NATIONS UNIES **A**

Assemblée générale

Distr. GÉNÉRALE
A/CN.9/446
10 février 1998

FRANÇAIS
Original : ANGLAIS

COMMISSION DES NATIONS UNIES
POUR LE DROIT COMMERCIAL INTERNATIONAL
Trente et unième session
New York, 1er-12 juin 1998

RAPPORT DU GROUPE DE TRAVAIL SUR LE COMMERCE ÉLECTRONIQUE
SUR LES TRAVAUX DE SA TRENTE-DEUXIÈME SESSION
(Vienne, 19-30 janvier 1998)

TABLE DES MATIÈRES

V.98-50892

TABLE DES MATIÈRES (suite)

INTRODUCTION

1. À sa vingt-neuvième session (1996), la Commission a décidé d'inscrire à son ordre du jour les questions relatives aux signatures numériques et aux autorités de certification. Le Groupe de travail sur le commerce électronique a été prié de réfléchir à l'opportunité de définir des règles uniformes concernant ces questions. Il a été convenu qu'à l'occasion des travaux de sa trente et unième session, le Groupe de travail pourrait entreprendre d'élaborer des projets de règles touchant certains aspects des questions susmentionnées. La Commission a prié le Groupe de travail de lui fournir des éléments d'information qui lui permettent de se prononcer en toute connaissance de cause sur le champ d'application des règles uniformes devant être élaborées. Il a été également convenu, s'agissant de donner un mandat plus précis au Groupe de travail, que les règles uniformes devant être élaborées devraient être consacrées notamment aux questions ci-après : fondement juridique des opérations de certification, y compris les nouvelles techniques d'authentification et de certification numériques; applicabilité de la certification; répartition des risques et des responsabilités entre utilisateurs, fournisseurs et tiers dans le contexte de l'utilisation de techniques de certification; questions spécifiques à la certification sous l'angle de l'utilisation des registres; et incorporation par référence[1].

2. À sa trentième session (1997), la Commission a été saisie du rapport du Groupe de travail sur les travaux de sa trente et unième session (A/CN.9/437). S'agissant de l'opportunité et de la faisabilité de l'élaboration de règles uniformes sur les questions des signatures numériques et des autorités de certification, le Groupe de travail a indiqué à la Commission qu'il était parvenu à un consensus quant à l'importance et à la nécessité de travailler à l'harmonisation du droit dans ce domaine. Bien que n'ayant pas pris de décision ferme sur la forme et la teneur de ces travaux, il était arrivé à la conclusion préliminaire qu'il était possible d'entreprendre l'élaboration d'un projet de règles uniformes, du moins sur les questions concernant les signatures numériques et les autorités de certification et peut-être sur des questions connexes. Le Groupe de travail a rappelé que dans le cadre des travaux futurs dans le domaine du commerce électronique, il pourrait être nécessaire de traiter, outre les questions relatives aux signatures numériques et aux autorités de certification, les sujets suivants : techniques autres que la cryptographie à clef publique; questions générales concernant les fonctions exercées par les tiers fournisseurs de services et contrats électroniques (A/CN.9/437, par. 156 et 157). En ce qui concerne la question de l'incorporation par référence, le Groupe de travail a conclu que le secrétariat n'avait pas besoin d'entreprendre de nouvelle étude car les problèmes fondamentaux étaient bien connus et il était clair que nombre d'aspects du conflit de formulaires et des contrats d'adhésion devraient être traités dans les dispositions législatives nationales applicables en raison, par exemple, de la protection du consommateur et d'autres considérations d'intérêt général. De l'avis du Groupe de travail cette question devrait être la première des questions de fond qu'il examinerait à sa prochaine session (A/CN.9/437, par. 155).

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

4. S'agissant du champ d'application et de la forme exacts de ces Règles uniformes, la Commission est généralement convenue qu'aucune décision ne pouvait être prise à ce stade précoce. On a estimé qu'il était justifié que le Groupe de travail axe son attention sur les questions relatives aux signatures numériques étant donné le rôle apparemment prédominant joué par la cryptographie à clef publique dans la nouvelle pratique du commerce électronique, mais les Règles uniformes devraient être compatibles avec l'approche techniquement neutre adoptée dans la Loi type de la CNUDCI sur le commerce électronique (dénommée ci-après "la Loi type"). Ainsi, les Règles uniformes ne devraient pas décourager l'utilisation d'autres techniques d'authentification. En outre, s'agissant de la cryptographie à clef publique, il pourrait être nécessaire que les Règles uniformes prennent en considération divers niveaux de sécurité et reconnaissent les divers effets juridiques et niveaux de responsabilité correspondant aux différents types de services fournis dans le contexte des signatures numériques. S'agissant des autorités de

certification, la Commission a certes reconnu la valeur des normes issues du marché mais il a été 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 transnationale.

5. On a en outre émis l'avis que dans le cadre des travaux futurs relatifs au commerce électronique, le Groupe de travail pourrait être amené, à un stade ultérieur, à examiner les questions de la compétence, des lois applicables et du règlement des litiges sur l'Internet[2].

6. Le Groupe de travail sur le commerce électronique, qui est composé de tous les États membres de la Commission, a tenu sa trente-deuxième session à Vienne du 19 au 30 janvier 1998. Ont assisté à cette session les représentants des États membres du Groupe de travail ci-après : Algérie, Allemagne, Australie, Autriche, Brésil, Bulgarie, Chine, Égypte, Espagne, États-Unis d'Amérique, Fédération de Russie, Finlande, France, Hongrie, Inde, Iran (République islamique d'), Italie, Japon, Mexique, Nigéria, Pologne, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, Singapour, Slovaquie, Soudan et Thaïlande.

7. Y ont également assisté les observateurs des États ci-après : : Angola, Bélarus, Bosnie-Herzégovine, Canada, Colombie, Costa Rica, Danemark, Grèce, Guatemala, Indonésie, Iraq, Irlande, Koweït, Liban, Malaisie, Maroc, Pays-Bas, Pakistan, Paraguay, République de Corée, République tchèque, Suède, Suisse, Turquie et Ukraine.

8. Y ont en outre assisté les organisations internationales ci-après : Centre du commerce international CNUCED/OMC, Conférence des Nations Unies sur le commerce et le développement (CNUCED), Organisation des Nations Unies pour l'éducation, la science et la culture (UNESCO), Organisation des Nations Unies pour le développement industriel (ONUDI), Organisation mondiale de la propriété intellectuelle (OMPI), Commission européenne, Organisation de coopération et de développement économiques (OCDE), Organisation mondiale du commerce (OMC), Centre régional du Caire pour l'arbitrage commercial international, Comité maritime international (CMI), Association internationale des ports (AIP), Association internationale du barreau, Chambre de commerce internationale (CCI), Internet Law and Policy Forum (ILPF) et Association européenne des étudiants en droit.

9. Le Groupe de travail a élu le bureau ci-après :

Président :	M. Mads Bryde ANDERSEN (Danemark);
Vice-Président :	M. PANG Khang Chau (Singapour);
Rapporteur :	M. Gritsana CHANGGOM (Thaïlande).

10. Le Groupe de travail était saisi des documents ci-après : ordre du jour provisoire (A/CN.9/WG.IV/WP.72); une note établie par le secrétariat pour la trente et unième session du Groupe de travail intitulée "Planification des travaux à venir en matière de commerce électronique : signatures numériques, tiers authentificateurs et questions juridiques connexes" (A/CN.9/WG.IV/WP.71), résumant les débats antérieurs du Groupe de travail sur la question de l'incorporation par référence; une note reproduisant le texte d'un projet de disposition sur l'incorporation par référence et des notes explicatives présentées par le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord (A/CN.9/WG.IV/WP.74); et une note du secrétariat renfermant un projet de règles uniformes sur les signatures numériques, les autres signatures électroniques, les tiers authentificateurs et les questions juridiques connexes (A/CN.9/WG.IV/WP.73).

11. Le Groupe de travail a adopté l'ordre du jour ci-après :

1. Élection du bureau.

2. Adoption de l'ordre du jour.

3. Aspects juridiques du commerce électronique : incorporation par référence.

4. Aspects juridiques du commerce électronique : projet de règles uniformes sur les signatures numériques, les autres signatures électroniques, les autorités de certification et les questions juridiques connexes.

5. Questions diverses.

6. Adoption du rapport.

I. DÉBATS ET DÉCISIONS

12. Le Groupe de travail a examiné la question de l'incorporation par référence en se fondant sur la note établie par le secrétariat (A/CN.9/WG.IV/WP.71) et la proposition présentée par le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord (A/CN.9/WG.IV/WP.74). Il est rendu compte des débats et des conclusions du Groupe de travail à ce sujet dans la section II ci-dessous. Après examen, le Groupe de travail a adopté le texte d'un projet d'article sur l'incorporation par référence. Le secrétariat a été prié d'élaborer, à partir des délibérations et décisions du Groupe de travail, un bref guide pour aider les États à incorporer et à appliquer le projet d'article. Il a été noté que le projet d'article ainsi que le guide pour son incorporation seraient soumis à la Commission à sa trente et unième session, prévue à New York du 1er au 12 juin 1998, pour faire l'objet d'un examen final et éventuellement être insérés dans la Loi type et le Guide pour son incorporation.

13. Le Groupe de travail a également examiné, en se fondant sur la note établie par le secrétariat (A/CN.9/WG.IV/WP.73), les questions suivantes : signatures numériques, autres signatures électroniques, autorités de certification et questions juridiques connexes. Il est rendu compte des délibérations et des conclusions du Groupe de travail à ce sujet dans la section III ci-dessous. Le secrétariat a été prié d'établir, à partir de ces délibérations et conclusions, un ensemble de dispositions révisées, avec d'éventuelles variantes, pour examen par le Groupe de travail lors d'une future session.

II. INCORPORATION PAR RÉFÉRENCE

14. Après un rappel des débats consacrés à la question de l'incorporation par référence et aux projets de textes proposés à ses précédentes sessions (A/CN.9/WG.IV/WP.71, par. 77 à 93), le Groupe de travail a été invité à examiner cette question en milieu électronique, à partir d'un projet de disposition proposé (A/CN.9/WG.IV/WP.74, annexe), libellé comme suit :

"1. Le présent article s'applique lorsqu'un message de données comporte une référence à des informations figurant ailleurs, ou lorsque son sens ne peut être pleinement déterminé que par référence à de telles informations (les "informations complémentaires").

2. Sous réserve des dispositions du paragraphe 5, le message de données a les mêmes effets que si les informations complémentaires étaient pleinement formulées dans ledit message. Toute référence au message de données constitue une référence audit message incluant toutes les informations complémentaires, si les conditions énoncées au paragraphe 3 sont remplies.

3. Les conditions visées au paragraphe 2 sont les suivantes. Le message de données :

a) identifie les informations complémentaires

i) par un nom collectif, une description ou un code; et

ii) en spécifiant comme il convient le document et les parties du document contenant les informations complémentaires et, lorsque ce document n'est pas disponible au public, le lieu où il peut-être trouvé et, lorsque le moyen d'accès n'est pas évident ou est limité de quelque manière que ce soit, la manière dont il peut-être trouvé; et

b) indique expressément ou permet de déduire clairement qu'il doit avoir les mêmes effets que si les informations complémentaires y étaient intégralement formulées.

