été convenu, comme hypothèse de travail, que les Règles uniformes devraient prendre la forme

de règles législatives assorties de commentaires, et non simplement de principes directeurs (voir A/CN.9/437, par. 27; A/CN.9/446, par. 25; et A/CN.9/457, par. 51 et 72).

B. Relations avec la Loi type de la CNUDCI sur le commerce électronique

1. Règles uniformes constituant un instrument juridique distinct

64. Les Règles uniformes auraient pu être incorporées dans une version augmentée de la Loi type, par exemple pour former une nouvelle troisième partie. Afin d'indiquer clairement que les Règles uniformes pourraient être adoptées soit de façon indépendante, soit en combinaison avec la Loi type, il a été finalement décidé que les Règles uniformes devraient constituer un instrument juridique distinct (voir A/CN.9/465, par. 37). Cette décision découle essentiellement du fait qu'au moment de l'établissement de la version définitive des Règles uniformes, la Loi type avait déjà été appliquée avec succès dans plusieurs pays et que de nombreux autres envisageaient de l'adopter. L'élaboration d'une version augmentée de la Loi type aurait pu compromettre le succès de la version originale en donnant à penser qu'il était nécessaire d'améliorer ce texte au moyen d'une mise à jour. En outre, l'élaboration d'une nouvelle version de la Loi type aurait pu introduire une confusion dans les pays qui l'avaient récemment adoptée.

2. Règles uniformes pleinement conformes à la Loi type

65. Lors de l'élaboration des Règles uniformes, tout a été mis en œuvre pour assurer une cohérence aussi bien avec le fond qu'avec la terminologie de la Loi type (voir A/CN.9/465, par. 37). Les dispositions générales de la Loi type ont été reproduites dans les Règles uniformes. Il s'agit de l'article premier (Champ d'application); des alinéas a), c) et d) de l'article 2 (Définitions de "message de données", "expéditeur" et "destinataire"), et des articles 3 (Interprétation), 4 (Dérogation conventionnelle) et 7 (Signature) de la Loi type.

66. 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 (A/CN.9/WG.IV/WP.84, par. 16). 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).

3. Relations avec l'article 7 de la Loi type

67. Lors de l'élaboration des Règles uniformes, il a été exprimé l'avis que la référence à l'article 7 de la Loi type dans le texte de l'article 6 des Règles uniformes devait être interprétée comme limitant le champ d'application des Règles aux situations dans lesquelles une signature électronique était utilisée pour satisfaire à une prescription légale impérative selon laquelle certains documents devaient être signés pour être valides. Dans la mesure où la loi contenait très peu de prescriptions de ce type applicables aux documents utilisés dans les transactions commerciales, le champ d'application des Règles uniformes était très étroit. On a généralement convenu, en réponse à cet argument, que cette interprétation de l'article 6 (et de l'article 7 de la Loi type) était incompatible avec l'interprétation du terme "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". En fait, le champ d'application tant de l'article 7 de la Loi type que de l'article 6 des Règles uniformes est particulièrement vaste dans la mesure où la plupart des documents utilisés dans le contexte de 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).

C. Règles "cadres" devant être complétées par des règlements techniques et par contrat

68. En tant que supplément à la Loi type de la CNUDCI sur le commerce électronique, les Règles uniformes ont pour objet de proposer des principes essentiels devant faciliter l'utilisation des signatures électroniques. Cependant, en tant que "cadre", les Règles uniformes elles-mêmes n'énoncent pas toutes les règles et tous les règlements qui peuvent être nécessaires (en sus des arrangements contractuels entre utilisateurs) pour appliquer ces techniques dans un État adoptant. Qui plus est, comme l'indique le présent Guide, les Règles uniformes n'ont pas pour objet de couvrir chaque aspect de l'utilisation des signatures électroniques. En conséquence, un État adoptant pourra souhaiter adopter des règlements destinés à compléter les procédures autorisées par les Règles uniformes et à prendre en compte les conditions particulières, éventuellement changeantes, prévalant dans l'État adoptant, sans compromettre les objectifs des Règles uniformes. Il est recommandé à tout État adoptant qui déciderait d'adopter une telle réglementation d'accorder une attention particulière à la nécessité de maintenir une certaine souplesse dans l'utilisation des systèmes de signature électronique par leurs utilisateurs.