4. L'identification mentionnée à l'alinéa a) du paragraphe 3 peut être effectuée indirectement, par référence à des informations figurant dans un autre document comportant l'identification requise, étant entendu que les conditions énoncées au paragraphe 3 doivent être remplies pour ce qui est de ladite référence.

5. Aucune disposition du présent article n'a d'incidences sur :

a) toute règle de droit exigeant qu'une notification appropriée soit donnée concernant la teneur des informations complémentaires, le document ou le lieu où se trouvent ces informations, ou le moyen d'accéder à ces informations, ou exigeant que ce lieu ou ce document soit accessible à une autre personne; ou

b) toute règle de droit relative à la validité des conditions aux fins de la formation des contrats, y compris l'acceptation d'une offre.

c) toute règle de droit relative aux effets des informations complémentaires incorporées ou à la validité du processus d'incorporation."

15. On a fait observer que : le projet de disposition devrait s'appliquer lorsqu'un message de données utiliserait l'incorporation par référence (par. 1); le principe général en était que l'information incorporée (non désignée par le mot "conditions", dans la mesure où toutes les informations ne créaient pas une obligation) devrait avoir le même effet que si elle était pleinement exprimée dans un message de données (par. 2); les conditions générales régissant l'incorporation par référence devraient être les suivantes : une identification claire et précise de l'information incorporée (ce qui était particulièrement important pour la protection des consommateurs et d'autres tiers), l'identification de l'endroit où ces informations pouvaient être consultées et de la manière dont elles pouvaient être consultées et l'indication de l'intention d'incorporer (par. 3); l'identification indirecte de la source d'information par référence à une autre source devrait être acceptable dans les mêmes conditions (par. 4); et toute règle de droit existante, applicable à l'incorporation par référence dans les communications sur papier devrait également être applicable aux communications électroniques (par. 5).

16. Il a été généralement convenu que cette question devait être traitée, dans la mesure où l'incorporation par référence était inhérente à l'utilisation des communications électroniques. Il a été indiqué que, dans les communications électroniques, de grandes quantités de données étaient nécessairement incorporées par référence (par exemple, dossiers de communication, déclarations de principe, signatures numériques dans les certificats). En outre, on a fait observer que l'incorporation par référence dans un contexte électronique pouvait être assurée par diverses méthodes, notamment, mais non exclusivement, localisateurs de ressources uniformes (URL), identificateurs d'objets (OID) ou autres enregistrements raisonnablement accessibles à une adresse donnée.

17. S'il a été admis que l'incorporation par référence présentait certains risques, par exemple pour le consommateur, on a fait valoir que, parallèlement, une telle pratique permettait aux consommateurs de tirer parti des possibilités qu'offraient uniquement les réseaux de communications électroniques. On a signalé que le principal

objet d'une disposition sur l'incorporation par référence était d'établir un équilibre entre les parties intéressées. Afin d'atteindre cet objectif, le Groupe de travail a été invité à examiner, parallèlement au projet de disposition susmentionné, un projet de disposition libellé comme suit :

"Variante A Sauf convention contraire des parties, une information est considérée comme faisant partie d'un message de données, si cela est expressément indiqué ou clairement implicite [et si le message de données indique la procédure à suivre pour accéder à cette information de manière raisonnable et en temps utile]. Cette information produit ses effets dans la mesure autorisée par la loi.

Variante B L'information n'est pas privée de ses effets juridiques au seul motif qu'elle est incorporée par référence dans un message de données."

18. S'agissant de la variante A, on a fait observer que les facteurs matériels à prendre en compte pour déterminer si une condition était raisonnablement accessible étaient notamment les suivants : disponibilité (horaire de fonctionnement du registre, facilité d'accès et niveaux acceptables de redondance); coût de l'accès (à l'exclusion des coûts des services de communications correspondants; s'il y a un coût, celui-ci devrait être raisonnable et proportionné à la valeur du contrat); structure (structure largement utilisée dans le domaine en question); intégrité (vérification de la teneur, authentification de l'expéditeur et mécanisme de correction des erreurs de communication); mesure dans laquelle la condition peut faire l'objet de modifications ultérieures (en l'absence d'un droit contractuel en la matière; notification des mises à jour; notification de la politique en matière de modification). Ces facteurs, a-t-on ajouté, pourraient être énoncés dans un guide pour l'incorporation des dispositions sur l'incorporation par référence (voir par. 23 et 24 ci-après).

19. Le Groupe de travail a poursuivi son débat sur la base des autres dispositions proposées ci-dessus. On a fait observer que ces dispositions avaient un certain nombre d'avantages en commun. Un de ces avantages était qu'elles visaient à faciliter l'incorporation par référence dans un contexte électronique en dissipant, dans de nombreuses juridictions, les incertitudes liées à la question de savoir si les dispositions traitant de l'incorporation par référence classique étaient applicables à l'incorporation par référence en milieu électronique. À cet égard, on a proposé que soit adoptée une autre approche, selon laquelle une large utilisation de l'incorporation par référence serait découragée dans un environnement électronique, ce qui réduirait le risque de voir se reproduire les difficultés liées au "conflit de formulaires" propres aux échanges commerciaux traditionnels sur papier. À l'appui de cette proposition, on a fait observer que si, en milieu papier, l'incorporation par référence était nécessaire pour des raisons de temps, d'espace et de coût, en milieu électronique, une grande quantité de données pouvaient être exprimées dans un message de données simplement, en temps utile et de façon peu coûteuse. Cette proposition a été contestée au motif qu'il ne convenait pas qu'une loi uniforme joue le rôle d'un code de conduite, ce qui découragerait l'emploi d'une méthode importante largement appliquée, dont l'utilisation était inhérente aux communications électroniques.

20. Un autre avantage des propositions susmentionnées, a-t-on fait observer, était qu'elles reconnaissaient qu'il ne devait pas y avoir d'incidences sur une loi nationale ou internationale sur la protection des consommateurs ou autre de caractère obligatoire (par exemple, les règles protégeant des parties plus faibles dans le cas de contrats d'adhésion). On a fait remarquer que la première proposition avait pour objet d'atteindre ces objectifs en énumérant les règles de droit qui n'étaient pas visées (par. 5) et que la deuxième proposition aboutissait au même résultat, dans la mesure où il était indiqué que l'information produisait ses effets "dans la mesure autorisée par la loi" (variante A), ou que l'information n'était pas privée de ses effets juridiques au seul motif qu'elle était incorporée par référence (variante B). Afin de préciser très clairement que les lois en vigueur n'étaient visées par aucun des libellés proposés, il a été suggéré que toute disposition sur l'incorporation par référence soit libellée conformément à la deuxième note afférente à l'article premier de la Loi type, qui indiquait expressément que cette Loi ne se substituait à aucune règle de droit visant à protéger le consommateur.

21. Toutefois, selon un avis, la première proposition et la variante A de la deuxième proposition présentaient un certain nombre d'inconvénients. Notamment, elles risquaient de contrarier des pratiques bien établies ou nouvelles en fixant une norme trop stricte. On a signalé que, dans de nombreuses pratiques, il serait impossible de satisfaire à la condition selon laquelle les données visées dans un message de données devaient être expressément indiquées ou clairement implicites pour être incorporées dans ledit message. On a cité l'exemple de l'incorporation par référence d'une charte-partie principale dans un connaissement émis au titre d'une sous-charte-partie, pratique qui, a-t-on fait valoir, serait entravée s'il fallait que l'intention d'incorporer les informations par référence soit expressément indiquée ou clairement implicite ou que ces informations soient raisonnablement accessibles. Un autre inconvénient tenait au fait que ces dispositions risquaient involontairement de porter atteinte aux règles de droit impératives et d'entraîner des résultats inéquitables. À cet égard, on a fait observer, qu'outre les deux conditions énoncées dans la première proposition et dans la variante A de la deuxième proposition, il conviendrait d'inclure un troisième élément, à savoir que l'incorporation par référence devrait être soumise à l'acceptation des parties. En particulier, dans un milieu EDI ouvert, on a estimé que l'acceptation des parties était essentielle.

22. En réponse à ces observations, il a été indiqué que le paragraphe 5 de la première proposition et la deuxième phrase de la variante A de la deuxième proposition avaient pour objet de prendre en compte précisément ces préoccupations et de faire en sorte que les dispositions sur l'incorporation par référence n'aillent pas à l'encontre des pratiques établies ou des règles impératives du droit national. Toutefois, on a estimé que ces dispositions pourraient soulever des questions d'interprétation. La variante B, a-t-on fait observer, ne présentait pas cet inconvénient, en ce sens qu'elle exprimait simplement le principe général de la non-discrimination énoncé à l'article 5 de la Loi type. Elle impliquait, a-t-on généralement reconnu, que l'incorporation par référence produirait uniquement les effets autorisés par la loi. Pour cette raison, le Groupe de travail est généralement convenu qu'elle était préférable.

23. D'un point de vue rédactionnel, il a été proposé que le libellé de la variante B soit aligné sur celui de l'article 5 de la Loi type et fasse référence, non seulement aux effets juridiques, mais aussi à la validité et à la force exécutoire. S'agissant de l'emplacement de la disposition sur l'incorporation par référence, il a été proposé que, compte tenu du fait que cette question concernait le commerce électronique en général et pas seulement les signatures numériques, elle soit insérée dans la Loi type en tant qu'article 5 *bis*. Pour aider les utilisateurs de la Loi type et les législateurs à interpréter la disposition sur l'incorporation par référence, il a également été proposé que des remarques générales et des informations explicatives concernant cette disposition soient incluses dans le Guide pour l'incorporation de la Loi type. On a fait observer que ce guide pourrait indiquer les facteurs à partir desquels les États pourraient vouloir adopter une version élargie de la disposition sur l'incorporation par référence. Ces facteurs pourraient s'inspirer du texte de la première proposition et de la variante A de la deuxième proposition. En général, cette proposition a été jugée acceptable, mais on a mis en garde contre le fait qu'une telle approche pourrait être incompatible avec l'approche adoptée à l'article 5 de la Loi type. Selon une opinion, les facteurs susmentionnés ne devraient pas être présentés comme des dispositions pouvant se substituer à celles de la Loi type. En général, on a estimé que, dans la rédaction de la partie du Guide traitant de l'incorporation par référence, il faudrait veiller à éviter de donner involontairement à entendre que des restrictions à l'incorporation par référence devraient être adoptées pour le commerce électronique, en plus de celles qui pourraient déjà s'appliquer aux échanges commerciaux sur papier.

24. Après un débat, le Groupe de travail a adopté la variante B, décidé qu'elle devrait être présentée à la Commission pour examen et éventuellement pour incorporation dans la Loi type en tant qu'article 5 *bis* et prié le secrétariat d'établir une note explicative à ajouter au Guide pour l'incorporation de la Loi type.

III. EXAMEN DU PROJET DE RÈGLES UNIFORMES SUR LES SIGNATURES ÉLECTRONIQUES

CHAPITRE PREMIER. CHAMP D'APPLICATION ET DISPOSITIONS GÉNÉRALES

25. Le Groupe de travail est convenu que la relation entre les Règles uniformes et la Loi type (notamment la question de savoir si les Règles uniformes sur les signatures numériques devraient constituer un instrument juridique distinct ou être incorporées dans une version élargie de la Loi type) devrait être clarifiée ultérieurement. S'il a été convenu qu'aucune décision ne pouvait être prise à ce stade, le Groupe de travail a cependant confirmé son hypothèse de travail, à savoir que les Règles uniformes devraient être préparées sous la forme de projets de disposition législatives, être compatibles avec les dispositions de la Loi type en général et d'une manière ou d'une autre incorporer des dispositions s'inspirant des articles premier (Champ d'application), 2 a), c) et e) (Définition des termes "message de données", "expéditeur" et "destinataire"), 3 (Interprétation) et 7 (Signature) de la Loi type.

26. Pour ce qui est du champ d'application des Règles uniformes, il a été jugé que celui-ci devrait être limité aux signatures numériques, à l'exclusion d'autres techniques d'authentification. Il a été rappelé, en réponse à cet avis, que, lorsqu'il avait conclu à titre préliminaire qu'il était possible d'entreprendre l'élaboration d'un projet de Règles uniformes sur les signatures numériques, le Groupe de travail, à sa session précédente, était également convenu qu'outre les signatures numériques et les autorités de certification, les travaux dans le domaine du commerce électronique devraient peut-être traiter aussi les questions touchant les techniques autres que la cryptographie à clef publique (A/CN.9/437, par. 156 et 157). Il a également été rappelé qu'à la trentième session de la Commission, il avait été jugé que, s'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, les Règles uniformes devraient cependant être compatibles avec l'approche techniquement neutre adoptée dans la Loi type de la CNUDCI sur le commerce électronique (voir ci-dessus, par. 4). Après un débat, le Groupe de travail a confirmé sa décision, à savoir que, tout en axant ses travaux sur l'élaboration de dispositions particulières traitant des techniques de signature numérique, il devrait également tirer de ces dispositions particulières des règles d'application plus générale applicables à d'autres techniques d'authentification.

CHAPITRE II. SIGNATURES ÉLECTRONIQUES

Section I. Signatures électroniques sécurisées

Article premier. Définitions

27. Le texte du projet d'article premier examiné par le Groupe de travail était le suivant :

"Aux fins des présentes Règles,

a) Le terme "signature" désigne tout symbole employé, ou toute autre procédure de sécurité adoptée par une personne [ou en son nom] en vue d'identifier cette personne et d'indiquer qu'elle approuve les renseignements sur lesquels la signature est apposée;

b) Les termes "signature électronique" désignent [une signature] [des données] sous forme électronique contenue(s) dans un message de données, ou jointes ou logiquement associées audit message [et utilisée(s) par une personne [ou en son nom] en vue d'identifier cette personne et d'indiquer qu'elle approuve la teneur du message de données] [et utilisée(s) pour satisfaire aux conditions énoncées à [l'article 7 de la Loi type de la CNUDCI sur le commerce électronique]];

c) Les termes “signature électronique sécurisée” désignent une signature électronique qui

i) est une signature numérique au sens de l’article 4 et satisfait aux conditions énoncées à l’article 5; ou

ii) peut, à partir du moment où elle apposée, être authentifiée comme celle d’une personne particulière à l’aide d’une procédure de sécurité qui est liée exclusivement à la personne qui l’utilise; susceptible d’identifier rapidement, objectivement et automatiquement cette personne; créée d’une manière ou à l’aide d’un moyen dont seule la personne l’utilisant a le contrôle; et liée au message de données auquel elle se rapporte d’une manière qui permette de l’invalider si le message est altéré; ou

iii) [pour ce qui est de la relation entre les parties participant à la création, l’envoi, la réception, la conservation ou le traitement de toute autre manière des messages de données dans la conduite ordinaire de leurs affaires,] est commercialement raisonnable compte tenu des circonstances, a été convenue au préalable et a été correctement appliquée par les parties.

Remarque générale

28. Il a été noté que les dispositions énoncées dans le projet d’article premier n’étaient pas conçues seulement comme des définitions, mais également comme un moyen de délimiter le champ d’application des Règles uniformes. La même technique de rédaction avait été retenue dans le contexte de la Loi type, mais il a été jugé dans l’ensemble que le projet d’article premier devrait sans doute être réexaminé par le Groupe de travail durant son examen du champ d’application des Règles uniformes.

Alinéa a)

29. Il a été jugé dans l’ensemble qu’il faudrait supprimer l’alinéa a). S’il pouvait être utile, pour les pays dans lesquels il n’y avait actuellement pas de définition du terme “signature”, d’inclure dans les Règles uniformes une définition de la “signature” fondée sur l’article 7 de la Loi type, il a été déclaré néanmoins qu’une telle définition n’était pas nécessaire aux fins des Règles uniformes. Une des raisons avancées pour sa suppression a été qu’une définition risquerait de mettre en danger l’acceptabilité de l’instrument dans les pays où la disposition énoncée à cet alinéa pourrait être incompatible avec les définitions en vigueur.

Alinéa b)

30. Il a été jugé dans l’ensemble que le libellé de l’alinéa b) devrait refléter le texte de l’article 7 de la Loi type. À cette fin, on pourrait, soit reproduire intégralement cet article à l’alinéa b), soit faire référence aux “conditions énoncées à l’article 7 de la Loi type”. Après un débat, le Groupe de travail a jugé préférable la seconde solution. Pour ce qui est de la forme, il a été convenu que les mots “des données” devraient être utilisés, plutôt que les mots “une signature”.

Alinéa c) : Remarques générales

31. Selon un avis, il ne serait pas approprié de définir une signature électronique comme “sécurisée”. Le fait qu’une technique donnée soit sécurisée ou non ne relevait pas d’une définition, mais était une question de fait à déterminer compte tenu des circonstances dans lesquelles la technique était utilisée. On a également critiqué l’utilisation du mot “sécurisée” au motif qu’elle introduisait un critère subjectif et qu’elle laissait entendre que les signatures n’entrant pas dans cette catégorie étaient intrinsèquement non sûres. Il a été répondu que la référence à une signature “sécurisée” devrait peut-être être remplacée par un libellé plus approprié, mais qu’elle n’avait été

utilisée dans les Règles uniformes que pour délimiter une catégorie de signatures électroniques d'une qualité telle que des effets juridiques particuliers pouvaient y être attachés. Pour ce qui est du point de savoir si l'utilisation du mot "sécurisée" constituait un critère subjectif, il a été déclaré que les techniques d'authentification n'étaient pas conçues dans le vide. Des normes mises en œuvre soit par réglementation, soit par le biais de pratiques volontaires issues de l'industrie, seraient disponibles pour déterminer le degré de sécurité d'une technique donnée. Après un débat, le Groupe de travail a décidé de partir de l'hypothèse qu'une catégorie (provisoirement désignée comme "sécurisée") serait utilisée pour traiter de la gamme des techniques auxquelles les Règles uniformes associeraient certains effets juridiques.

32. Selon un avis, il ne serait peut-être pas approprié de disposer que les mêmes effets juridiques seraient associés à une large gamme de techniques d'authentification qui, a-t-on-dit, allaient de techniques intrinsèquement sûres (par exemple, la signature numérique) à des techniques intrinsèquement peu sûres (par exemple, certaines techniques d'authentification pouvant être convenues par les parties). Il a été répondu que l'alinéa c) avait précisément pour objet de créer une catégorie dans laquelle les plus sûres des signatures numériques pourraient être mises sur un pied d'égalité avec d'autres techniques, à condition que ces techniques satisfassent à la norme sévère énoncée au sous-alinéa ii) de l'alinéa c). Pour ce qui est du sous-alinéa iii) de l'alinéa c), on pourrait envisager de le placer dans une disposition distincte traitant de l'autonomie des parties. Il a été convenu qu'il faudrait sans doute rouvrir le débat sur les définitions après qu'auraient été examinées les dispositions relatives aux effets juridiques de ces définitions.

Sous-alinéa c) i)

33. Le sous-alinéa c) i) a été jugé dans l'ensemble acceptable quant au fond. Toutefois, selon un avis, les conditions énoncées à l'article 5, auquel il était fait référence à l'alinéa c) i) ne garantissaient pas suffisamment que la qualité des signatures numériques en faisait des signatures électroniques sécurisées. Il a été proposé de réexaminer la question dans le cadre de l'article 5.

Sous-alinéa c) ii)

34. On a craint que la charge de la preuve en vertu du sous-alinéa c) ii) ne soit si lourde que les présomptions énoncées dans le projet d'article 2-1 auraient peu de sens dans le cas où seraient utilisées des signatures électroniques non numériques. Il a été répondu que le sous-alinéa c) ii) et le projet d'article 2 avaient été conçus à des fins différentes. Il a toutefois été convenu qu'il faudrait sans doute préciser la relation entre le sous-alinéa c) ii) et le projet d'article 2 dans le projet révisé de Règles uniformes qu'élaborerait le secrétariat.

35. Il a été jugé dans l'ensemble que la teneur du sous-alinéa c) ii) était importante, afin de garantir la neutralité quant aux techniques utilisées dans les Règles uniformes. Selon un avis, puisque le sous-alinéa c) ii) avait pour objet de définir certains critères auxquels devait satisfaire une technique donnée, afin de déclencher les présomptions énoncées dans le projet d'article 2, il n'était pas important de savoir si cette technique était utilisée ou non avec l'intention de signer. De ce fait, il a été proposé de supprimer les mots "peut être authentifiée comme celle d'une personne particulière".

36. D'autres suggestions ont été faites quant au libellé du sous-alinéa c) ii). Selon une suggestion, il faudrait supprimer les mots "rapidement" et "automatiquement". Il a été déclaré que l'identification "rapide" et "automatique" d'une personne n'était pas inhérente à la plupart des techniques d'authentification (y compris certaines techniques de signature numérique) et n'était pas clairement liée à la sécurité de la procédure d'authentification et à l'intégrité des données signées électroniquement. Selon une autre suggestion, il faudrait compléter les mots "d'une procédure de sécurité" par les mots "ou d'une combinaison de procédures de sécurité". Après un débat, ces suggestions ont été adoptées par le Groupe de travail.