69. On notera que les techniques de signature électronique envisagées dans les Règles uniformes, outre qu'elles soulèvent des questions de procédure qui pourront devoir être traitées dans les règles techniques d'application, peuvent soulever certaines questions juridiques dont la réponse ne se trouvera pas nécessairement dans les Règles uniformes, mais plutôt dans d'autres textes de loi. Ces autres textes de loi pourront inclure, par exemple, les textes de procédure administrative, contractuelle, pénale et judiciaire applicables, que les Règles uniformes n'ont pas pour vocation de traiter.

D. Certitude supplémentaire quant aux effets juridiques des signatures électroniques

70. L'une des principales caractéristiques des Règles uniformes est de conférer davantage de certitude à l'application des critères souples énoncés à l'article 7 de la Loi type s'agissant de la reconnaissance d'une signature électronique comme équivalent fonctionnel d'une signature manuscrite.

L'article 7 de la Loi type est rédigé 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 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 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.

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.

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

71. L'article 7 se fonde sur la reconnaissance des fonctions remplies par la signature dans les échanges sur papier. Lors de l'élaboration de la Loi type, les fonctions ci-après d'une signature ont été envisagées: identifier une personne; apporter la certitude de la participation personnelle de cette personne à l'acte de signer; associer cette personne à la teneur d'un document. On a noté que la signature pouvait en outre remplir diverses autres fonctions, selon la nature du document. Par exemple, elle pouvait attester l'intention d'une partie d'être liée par le contrat qu'elle avait signé; l'intention d'une personne de revendiquer la paternité d'un texte; l'intention d'une personne de s'associer à la teneur d'un document écrit par quelqu'un d'autre; le fait qu'une personne s'était rendue en un lieu donné, à une heure donnée.

72. Afin de garantir qu'un message devant être authentifié ne puisse se voir refuser valeur juridique du simple fait qu'il n'a pas été authentifié de la manière voulue pour les documents sur papier, une formule générale a été retenue pour l'article 7. Cet article définit les conditions générales dans lesquelles les messages de données seraient réputés authentifiés avec suffisamment de crédibilité et seraient opposables au vu des exigences en matière de signature entravant actuellement le commerce électronique. L'article 7 s'attache aux deux fonctions essentielles d'une signature, à savoir l'identification de l'auteur d'un document et la confirmation que l'auteur approuve la teneur dudit document. Le paragraphe 1 a) énonce le principe selon lequel, pour les messages électroniques, les fonctions juridiques essentielles d'une signature sont respectées par une méthode qui permet d'identifier l'expéditeur d'un message de données et de confirmer que l'expéditeur approuve la teneur de ce message de données.

73. Le paragraphe 1 b) institue une approche souple en ce qui concerne le degré de fiabilité que doit garantir la méthode d'identification utilisée au paragraphe 1 a). La méthode utilisée en vertu du paragraphe 1 a) devrait être aussi fiable que cela est approprié au vu de l'objet pour lequel le message de données a été créé ou communiqué, compte tenu de toutes les circonstances, y compris tout accord entre l'expéditeur et le destinataire du message de données.

74. Pour déterminer si la méthode utilisée en vertu du paragraphe 1 est appropriée, les facteurs juridiques, techniques et commerciaux à prendre en considération sont les suivants: 1) le degré de perfectionnement du matériel utilisé par chacune des parties; 2) la nature de leur activité commerciale; 3) la fréquence avec laquelle elles effectuent entre elles des opérations commerciales; 4) la nature et l'ampleur de l'opération; 5) le statut et la fonction de la signature dans un régime législatif et réglementaire donné; 6) la capacité des systèmes de communication; 7) les procédures d'authentification proposées par les opérateurs des systèmes de communication; 8) la série de procédures d'authentification communiquée par un intermédiaire; 9) l'observation des coutumes et pratiques commerciales; 10) l'existence de mécanismes d'assurance contre les messages non autorisés; 11) l'importance et la valeur de l'information contenue dans le message de données; 12) la disponibilité d'autres méthodes d'identification et le coût de leur mise en œuvre; 13) le degré d'acceptation ou de non-acceptation de la méthode d'identification dans le secteur ou domaine pertinent, tant au moment où la méthode a été convenue qu'à celui où le message de données a été communiqué; et 14) tout autre facteur pertinent

(Guide pour l'incorporation de la Loi type de la CNUDCI sur le commerce électronique, par. 53 et 56 à 58).