Sous-alinéa c) iii)

37. Il a été proposé de supprimer le sous-alinéa iii). En effet, en accordant le statut de “signature électronique sécurisée” à toute procédure pouvant être convenue par les parties, le risque serait de permettre l’utilisation de toute procédure à faible sécurité pour produire des effets juridiques. À ce propos, on a estimé qu'actuellement, la seule technique d'authentification “sécurisée” était la signature numérique. Il a été répondu que, conformément au principe de la liberté contractuelle, les parties devraient être libres de convenir, entre elles, de se fier à une technique d'authentification moins sécurisée que le type de signature électronique décrit au sous-alinéa c) ii) et d'associer les présomptions énoncées dans le projet d'article 2 à l'utilisation de cette technique d'authentification. Il a également été noté que la référence au caractère raisonnable de la signature avait pour objet de protéger contre une reconnaissance illimitée de techniques d'authentification potentiellement peu sûres par le biais de l'autonomie des parties. On a toutefois mis en garde contre le recours à la notion du caractère “commercialement raisonnable” pour offrir une telle protection. Dans un certain nombre de pays, le simple fait que des parties “commerciales” aient convenu d'une procédure suffirait à interpréter cette procédure comme “commercialement raisonnable”. Pour ce qui est de la forme, il a été demandé s'il n'y avait pas incompatibilité entre l'utilisation des mots “commercialement raisonnable” et le libellé retenu à l'article 7 de la Loi type. Il a été rappelé que les mots “commercialement raisonnable” avaient été utilisés à l'article 5 de la Loi type de la CNUDCI sur les virements internationaux, mais le Groupe de travail a jugé qu'il faudrait peut-être retenir un libellé plus approprié afin d'éviter l’interprétation susmentionnée. Il a été avancé qu'une référence à une stipulation expresse des parties, selon laquelle la technique convenue produirait les effets d'une signature électronique sécurisée en vertu du projet d'article 2, devrait sans doute être incluse au sous-alinéa iii). Il a également été proposé de conserver dans le sous-alinéa iii) les mots “pour ce qui est de la relation entre les parties”, sans crochets.

38. Il a été demandé si le sous-alinéa iii) pourrait être utilisé par les parties pour écarter des règles de droit impératives concernant la forme de certains actes juridiques. Il a été déclaré que cette interprétation serait inacceptable, étant donné qu'une telle liberté contractuelle n'existait pas dans un environnement papier. S'il a été convenu qu'en vertu de la loi d'un certain nombre de pays, certaines conditions de forme impératives pouvaient être écartées par convention privée, de telles conditions impératives s'appliquaient en général à une catégorie très étroite d'opérations, qui pourraient probablement faire l'objet d'une exclusion expresse du champ d'application d'une disposition générale traitant de l'autonomie des parties.

39. Le Groupe de travail a ensuite étudié la manière dont l'autonomie des parties serait traitée dans les Règles uniformes. Il a été rappelé que la simple référence à l'article 4 (Dérogation conventionnelle) de la Loi type ne suffirait sans doute pas à offrir une solution satisfaisante, étant donné que l'article 4 établissait une distinction entre les dispositions de la Loi type pouvant être librement modifiées par convention et les dispositions devraient être considérées comme impératives, à moins qu'une dérogation conventionnelle ne soit autorisée par la loi applicable extérieurement à la Loi type. Pour ce qui est des signatures électroniques, l'importance pratique des réseaux “fermés” rendait nécessaire une large reconnaissance de l'autonomie des parties. Toutefois, les restrictions d'ordre public à la liberté contractuelle, y compris les lois protégeant les consommateurs contre des contrats d'adhésion excessifs, devraient sans doute également être prises en considération. Il a été proposé que les Règles uniformes comportent une disposition similaire à l’article 4-1 de la Loi type aux termes de laquelle, sauf disposition contraire des Règles uniformes ou de toute autre loi applicable, les signatures électroniques et les certificats qui étaient émis ou reçus, ou auxquels on se fiait conformément aux procédures convenues entre les parties à une opération se verraient accorder les effets spécifiés dans la convention. En outre, il a été proposé que le Groupe de travail envisage d’énoncer une règle d’interprétation, aux termes de laquelle, pour déterminer si un certificat, une signature électronique ou un message de données confirmé par référence à un certificat étaient suffisamment fiables à une fin particulière, toutes les conventions pertinentes entre les parties, tout comportement des parties et tout usage commercial pertinent devraient être pris en compte.

40. A titre de variante, le Groupe de travail a été invité à examiner un nouvel article proposé qui serait libellé comme suit :

> "1. Lorsque la loi exige la signature d'une personne, cette condition est remplie par une signature électronique si :
>
> a) l'utilisation de la signature électronique a été convenue par les parties à l'opération, ou
>
> b) la signature électronique était aussi fiable qu'il était approprié, compte tenu des fins pour lesquelles elle était utilisée.
>
> 2. Pour déterminer si une signature électronique est aussi fiable qu'il convient à des fins particulières, sont pris en compte tout comportement des parties et tout usage commercial pertinent."

41. Le débat s'est poursuivi sur la base du nouvel article proposé. Il a été déclaré que le texte proposé se fondait sur l'approche retenue à l'article 7 de la Loi type et élargissait cette approche. En particulier, il a été indiqué que : l'alinéa a) du paragraphe 1 avait pour objet de permettre aux parties de déterminer le type de signature électronique qu'elles souhaitaient utiliser dans leurs opérations commerciales; cet alinéa s'inspirait de l'article 7-1 b) de la Loi type; et le paragraphe 2 constituait un effort d'explication de l'alinéa b). Selon un avis, si le nouvel article proposé était inclus dans les Règles uniformes, le paragraphe 2 du projet d'article 2 ne serait plus nécessaire et pourrait être supprimé.

42. On a en général objecté à cette proposition qu'elle était clairement contraire à l'article 7 de la Loi type à plusieurs égards, et notamment qu'elle n'incluait pas d'éléments relatifs à l'identification et à l'approbation, appelant ainsi "signature" quelque chose qui, sur la base de la Loi type, n'était pas une signature; elle autorisait les parties à déroger à des règles de droit impératives relatives à la signature, supplantant ainsi des règles qui, en vertu de l'article 7-2 de la Loi type, pouvaient établir une obligation en matière de signature ou des conséquences juridiques en l'absence de signature, et elle n'incluait pas de disposition similaire à l'article 7-3 de la Loi type autorisant les Etats à exclure l'application de l'article 7 dans certains cas (par exemple, effets de commerce).

43. Il a été jugé dans l'ensemble que le principal inconvénient du nouvel article proposé tenait au fait qu'à la différence de l'article 7 de la Loi type et contrairement aux règles applicables dans un environnement papier, il permettait aux parties de déroger à des règles de droit impératives. Aussi risquerait-il d'avoir pour conséquence de contrevenir à la Loi type et aux lois nationales relatives à la signature et d'avoir des effets inappropriés sur les droits des tiers. En outre, selon un avis largement partagé, il reprenait sans nécessité des éléments énoncés dans le projet d'article premier des Règles uniformes.

44. Afin d'aligner le nouvel article proposé sur l'article 7 de la Loi type et de traiter des problèmes susmentionnés, diverses suggestions ont été faites. Selon un avis, il fallait inclure une référence aux caractéristiques essentielles de la signature, à savoir celles qui tenaient à l'identification d'une personne et à l'approbation de la teneur d'un message, en insérant à la fin du chapeau du paragraphe 1 de l'article proposé le libellé suivant : "c'est la signature de cette personne", et, selon un autre avis, il faudrait faire prévaloir la loi applicable en introduisant au début de l'alinéa a) du paragraphe 1 le libellé suivant : "sous réserve du droit applicable". Selon une autre suggestion, comme dans l'article 7 de la Loi type, la conjonction entre les alinéas a) et b) devrait être "et" et non "ou". Selon une autre suggestion encore, la prise en compte du comportement des parties et des usages commerciaux pertinents prévue au paragraphe 2 du nouvel article devrait être autorisée plutôt qu'imposée, résultat qui pourrait être obtenu en remplaçant le mot "sont" par les mots "peuvent être". Enfin, selon un autre avis, les éléments essentiels des paragraphes 2 et 3 de l'article 7 de la Loi type devraient être introduits dans le nouvel article proposé.

45. Selon un avis largement partagé, au lieu de modifier le nouvel article proposé, le Groupe de travail devrait s'efforcer d'énoncer les principes fondamentaux concernant la mesure dans laquelle l'autonomie des parties devrait être prise en compte dans les Règles uniformes. Il a été convenu que les Règles ne devraient pas limiter l'autonomie des parties pour ce qui est des relations entre elles. Il a également été convenu que le Groupe de travail devrait s'attacher à identifier les types d'opération (et dans le cas des signatures numériques, les types de certificat) qui supposaient un niveau de sécurité élevé et pourraient donc être soumis aux règles impératives des lois en vigueur dans un certain nombre de pays. Pour ce qui est des conditions de forme légale qui risquaient d'empiéter sur l'autonomie des parties, il a été jugé dans l'ensemble que l'on pourrait établir une distinction utile entre les exigences en matière de signature concernant la preuve (qui pourraient être soumises à l'autonomie des parties) et les conditions de forme prescrites à des fins de validité (qui seraient normalement impératives).

46. Après un débat, le Groupe de travail a prié le secrétariat d'élaborer une version révisée du projet d'article premier, compte tenu des délibérations et des décisions ci-dessus.

Article 2. Présomptions

47. Le texte du projet d'article 2 examiné par le Groupe de travail était le suivant :

"1. En ce qui concerne un message de données authentifié à l'aide d'une signature électronique sécurisée, il est présumé, sauf preuve contraire, que :

a) le message de données n'a pas été altéré après que la signature électronique sécurisée y a été apposée;

b) la signature électronique sécurisée est la signature de la personne à laquelle elle se rapporte; et

c) la signature électronique sécurisée a été apposée par cette personne dans l'intention de signer le message.

2. En ce qui concerne un message de données authentifié à l'aide d'une signature électronique autre qu'une signature électronique sécurisée, aucune des dispositions des présentes Règles n'a d'incidence sur les règles juridiques ou les règles de preuve existantes concernant l'obligation d'établir l'authenticité et l'intégrité d'un message de données ou d'une signature électronique.

3. Les dispositions du présent article ne s'appliquent pas à ce qui suit : [...].

[4. Les présomptions énoncées au paragraphe 1 peuvent être réfutées par :

a) une preuve montrant qu'une procédure de sécurité employée pour vérifier une signature électronique ne doit pas être, en général, reconnue comme fiable, en raison des progrès de la technologie, de la manière dont la procédure de sécurité a été appliquée, ou pour d'autres raisons;

b) une preuve montrant que la procédure de sécurité convenue entre les parties au titre du sous-alinéa c) iii) de l'article premier n'a pas été appliquée de manière fiable; ou

c) une preuve relative à des faits dont la partie s'étant fiée à la signature avait connaissance, qui tendraient à indiquer que la confiance en la procédure de sécurité n'était pas raisonnable. Le caractère commercialement raisonnable d'une procédure de sécurité convenue par les parties au titre du sous-alinéa c) iii) et de l'article premier doit être déterminé en fonction des objectifs de la procédure et des circonstances commerciales au moment où les parties sont convenues d'adopter la procédure,

notamment la nature de la transaction, le niveau technologique des parties, le volume de transactions analogues effectuées par l'une ou l'autre d'entre elles ou les deux, l'existence d'autres formules proposées à la partie mais rejetées par elle, le coût d'autres procédures, et les procédures généralement utilisées pour des types de transactions analogues.]"

48. Il a certes été convenu que le principe de la neutralité quant aux techniques utilisées devrait être pris en compte dans les Règles uniformes par le biais de la reconnaissance des effets juridiques découlant de l'utilisation de signatures électroniques fondées sur des techniques non numériques, mais le Groupe de travail a décidé qu'il n'examinerai le projet d'article 2 qu'après avoir achevé son examen des autres projets d'articles des Règles uniformes.

Article 3. Attribution

49. Le texte du projet d'article 3 examiné par le Groupe de travail était le suivant :

"1. Variante A Sous réserve des dispositions de [l'article 13 de la Loi type de la CNUDCI sur le commerce électronique], l'expéditeur d'un message de données sur lequel est apposée sa signature électronique sécurisée est [lié par le contenu] [réputé être le signataire] du message de la même manière que si celui-ci était signé [à la main] conformément à la loi applicable au contenu du message.

Variante B Pour ce qui est de la relation entre le détenteur d'une clef privée et toute tierce partie se fiant à une signature numérique qui peut être [vérifiée] [authentifiée] à l'aide de la clef publique certifiée correspondante, la signature numérique [est réputée être celle du détenteur] [satisfait aux conditions énoncées à [l'article 7-1 de la Loi type de la CNUDCI sur le commerce électronique]].

2. Le paragraphe 1 ne s'applique pas si

a) [l'expéditeur] [le détenteur] peut établir que la [signature électronique sécurisée] [clef privée] a été employée sans autorisation et qu'il n'aurait pas pu empêcher un tel emploi en exerçant un soin raisonnable; ou

b) la partie se fiant à la signature savait ou aurait dû savoir, si elle s'était informée auprès [de l'expéditeur] [de l'autorité de certification] ou avait pris d'autres dispositions raisonnables, que la signature [électronique sécurisée] [numérique] n'était pas celle [de l' expéditeur] [du détenteur de la clef privée].

Remarques générales

50. Le Groupe de travail a d'abord examiné l'objet et la portée du projet d'article 3 et sa relation avec les articles 7 et 13 de la Loi type de la CNUDCI sur le commerce électronique.

51. Des avis divergents ont été exprimés sur le point de savoir si le projet d'article ne devrait traiter que de l'attribution des signatures électroniques sécurisées (ou des signatures numériques) ou s'il devrait également aborder la question de la responsabilité du signataire supposé envers les parties se fiant à la signature. Selon un avis, le projet d'article 3 devrait avoir pour objet de rattacher une signature au signataire supposé et de garantir l'intégrité d'un message de données. Selon un autre avis, le principal objet du projet d'article 3 devrait être d'inciter à utiliser les signatures numériques en répartissant comme il convient les responsabilités en cas de préjudice subi par une partie se fiant à la signature, lorsque le signataire supposé n'avait pas exercé un soin raisonnable et évité une

utilisation non autorisée de sa signature (voir par. 58 ci-après). Selon l'avis qui a prévalu, ces deux questions devraient être traitées. À ce propos, on a noté qu'il fallait faire preuve de prudence lorsque l'on traiterait des questions de la responsabilité, en raison du risque d'incompatibilité avec l'approche retenue dans la Loi type, en vertu de laquelle les questions contractuelles étaient régies par la loi applicable en dehors de la Loi type. Il a été répondu que les Règles uniformes se fondaient sur une approche quelque peu différente, car elles traitaient déjà, entre autres, de la responsabilité des autorités de certification. Après un débat, le Groupe de travail est convenu d'envisager les deux questions, peut-être dans des dispositions séparées (voir par. 55 et 60 ci-après).

52. Pour ce qui est de la portée du projet d'article 3, il a été avancé que celle-ci devrait se limiter aux signatures numériques et que le projet d'article 3 devrait être déplacé en conséquence dans la Loi type. À l'appui de cet avis, il a été noté que les signatures numériques étaient si connues et si répandues qu'elles méritaient de se voir accorder la priorité. En outre, la question de l'attribution des signatures numériques était suffisamment importante pour ne pas être traitée en même temps que l'attribution d'autres types de signatures électroniques. Selon un autre avis, les règles énoncées dans le projet d'article 3 devraient s'appliquer tant aux signatures numériques qu'aux autres signatures électroniques. Selon l'avis qui a prévalu, dans la mesure du possible, les questions traitées au projet d'article 3 devraient l'être d'une manière neutre quant aux techniques utilisées, afin d'englober une large gamme de signatures électroniques.

53. Pour ce qui est de la relation entre le projet d'article 3 et les articles 7 et 13 de la Loi type, il a été noté que l'article 7 traitait des conditions pour les signatures et l'article 13 de l'attribution des messages. On s'est demandé si le projet d'article 3 ne faisait pas que répéter les dispositions de l'article 13 de la Loi type. Il a été répondu que le projet d'article 3 traitait de l'attribution d'une signature électronique, en la distinguant de l'attribution d'un message de données et offrait une protection particulière au signataire supposé lorsque sa signature était utilisée sans autorisation et lorsqu'il n'aurait pu éviter une telle utilisation non autorisée en exerçant un soin raisonnable.

Paragraphe 1

54. Les variantes A et B ont toutes deux reçu un appui. À l'appui de la variante A, il a été déclaré qu'elle se fondait sur une approche neutre quant aux techniques utilisées et s'appliquait donc à différents types de techniques appliquées dans le commerce international. À ce propos, il a été noté que cette neutralité devrait également s'appliquer à la manière dont une technique particulière était mise en œuvre (par exemple, une signature numérique avec ou sans certificat). Cette neutralité quant à la mise en œuvre pouvait être assurée, a-t-on noté, au moyen d'une règle générale aux termes de laquelle le destinataire du message de données s'étant fondé raisonnablement sur une signature électronique sécurisée serait habilité à considérer que le message émanait bien du signataire supposé (voir A/CN.9/WG.IV/WP.73, par. 35 et 36). À l'appui de la variante B, il a été déclaré qu'elle était axée, comme il convient, sur les signatures numériques qui, à la différence des autres types de signature électronique, étaient suffisamment connues et largement répandues.

55. Toutefois, les deux variantes A et B ont fait l'objet de critiques car elles mélangeaient, de manière inappropriée, deux questions différentes, à savoir l'attribution et la responsabilité. En outre, diverses préoccupations ont été exprimées et des observations ont été faites à propos des deux variantes. Pour ce qui est de la variante A, on a noté que : les premiers mots n'étaient pas suffisamment clairs; l'utilisation du terme "expéditeur" n'était pas appropriée pour un certain nombre de raisons, notamment le fait que le signataire d'un message de données n'était pas nécessairement l'expéditeur; les mots "est lié par le contenu" se rattachaient au droit général des obligations et non à la simple attribution d'une signature électronique au signataire supposé; et la référence à la loi applicable devait renvoyer à la loi applicable au message de données dans son ensemble et non à sa teneur.

56. Pour ce qui est de la variante B, il a été noté que : afin de ne pas déroger aux exceptions énoncées dans d'autres dispositions des Règles uniformes relatives , par exemple, aux clefs privées compromises, il faudrait ajouter un libellé tel que le suivant au début de la variante B : "sous réserve des dispositions des articles..."; conformément

à l'approche retenue à l'article 13 de la Loi type, il faudrait faire référence à une vérification effective de l'utilisation authentifiée d'une signature numérique et pas seulement à l'aptitude du détenteur de la clef privée à vérifier cette utilisation; afin d'éviter les cas où une signature numérique pouvait être attribuée au signataire supposé, même s'il avait annulé le certificat, il faudrait utiliser, par exemple, le libellé suivant : "une clef privée figurant dans un certificat valide"; aucune référence ne devrait être faite à l'article 7 de la Loi type, car cet article traitait des conditions pour la signature et non de l'attribution d'une signature.

Paragraphe 2

57. S'il a été convenu au sein du Groupe de travail que le paragraphe 2 était dans l'ensemble acceptable, on a craint que l'utilisation du terme "soin raisonnable" ne soit source d'incertitude. Afin de répondre à cette préoccupation, diverses suggestions ont été faites. Selon l'une d'entre elles, la signature devrait être attribuée au signataire supposé si celui-ci ne pouvait établir que la signature avait été utilisée sans autorisation. Selon une autre suggestion, la signature devrait être réputée être celle du signataire supposé si, en outre, ce dernier ne pouvait établir qu'il n'aurait pu éviter une utilisation non autorisée, sans qu'il soit nécessaire de faire référence à la notion de "soin raisonnable". On a objecté à cette suggestion qu'elle alourdirait de manière inappropriée la responsabilité du signataire supposé.

Suggestions relatives à un nouvel article 3

58. Afin de répondre aux préoccupations émises à propos du projet d'article 3 et en partant du principe que la question de l'attribution des signatures électroniques sécurisées était suffisamment traitée dans le projet d'article 2 des Règles uniformes, on a suggéré d'axer le projet d'article 3 sur la question de la responsabilité du signataire supposé; ainsi, l'article 3 pourrait être libellé comme suit :

> "1. Pour ce qui est de la relation entre le détenteur d'une clef privée et toute personne se fiant à une signature numérique, le détenteur n'est pas lié par le message s'il ne l'a pas signé.
>
> 2. Si le détenteur de la clef n'a pas exercé un soin raisonnable afin d'empêcher l'autre partie de se fier à une signature numérique employée sans autorisation, il est tenu de dédommager la partie en question pour tout préjudice qui lui aurait été causé. La partie s'étant fiée à la signature n'est habilitée à recevoir un tel dédommagement que si elle a demandé des renseignements à l'autorité de certification ou a de toute autre manière exercé un soin raisonnable afin d'établir que la signature numérique n'était pas celle du détenteur."

59. Il a été dans l'ensemble convenu que le libellé proposé établissait à juste titre une distinction entre l'attribution d'une signature et la responsabilité en cas de préjudice causé par l'utilisation non autorisée d'une signature, mais il a été noté qu'il ne répondait pas suffisamment aux préoccupations exprimées à propos des variantes A et B. En outre, on a jugé qu'il déplaçait la charge de la preuve sur la partie se fiant à la signature, qui devait établir qu'elle avait exercé un soin raisonnable afin de prouver que la signature était celle du signataire supposé. Il a été convenu dans l'ensemble qu'il serait préférable de retenir une approche neutre quant aux techniques utilisées et que les questions de l'attribution et de la responsabilité devraient être traitées séparément.

60. Compte tenu de cette approche, le Groupe de travail a été invité à examiner un autre libellé rédigé comme suit :

> "Attribution de signatures électroniques sécurisées
>
> Pour ce qui est de la relation entre le signataire supposé et la partie se fiant à la signature, une signature électronique sécurisée est réputée être celle du signataire supposé, à moins que ce dernier ne puisse établir que ladite signature a été utilisée sans autorisation.