75. S'appuyant sur l'exigence souple exprimée à l'article 7-1 b) de la Loi type, les articles 6 et 7 des Règles uniformes établissent un mécanisme par lequel les signatures électroniques qui satisfont à des critères objectifs de fiabilité technique peuvent bénéficier d'une détermination rapide quant à leur production d'effets juridiques. Les Règles uniformes ont pour effet de reconnaître deux catégories de signatures électroniques. La première catégorie, qui est la plus vaste, est celle décrite à l'article 7 de la Loi type. Elle comprend toute "méthode" pouvant être utilisée pour satisfaire à une exigence légale de signature manuscrite. Les effets juridiques d'une telle "méthode" comme équivalent d'une signature manuscrite dépend de la démonstration de sa fiabilité à un juge des faits. La seconde catégorie, plus étroite, est celle créée par les Règles uniformes. Elle comprend des méthodes de signature électronique qui peuvent être reconnues par une autorité publique, une entité privée accréditée, ou les parties elles-mêmes comme satisfaisant aux exigences de fiabilité technique énoncées dans les Règles uniformes. L'avantage d'une telle reconnaissance est qu'elle apporte aux utilisateurs de ces méthodes de signature électronique (parfois appelées "renforcées", "sécurisées" ou "qualifiées") une certitude avant que ceux-ci n'utilisent effectivement lesdites techniques.

E. Règles fondamentales de conduite applicables aux parties concernées

76. Les Règles uniformes ne traitent pas en détail des questions de responsabilité qui peuvent intéresser les différentes parties prenant part au fonctionnement de systèmes de signature électronique. Ces questions relèvent de la loi applicable en dehors des Règles uniformes. Cependant, les Règles uniformes fixent des critères permettant d'évaluer la conduite desdites parties, c'est-à-dire le signataire, la partie se fiant à la signature et le prestataire de services de certification.

77. Quant au signataire, les Règles uniformes partent du principe de base qu'il doit prendre des dispositions raisonnables à l'égard de son dispositif de signature électronique. Le signataire doit normalement prendre des dispositions raisonnables pour éviter toute utilisation non autorisée de ce dispositif. Lorsque le signataire sait ou aurait dû savoir que le dispositif de signature a été compromis, il doit en informer sans tarder toute personne dont on peut raisonnablement penser qu'elle se fiera à la signature électronique ou offrira des services étayant cette signature. Lorsqu'un certificat est utilisé pour étayer la signature électronique, le signataire doit prendre des dispositions raisonnables pour garantir l'exactitude et l'exhaustivité de toutes les déclarations essentielles faites par lui en rapport avec le certificat.

78. Une partie se fiant à la signature doit prendre des mesures raisonnables pour vérifier la fiabilité d'une signature électronique. Lorsque la signature électronique est étayée par un certificat, la partie se fiant à la signature doit prendre des mesures raisonnables pour vérifier la validité, la suspension ou la révocation du certificat, et tenir compte de toute restriction concernant le certificat.

79. Il incombe, en règle générale, à un prestataire de services de certification d'utiliser des systèmes, des procédures et des ressources humaines fiables, et d'agir en conformité avec les déclarations qu'il fait s'agissant de sa politique et de ses pratiques. En outre, le prestataire de services de certification doit prendre des dispositions raisonnables pour garantir l'exactitude et l'exhaustivité de toutes les déclarations essentielles faites par lui en rapport avec le certificat. Dans le certificat, le prestataire doit fournir des renseignements essentiels permettant à la partie se fiant à la signature d'identifier le prestataire. Il doit également déclarer: 1) que la personne qui est identifiée dans le

certificat contrôlait le dispositif de signature au moment de la signature; et 2) que le dispositif de signature était opérationnel à la date ou avant la date à laquelle le certificat a été émis. Lorsqu'il traite avec la partie se fiant à la signature, le prestataire de services de certification doit fournir des renseignements supplémentaires concernant: 1) la méthode utilisée pour identifier le signataire; 2) toute restriction apportée à l'objet ou à la valeur pour lequel ou laquelle le dispositif de signature ou le certificat peut être utilisé; 3) l'état opérationnel du dispositif de signature; 4) toute restriction apportée au champ d'application ou à la portée de la responsabilité du prestataire de services de certification; 5) le fait de savoir si le signataire a ou non les moyens de notifier qu'un dispositif de signature a été compromis; et 6) le fait de savoir si un service de révocation rapide est offert ou non.

80. Pour faciliter l'évaluation de la fiabilité des systèmes, des procédures et des ressources humaines utilisés par le prestataire de services de certification, les Règles uniformes fournissent une liste non exhaustive de facteurs indicatifs.

F. Un cadre neutre quant aux techniques employées

81. Compte tenu de la rapidité des progrès techniques, les Règles uniformes prévoient la reconnaissance juridique des signatures électroniques quelles que soient les techniques employées (signatures numériques recourant à la cryptographie asymétrique ou biométrie, par exemple).