Responsabilité liée aux signatures électroniques sécurisées

Lorsque la signature électronique sécurisée n'était pas autorisée et que le signataire supposé n'a pas exercé un soin raisonnable pour empêcher le destinataire de se fier au message, le signataire supposé est tenu de verser des dommages-intérêts afin de dédommager la partie lésée s'étant fiée à la signature, à moins que cette dernière n'ait pas demandé de renseignements auprès d'un tiers approprié ou ait su, ou aurait dû savoir, de toute autre manière que la signature n'était pas celle du signataire supposé."

61. Après un débat, le Groupe de travail a prié le secrétariat de tenir compte du libellé proposé lorsqu'il établirait une version révisée des Règles uniformes en vue de leur examen à une session ultérieure du Groupe. Plusieurs délégations ont exprimé la crainte que le libellé proposé soit incompatible avec leur législation nationale sur les délits civils.

Section II. Signatures numériques

Article 4. Définition

62. Le texte de l'article 4 examiné par le Groupe de travail était le suivant :

"Aux fins des présentes Règles,

Variante A Les termes "signature numérique" désignent un type de signature électronique consistant en la transformation d'un message de données à l'aide d'une fonction d'abrégement du message et d'un système de cryptographie asymétrique permettant à toute personne en possession du message de données initial non transformé et de la clef publique du signataire de déterminer avec exactitude :

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

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

Variante B a) les termes "signature numérique" désignent une valeur numérique apposée à un message de données qui, grâce à une procédure mathématique connue associée à la clef cryptographique privée de l'expéditeur, permet de déterminer que cette valeur numérique n'a pu être obtenue qu'avec la clef privée de l'expéditeur;

b) les procédures mathématiques utilisées pour créer les signatures numériques en vertu des présentes Règles sont basées sur le chiffrement à clef publique. Appliquées à un message de données, ces procédures mathématiques opèrent une transformation du message de telle sorte qu'une personne en possession du message initial et de la clef publique de l'expéditeur peut déterminer avec exactitude :

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

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

63. Bien que les variantes A et B aient toutes deux bénéficié d'un certain appui, aucune n'a été adoptée par le Groupe de travail.

64. À l'appui de la variante A, il a été déclaré que, dans la mesure où elle visait uniquement la création d'une signature numérique sans mention d'une technologie particulière, elle était suffisamment souple pour englober différents types de signature numérique. On a craint, toutefois, qu'elle ne permette pas de reconnaître les différentes manières de mettre en œuvre une infrastructure à clef publique (par exemple avec ou sans recours à une fonction d'abrégement du message) et les différentes fonctions possibles d'une signature numérique (par exemple, la fonction consistant à identifier le signataire ("signature sécurisée") ou bien celle consistant à établir l'intégrité du message de données ("message sécurisé"), ou encore une combinaison des deux). Dans le cadre de cet échange de vues, il a été proposé, pour assurer une reconnaissance internationale des différents types de signatures numériques et de certificats, que le Groupe de travail envisage d'élaborer une convention au lieu d'un supplément à la Loi type (voir par. 212 ci-après).

65. En réponse aux craintes susmentionnées, on a fait observer que l'incorporation des éléments d'identification du signataire et de vérification de l'intégrité du message dans une définition de la "signature numérique" était une approche bien établie. En outre, cette approche qui visait à établir un équivalent fonctionnel d'une signature dans un environnement papier, était compatible avec l'approche adoptée dans la Loi type. Il serait par ailleurs trop ambitieux d'essayer de prendre en considération tous les types de signature numérique, et cela retarderait les progrès dans un domaine où une réglementation s'imposait d'urgence pour éviter des discordances dans le droit du fait de l'adoption d'approches différentes dans les législations nationales. On a fait observer, à cet égard, que la variante A, en définissant la signature numérique comme un type de signature électronique, limiterait ce terme aux applications de la cryptographie à clef publique censées servir d'équivalent fonctionnel d'une signature dans un environnement papier. La variante B, en revanche, serait suffisamment générale pour englober toutes les applications de la technologie des signatures numériques, y compris celles qui ne visaient pas à servir d'équivalents fonctionnels des signatures.

66. À l'appui de la variante B, on a fait observer que cette dernière offrait une plus grande certitude dans la mesure où elle était libellée en termes plus techniques et faisait expressément référence à la cryptographie à clef publique qui était réputée être une technologie très répandue. Mais on a exprimé en même temps la crainte que la variante B soit trop restrictive dans la mesure où la création d'une signature numérique y était fondée sur une certaine procédure mathématique, ce qui pouvait exclure de futurs progrès techniques susceptibles de rendre obsolètes les procédures actuellement acceptées. Il a été proposé de faire référence, dans le projet de dispositions, aux "procédures mathématiques les plus récentes".

67. On a fait valoir, à l'encontre des variantes A et B, que la référence à une "transformation du message de données" ne définissait pas correctement une "signature numérique". On a expliqué que le traitement du message par l'utilisation d'un algorithme n'entraînait pas une transformation de la totalité de ce message, mais uniquement de sa représentation numérique. Pour remédier à ce problème, on a proposé le libellé suivant :

> "Les termes 'signature numérique' désignent une transformation cryptographique (à l'aide d'une technique cryptographique asymétrique) de la représentation numérique d'un message de données, de telle sorte que toute personne en possession du message de données et de la clef publique appropriée puisse déterminer :
>
> a) que si la transformation a été opérée à l'aide de la clef privée correspondant à la clef publique appropriée; et
>
> b) que le message de données n'a pas été altéré après la transformation cryptographique."

68. On a déclaré, à l'appui du texte proposé, qu'en évitant de faire référence à la clef privée du signataire, on tenait compte du fait que les Règles uniformes devaient viser les signatures numériques utilisées à d'autres fins que la seule identification du signataire. On a également déclaré qu'en évitant de mentionner la fonction d'abrégement du message, on englobait également les signatures numériques créées à l'aide d'une autre procédure.

69. Au cours du débat, il a été proposé que le Groupe de travail examine, purement à des fins de comparaison, le texte adopté en 1988 par l'Organisation internationale de normalisation, qui était libellé comme suit : "Signature numérique : données ajoutées à une unité de données, ou transformation cryptographique d'une unité de données, permettant à un destinataire de prouver la source et l'intégrité de l'unité de données et protégeant contre la contrefaçon (par le destinataire par exemple) (ISO 7498/2). Il a aussi été proposé d'inclure la définition de l'ISO dans les Règles uniformes. Il a été convenu que cette définition démontrait l'adoption d'une approche technique, mais de nombreux membres du Groupe de travail se sont montrés sceptiques quant à son adéquation aux fins des Règles uniformes.

70. Après un débat, il a été généralement convenu que le Groupe de travail devrait reporter sa décision sur la définition des termes "signature numérique" jusqu'à ce qu'il ait terminé l'examen des dispositions de fond et soit parvenu à une conclusion quant au champ d'application de ces dispositions. En particulier, la définition des termes "signature numérique" pourrait varier selon que les Règles uniformes viseraient uniquement les utilisations de techniques informatiques ayant pour objet de reproduire, dans un environnement électronique, les fonctions traditionnellement remplies par les signatures manuscrites dans les transactions commerciales internationales ou que le champ d'application de ces Règles serait étendu à d'autres utilisations des "signatures numériques". Le secrétariat a été prié d'établir d'autres libellés en se fondant sur les variantes A et B et sur la proposition susmentionnée (voir par. 67 ci-dessus) et en tenant compte des observations formulées, en vue d'un examen de la question à une session future.

Article 5. Effets

71. Le texte du projet d'article 5 examiné par le Groupe de travail était le suivant :

"1. Lorsqu'une signature numérique est apposée sur la totalité ou sur toute partie d'un message de données, cette signature est réputée être une signature électronique sécurisée pour la partie du message en question si :

a) elle a été créée pendant la période d'effet d'un certificat [valide] et est vérifiée par référence à la clef publique indiquée dans ce certificat; et

b) le certificat est considéré comme rattachant avec précision une clef publique à l'identité d'une personne pour les raisons suivantes :

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

ii) le certificat a été émis d'une autre manière par une autorité de certification conformément aux normes établies par ... [*l'État adoptant indique l'organe ou l'autorité ayant pouvoir d'établir des normes reconnues concernant les fonctions des autorités de certification agréées*].

2. Lorsqu'une signature numérique apposée sur la totalité ou sur toute partie d'un message de données ne satisfait pas aux conditions énoncées au paragraphe 1, cette signature est considérée comme une signature électronique sécurisée pour la partie du message considérée s'il existe des preuves suffisantes montrant que le certificat rattache avec précision la clef publique à l'identité de son détenteur.

3. Les dispositions du présent article ne s'appliquent pas à ce qui suit : [...]."

Remarques générales

72. Il a été jugé dans l'ensemble, dès l'ouverture du débat, que le projet d'article 5, quant au fond, devrait être examiné plus en détail par le Groupe de travail, compte tenu des décisions qui seraient prises à propos de la portée des Règles uniformes. En particulier, le projet d'article 5 dépendait directement de la décision qui serait prise à propos de l'utilisation ou non, dans les Règles uniformes, de la notion de "signature électronique sécurisée". Les effets juridiques de l'utilisation de certificats dans le contexte des signatures numériques dépendraient également de la définition du "certificat" en vertu du projet d'article 8. Si les Règles uniformes n'englobaient que les cas où la signature numérique était utilisée aux fins d'opérations commerciales internationales avec l'intention de signer (c'est-à-dire, d'identifier le signataire et de rattacher le signataire à l'information signée), il pourrait être acceptable que le certificat n'ait pour fonction que de relier une paire de clefs à l'identité d'une personne. Dans ce cas, il devrait être spécifié que les Règles uniformes ne traitaient que d'un type particulier de certificat ("certificat d'identité"), notamment parce que d'autres types de certificat pouvaient être utilisés dans le commerce électronique, par exemple pour déterminer les pouvoirs d'une personne ("certificat de pouvoirs"). Selon un avis, ces derniers certificats devraient être traités par le projet d'article 5, au même titre que les certificats d'identité. Durant le débat, il a été proposé que référence soit faite, dans le projet d'article 5, au certificat garantissant l'intégrité de l'information contenue dans le message de données. Il a été répondu que, si la vérification de l'intégrité des données était une conséquence importante de l'utilisation d'un certificat dans le contexte de la signature numérique, il ne s'agissait pas là d'un élément caractéristique du certificat lui-même.

73. Après un débat, le Groupe de travail a décidé de procéder à l'examen du projet d'article 5. Il a toutefois été convenu que le débat devrait être rouvert après que le Groupe de travail aurait achevé son examen des dispositions de fond des Règles uniformes.

Titre

74. De l'avis d'un grand nombre de participants, le titre du projet d'article 5 n'était pas assez descriptif et risquait d'être source d'erreur. Il a été décidé de le modifier, par exemple de la manière suivante : "Signatures numériques étayées par des certificats".

Paragraphe 1

Chapeau

75. Certains ont estimé que la référence à la notion de "signature numérique sécurisée" n'était pas nécessaire dans le projet d'article 5 et devrait être remplacée par une référence aux conditions énoncées à l'article 7 de la Loi type. Il a été répondu qu'une telle référence à l'article 7 de la Loi type limiterait de manière inappropriée le champ d'application du projet d'article 5 en supposant l'existence de conditions légales de la signature, qui devraient être remplies dans un contexte électronique. L'objet du projet d'article 5 était plus large et il visait directement à éviter toute incertitude quant aux effets juridiques des signatures numériques, à condition que soient respectées certaines normes techniques, qu'il existe ou non des conditions particulières applicables à la signature.

76. Après un débat, le Groupe de travail a décidé que les références à une "signature électronique sécurisée" et aux conditions énoncées à l'article 7 de la Loi type devraient être conservées en tant que variantes, en vue d'un nouvel examen par le Groupe de travail lors d'une session future. Le chapeau du projet d'article 5 devrait être libellé comme suit : "Pour ce qui est de la totalité ou de toute partie d'un message de données, lorsque l'expéditeur est identifié par une signature numérique, la signature numérique [est une signature électronique sécurisée] [remplit les conditions énoncées à l'article 7 de la Loi type de la CNUDCI sur le commerce électronique] si :".

Alinéa a)

77. L'alinéa a) a été jugé dans l'ensemble acceptable quant au fond. Afin de mieux mettre l'accent sur la fiabilité requise du processus utilisé pour la signature numérique, il a été décidé d'insérer le mot "de manière sécurisée", afin de qualifier tant la création de la signature numérique que sa vérification par référence à la clef publique indiquée dans le certificat. Il a également été décidé que la référence à la validité du certificat serait conservée sans crochets dans le projet de disposition.

Alinéa b)

78. Pour ce qui est du sous-alinéa i) de l'alinéa b), il a été jugé dans l'ensemble que les mots "agréé" ou "enregistré" étaient préférables au mot "habilité" dans une disposition traitant des cas où les États adopteraient une approche réglementaire des infrastructures à clef publique. Pour ce qui est du sous-alinéa ii), on a jugé que cette disposition devrait être supprimée, car le champ d'application du projet d'article 5 devrait se limiter à l'utilisation de certificats émis par des autorités de certification agréées par l'État adoptant. Toutefois, selon l'avis qui a prévalu, il faudrait faire référence aux normes de l'industrie et aux mécanismes qui pourraient être élaborés par les praticiens afin de garantir la fiabilité de telles normes. Il a été convenu qu'une telle référence était nécessaire, compte tenu de l'approche "duale" en matière de signatures numériques et d'infrastructures à clef publique adoptée par le Groupe de travail lors de sa session précédente. En vertu de cette approche, les normes industrielles seraient reconnues aux côtés des règles officielles. Il a été noté que, dans certains pays, les autorités publiques ne souhaiteraient sans doute pas participer à l'établissement de normes de sécurité pour les signatures numériques. À ce propos, il a été déclaré que le projet d'article 5 ne devrait pas se contenter de mentionner les "normes de sécurité", mais englober plus largement les différents types de normes qui pourraient être élaborés par l'industrie.

79. Pour ce qui est de la référence aux normes industrielles reconnues, il a été proposé de s'inspirer de l'article 9-2 de la Convention des Nations Unies sur les contrats de vente internationale de marchandises, qui fait référence à "tout usage dont [les parties] avaient connaissance ou auraient dû avoir connaissance et qui, dans le commerce international, est largement connu et régulièrement observé par les parties à des contrats de même type dans la branche commerciale considérée". Il a été jugé dans l'ensemble, toutefois, qu'une référence à des "normes commercialement appropriées et internationalement reconnues" serait plus satisfaisante.

80. Compte tenu du débat ci-dessus, il a été convenu que l'alinéa b) devrait être modifié comme suit, aux fins d'un examen futur :

"b) le certificat rattache une clef publique à l'identité d'une personne en vertu du fait que :

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

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

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

Paragraphe 2

81. Le paragraphe 2 a suscité diverses préoccupations. Selon un avis, il risquait de faire double emploi avec l'article 2, qui énonçait les présomptions légales liées à la "signature électronique sécurisée". Il a été répondu que le paragraphe 2 était nécessaire pour établir un lien entre une signature numérique qui pourrait être reconnue (par exemple, par un tribunal) comme reliant la clef publique au détenteur, même si elle ne remplissait pas formellement les conditions énoncées au paragraphe 1, et d'autres dispositions des Règles uniformes (par exemple, le projet d'article 3 révisé relatif à la responsabilité liée aux signatures électroniques sécurisées"). À ce propos, il a été jugé que l'on pourrait introduire dans le projet d'article 3 les mots "Nonobstant les dispositions de l'article 5" .

82. On a craint également que le paragraphe 2 n'énonce une norme excessivement souple pour la reconnaissance des signatures numériques ne répondant pas par ailleurs aux conditions énoncées au paragraphe 1. Tel qu'il était actuellement rédigé, le paragraphe 2 pourrait amener à considérer comme "sécurisées" des signatures numériques fondées sur des procédures peu sûres, par exemple du fait d'une longueur insuffisante de la clef. Il a été répondu que, s'il faudrait peut-être ajouter une référence à la fiabilité des procédures techniques, soit dans le projet d'article 5, soit dans la définition de la "signature électronique sécurisée", une disposition telle que le paragraphe 2 était nécessaire, afin de préserver la possibilité que les parties soient autorisées à établir devant un tribunal judiciaire ou arbitral que la signature numérique qu'elles utilisaient était suffisamment fiable pour se voir accorder une valeur légale, même si elle n'était pas utilisée dans le contexte du paragraphe 1. On a émis la crainte, cependant, que le fait de considérer des signatures comme "sécurisées" crée des présomptions et assigne des responsabilités extracontractuelles en vertu des articles 2 et 3. Il faudrait, a-t-on déclaré, que de telles conséquences importantes puissent être déterminées par rapport à des règles et normes claires avant l'utilisation de la signature, et non imposées ultérieurement par un tribunal à une partie ne se doutant de rien.

83. Diverses suggestions ont été faites sur la manière d'exprimer la référence aux règles générales en matière de preuve énoncées au paragraphe 2. Selon un avis, le paragraphe 2 devrait être d'une portée plus large, afin d'englober non seulement les cas où un certificat était utilisé, mais aussi tout autre cas où une signature numérique ou toute autre signature électronique était utilisée. Selon cet avis, la référence au "certificat" devrait être supprimée au paragraphe 2, qui devrait être déplacé dans la section traitant des signatures électroniques en général. Selon un autre avis, le champ d'application du paragraphe 2 devrait être plus étroit et la disposition ne devrait s'appliquer que lorsque la signature numérique était créée durant la période d'effet d'un certificat. Selon cet avis, la règle énoncée au paragraphe 2 devrait être incorporée à l'alinéa b) du paragraphe 1 de la manière suivante :

> "iv) des preuves suffisantes font apparaître que le certificat rattache avec précision la clef publique à l'identité du détenteur."

84. Après un débat, le Groupe de travail n'est pas arrivé à un consensus sur la portée et l'emplacement de la disposition énoncée au paragraphe 2. Le secrétariat a été prié d'élaborer un projet de disposition révisé comportant des variantes, afin de tenir compte du débat, en vue de sa soumission au Groupe de travail lors d'une session ultérieure.

Article 6. Signature par des personnes morales

85. Le texte du projet d'article 6 examiné par le Groupe de travail était le suivant :

> "[Une personne morale peut identifier un message de données en apposant sur ce message la clef cryptographique publique certifiée pour cette personne morale. La personne morale n'est considérée [comme étant l'expéditeur] [comme ayant approuvé l'envoi] du message que si le message est également signé numériquement par la personne physique autorisée à agir au nom de cette personne morale.]"

86. Il a été rappelé qu'à la session précédente du Groupe de travail, il avait été jugé dans l'ensemble que le projet d'article 6 devrait être supprimé. Ce dernier avait été conservé entre crochets, afin de rappeler au Groupe de travail qu'il devrait peut-être étudier plus en détail la mesure dans laquelle les Règles uniformes devraient valider les fonctions d'"agents électroniques" ayant pour objet d'authentifier automatiquement des messages de données (voir A/CN.9/437, par. 115 à 117). Le Groupe de travail a décidé que la question des "agents électroniques" devrait être examinée ultérieurement. Il a toutefois été décidé que le projet d'article 6 serait supprimé, car il pourrait être considéré comme empiétant de manière inappropriée sur d'autres domaines du droit (par exemple, le droit de la représentation et les dispositions du droit des sociétés traitant de la représentation des sociétés par des personnes physiques).

Section III. Autres signatures électroniques

87. De l'avis général, la Section III devrait être maintenue dans les Règles uniformes, en attendant qu'une décision soit prise quant à la question de savoir si le principe de la non-discrimination énoncé dans la définition de "signature" et de "signatures électroniques sécurisées" (et exprimé en vertu du statut juridique reconnu à toute technique d'authentification pouvant être considérée comme une signature électronique "sécurisée"), devrait être également exprimée sous forme de disposition plus précise traitant des techniques d'authentification autres que les signatures numériques.

88. Afin de fournir davantage de renseignements au Groupe de travail sur la manière dont les signatures numériques et d'autres techniques d'authentification pourraient fonctionner, un certain nombre d'exposés de caractère technique ont été présentés. Ces exposés sont récapitulés ci-dessous (par. 89 à 105).

89. On a rappelé que le commerce électronique sécurisé exigeait que les parties à une transaction puissent s'authentifier. S'agissant de l'interaction électronique (par exemple les achats sur l'Internet), dans de nombreux cas, les méthodes traditionnelles d'authentification étaient, soit inexistantes soit dépourvues de fiabilité. Le besoin de méthodes fiables d'authentification électronique allait au-delà des exigences du commerce et s'appliquait à presque tous les types d'interaction dans un environnement numérique.

90. On a fait observer qu'il existait actuellement une grande diversité de solutions pour répondre à ces besoins. Ces solutions comportaient un élément technologique et un élément méthodologique. Si l'attention était en général principalement axée sur les différentes technologies, il ne fallait pas sous-estimer l'impact de la méthodologie ou du modèle commercial qui sous-tendait la solution offerte par l'authentification électronique. Outre de nombreuses approches technologiques, le marché offrait également une grande richesse de méthodologies qui mettaient à profit ces technologies. La diversité des solutions mettait en évidence les différents types d'authentification qu'exigeaient les nombreuses situations que l'on pouvait rencontrer dans un environnement numérique. À mesure que cet environnement se développait, de nouvelles solutions devenaient nécessaires.

91. Les méthodes d'authentification pouvaient être regroupées en plusieurs catégories selon la caractéristique faisant l'objet de l'authentification. Les trois catégories principales ont été présentées comme suit : 1) "quelque chose que vous savez"; 2) "quelque chose que vous êtes"; et 3) "quelque chose que vous avez". De nombreuses solutions se fondaient sur une combinaison de ces trois caractéristiques.