V. ASSISTANCE OFFERTE PAR LE SECRÉTARIAT DE LA CNUDCI

A. Aide à l'élaboration d'une législation

82. Dans le cadre de ses activités de formation et d'assistance, le secrétariat de la CNUDCI aide les États, par des consultations techniques, à élaborer une législation sur la base des Règles uniformes de la CNUDCI sur les signatures électroniques. La même assistance est offerte aux États qui envisagent d'adopter une législation fondée sur d'autres lois types de la CNUDCI, ou qui envisagent d'adhérer à l'une des conventions sur le droit commercial international élaborées par la CNUDCI.

83. Pour tout renseignement complémentaire concernant les Règles uniformes et les autres lois types et conventions élaborées par la CNUDCI, on peut s'adresser au secrétariat à l'adresse suivante:

Service du droit commercial international, Bureau des affaires juridiques
Organisation des Nations Unies
Centre international de Vienne
B.P. 500
A-1400 Vienne (Autriche)

Téléphone: (+43-1) 26060-4060 ou 4061
Télécopie: (+43-1) 26060-5813
Adresse électronique: uncitral@uncitral.org
Site Internet: http://www.uncitral.org

B. Renseignements sur l'interprétation des textes législatifs fondés sur les Règles uniformes

84. Le secrétariat souhaiterait recevoir toute observation concernant les Règles uniformes et le Guide, ainsi que des renseignements concernant l'incorporation des textes législatifs

fondés sur les Règles uniformes. Une fois incorporées, les Règles uniformes seront incluses dans le système d'information sur la jurisprudence relative aux instruments de la CNUDCI, qui rassemble et diffuse des informations sur la jurisprudence relative aux conventions et lois types émanant de la CNUDCI. Ce système a pour objet de faire connaître au niveau international les textes législatifs élaborés par la CNUDCI et de faciliter leur interprétation et leur application uniformes. Le secrétariat publie, dans les six langues officielles de l'Organisation des Nations Unies, des résumés de décisions et met à disposition, contre remboursement des frais de reproduction, les décisions à partir desquelles les résumés ont été établis. Le système est expliqué dans un guide de l'utilisateur disponible auprès du secrétariat sous forme imprimée (A/CN.9/SER.C/GUIDE/1) ainsi que sur le site Internet susmentionné.

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] A/CN.9/467, par. 18 à 20.

[4] *Documents officiels de l'Assemblée générale, cinquante-deuxième session, Supplément n° 17* (A/55/17), par. 380 à 383.

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

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

[7] Ibid., *cinquante-troisième session, Supplément n° 17* (A/53/17), par. 207 à 211.

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

[9] Ibid., *cinquante-cinquième session, Supplément n° 17* (A/55/17), par. 380 à 383.

[10] Cette section est reprise du document A/CN.9/WG.IV/WP.71, partie I.

[11] De nombreux éléments de la description du fonctionnement d'un système de signature numérique dans la présente section s'appuient sur les directives en matière de signature numérique (Digital Signature Guidelines) élaborées par l'American Bar Association, p. 8 à 17.

[12] Certaines normes existantes telles que les directives concernant les signatures électroniques de l'Association du barreau américain contiennent la notion d'"irréalisabilité informatique" pour décrire l'irréversibilité escomptée du processus, c'est-à-dire l'espoir qu'il sera impossible de déduire la clef privée secrète d'un utilisateur à partir de sa clef publique. "Irréalisable par des moyens informatiques" est un concept relatif fondé sur la valeur des données protégées, l'infrastructure informatique requise pour les protéger, le temps nécessaire pour les protéger, ainsi que le coût et le temps nécessaires pour attaquer les données, ces facteurs étant évalués tant en fonction de la situation actuelle que des futurs progrès technologiques" (directives concernant les signatures électroniques de l'Association du barreau américain, p. 9, note 23).

[13] Dans des situations où les clefs cryptographiques publiques et privées seraient émises par les utilisateurs eux-mêmes, cette confiance pourrait devoir être conférée par les certificateurs de clefs publiques.

[14] La question de savoir si un gouvernement devrait avoir la capacité technique de conserver ou de recréer des clefs de confidentialité privées pourra être traitée au niveau de l'autorité centrale.

[15] Dans le contexte d'une certification croisée, cependant, il faudrait, pour assurer une compatibilité internationale, que toutes les infrastructures à clef publique établies dans différents pays puissent communiquer entre elles.