92. La première catégorie ("quelque chose que vous savez") était une des caractéristiques les plus couramment utilisées pour authentifier les individus. Les mots de passe et les numéros d'identification personnels relevaient de cette catégorie. La plupart des systèmes informatiques offraient un choix de mots de passe qui permettaient à ceux qui détenaient un mot de passe valide d'accéder à des ressources. Par exemple, l'accès automatique aux informations relatives à un compte bancaire exigeait des utilisateurs qu'ils connaissent le bon numéro d'identification personnel associé au compte interrogé. Dans cette catégorie, un autre type d'authentification se fondait sur des informations personnelles que seul un individu donné était censé connaître. Par exemple, dans certaines juridictions, il était

courant qu'une banque demande à un individu de donner le nom de jeune fille de sa mère lors de l'ouverture d'un compte bancaire. Cette information pouvait être utilisée ultérieurement pour authentifier le titulaire du compte. Si cette catégorie d'authentification était largement utilisée dans la pratique, elle présentait certaines faiblesses. Premièrement, elle impliquait habituellement que les informations partagées soient secrètes ou difficiles à obtenir. Deuxièmement, elle impliquait que les parties aient eu une relation préalable leur permettant de "partager" l'élément secret de la connaissance (par exemple, le mot de passe, le numéro d'identification personnel ou le nom de jeune fille de la mère).

93. La seconde catégorie des méthodes d'authentification ("quelque chose que vous êtes") renvoyait souvent à la biométrie. Cette approche mettait à profit des qualités innées de l'individu aux fins de l'authentification. Certains aspects innés utilisés en biométrie étaient notamment les suivants : empreintes digitales, empreinte rétinienne, iris, empreintes de mains, empreintes vocales et signatures manuscrites. Dans la mesure où toutes ces caractéristiques étaient uniques pour chaque individu, elles offraient une excellente méthode d'authentification. Si les informations concernant ces caractéristiques pouvaient être rendues publiques, alors ce type d'authentification n'exigerait plus une relation préalable. En outre, ces approches pouvaient souvent assurer une authentification efficace car il était très difficile de manipuler ou d'induire en erreur ces systèmes. Un inconvénient de ces techniques était que leur mise en œuvre coûtait plus cher car il fallait utiliser certains types de matériel pour obtenir des informations sur l'aspect considéré. Une autre préoccupation suscitée par certaines applications relevant de cette catégorie était liée au mécanisme utilisé pour collecter des informations biométriques. Dans certains cas, ces dispositifs étaient jugés importuns (par exemple, le scanner de la rétine supposait que les utilisateurs appliquent l'œil sur un oculaire, après quoi une lumière rouge était utilisée pour scanner la rétine). Dans d'autres cas, l'information obtenue par le scanner d'authentification pouvait divulguer des renseignements sur la santé de l'individu que celui-ci ne voulait pas rendre publics (par exemple, certaines conditions de santé pouvaient être diagnostiquées par des irrégularités dans l'iris et de ce fait, si un scanner de l'iris n'était pas physiquement gênant, certains considéraient qu'il empiétait sur la vie privée). Enfin, certains de ces mécanismes n'étaient pas toujours fiables lorsque les conditions d'utilisation étaient "anormales" (par exemple, empreintes digitales présentant une coupure sur un doigt). Néanmoins, les solutions biométriques étaient largement considérées comme l'une des méthodes d'authentification les plus efficaces et étaient actuellement utilisées dans la pratique. On a donné des exemples d'un pays où les services d'immigration et de naturalisation mettaient à l'essai une technologie d'empreintes de mains pour accélérer le contrôle des passeports; en outre, des compagnies d'assurance utilisaient la biométrie pour authentifier la signature d'individus dans le traitement des sinistres.

94. La troisième catégorie de méthodes d'authentification ("quelque chose que vous avez") a été présentée comme l'un des domaines les plus actifs de l'authentification électronique. Ce "quelque chose" pouvait être matériel (par exemple, un mécanisme de questions-réponses) ou être une information (par exemple, une clef cryptographique). Un mécanisme de questions-réponses était similaire à l'approche du secret partagé adoptée dans la catégorie "quelque chose que vous savez", mais il impliquait l'utilisation de matériel. Cette solution exigeait que l'on donne à des individus un mécanisme qui était unique et qui était affecté à un utilisateur seulement. Lorsque l'individu voulait accéder à un service, le système hôte lui demandait de s'identifier (habituellement par un nom d'utilisateur) puis le système produisait une question numérique fondée sur l'information qu'il détenait sur le mécanisme unique affecté à l'individu. L'individu entrait alors ce numéro dans le mécanisme qui produisait une réponse numérique. Cette réponse numérique pouvait ensuite être saisie dans le système auquel le détenteur du mécanisme voulait accéder. Le système hôte "savait" qu'il n'y avait qu'une réponse acceptable à la question numérique posée à l'individu et que cette réponse acceptable ne pouvait être produite que par le mécanisme unique affecté à cet individu. De ce fait, si l'individu entrait la bonne réponse numérique, le système hôte "savait" que la personne qui essayait d'y accéder était bien celle qu'elle prétendait être. Ce type de mécanisme était couramment utilisé pour authentifier les individus qui cherchaient à accéder à distance à des systèmes informatiques. Il était également utilisé par une banque dans le cadre d'un projet pilote de services bancaires à domicile dénommé "browser banking" car il permettait à un individu d'accéder à un compte bancaire à partir de n'importe quel navigateur ou machine. Cette

application mettait en évidence l'un des atouts de cette méthode. En effet, si elle exigeait un élément matériel, elle n'impliquait pas de modification du système comme les cartes à puce.

95. Une autre sous-catégorie de la troisième catégorie portait sur l'utilisation des signatures numériques. L'aspect majeur de la technologie des signatures numériques était l'utilisation d'une clef privée pour créer une signature numérique et l'utilisation d'une clef publique pour authentifier la signature numérique. La clef privée utilisée pour créer les signatures numériques pouvait être stockée sur un disque dur ou sur une carte à microprocesseur et devait être conservée de façon très confidentielle par l'utilisateur. La clef publique était largement répandue. Différentes théories étaient associées à l'application de la technologie des signatures numériques, chacune offrant un moyen de donner confiance au destinataire d'une signature numérique.

96. Une des premières méthodes consistait à créer un répertoire des personnes et des clefs publiques. Selon ce modèle, le destinataire d'un document signé numériquement vérifiait la clef publique du signataire du document dans un répertoire fiable. Il a été indiqué qu'actuellement, plusieurs applications étaient fondées sur ce modèle.

97. Une autre approche, découlant de l'approche ci-dessus se fondait sur des certificats numériques. Ces certificats étaient des documents électroniques, numériquement signés par une entité de confiance. Lorsqu'un document était signé numériquement, une copie du certificat numérique du signataire y était jointe. Celle-ci contenait des informations sur la personne et sur sa clef publique. Lorsque le destinataire recevait le message et le certificat numérique, il utilisait la clef publique figurant dans le certificat numérique pour authentifier le message.

98. L'une des utilisations courantes des certificats numériques se fondait sur une norme (ISO X.509), qui offrait une hiérarchie d'entités de confiance utilisables pour authentifier les parties. Cette approche était souvent désignée sous le nom de "modèle des cartes de crédit", car elle se fondait sur le modèle retenu dans l'industrie des cartes de crédit. Par exemple, un commerçant pouvait ne pas connaître un consommateur, mais être disposé à accepter certaines cartes à des fins de paiement, car il savait que la carte était délivrée au consommateur par une banque (le nom de la banque figurant toujours sur la carte), qui était autorisée à émettre ladite carte par la société de cartes de crédit. Même si le commerçant ne connaissait pas la banque ayant délivré la carte, il pouvait faire confiance au consommateur, car il savait que celui-ci avait été authentifié par la banque et que la banque avait été authentifiée par la société de cartes de crédit. De même, les hiérarchies de la norme X.509 permettaient l'authentification des certificats numériques par une chaîne hiérarchique d'entités de confiance (appelées "Autorités de certification"), qui pouvait être vérifiée par le destinataire du certificat. La dernière autorité de certification dans cette chaîne de confiance était désignée sous le nom d' autorité de base (*root*). De ce fait, la signature numérique d'un document selon cette méthode consistait en l'envoi du certificat numérique du signataire et de tous les certificats numériques connexes associés à la hiérarchie utilisée. Selon ce modèle, le destinataire pouvait vérifier l'ensemble de la chaîne de confiance, sans avoir à se reporter à un répertoire en ligne. Cette approche était considérée comme particulièrement bien adaptée aux communications de confiance entre un grand nombre de personnes n'ayant aucun contact, ou que des contacts limités, entre elles. L'un des atouts de cette approche, l'aptitude à rattacher de nombreux certificats à une autorité de base, était aussi une de ses faiblesses. Si l'autorité de base était compromise, tout ce qui était au-dessus perdait sa fiabilité.

99. Une autre variante de l'utilisation des certificats numériques était souvent désignée sous le nom de "modèle de réseau confiance" (*web of trust model)*. Dans ce modèle, il n'y avait pas d'autorité de certification. Les certificats numériques étaient créés par des individus. Il n'y avait pas d'autorité de base. Les individus décidaient à qui ils se fieraient et dans quelle mesure. Le modèle était conçu pour des petites collectivités d'usagers ayant des contacts réguliers et était difficile à mettre en œuvre à grande échelle. Néanmoins, ce modèle était actuellement utilisé dans de nombreux contextes.

100. Il a été déclaré que l'un des importants éléments à prendre en compte pour mieux comprendre l'utilisation des certificats numériques X.509 était l'importance historique accordée à l'identité. Comme la norme X.509

découlait du répertoire X.500, elle était naturellement axée sur l'association de clefs publiques à l'identité de personnes. Cette importance accordée à l'identité, a-t-on déclaré, compliquait de nombreuses questions d'ordre public, liées à l'utilisation des signatures numériques. S'il était clair que certains certificats numériques authentifiaient l'identité d'une personne, il était également clair que d'autres certificats numériques avaient des fonctions autres que cette authentification. De tels certificats pouvaient également être utilisés pour authentifier les droits d'un individu ou ses relations, sans pour cela certifier son identité. Dans de nombreux cas, il n'était pas nécessaire, ou il n'était parfois même pas souhaitable de connaître l'identité de l'individu. Il existait de nombreux certificats délivrés à des fins spéciales qui ne pouvaient être utilisés que pour certaines fonctions, de même que la carte de crédit d'un individu ne pouvait être utilisée pour authentifier son identité et qu'un passeport ne pouvait l'être pour acheter des marchandises. Cette tendance à se fonder sur l'identité, quoique logique, pouvait limiter considérablement l'utilisation de cette technologie. Si chaque application fondée sur les signatures numériques devait remplir les strictes conditions d'un certificat d'identité à usage général, alors la technologie serait très difficile à utiliser et très onéreuse. Il importait de se rappeler qu'il existait un large éventail d'exigences en matière d'authentification et que la technologie était suffisamment souple pour répondre à toutes ces exigences.

101. Lorsque certaines sociétés de cartes de crédit avaient décidé de mettre au point une méthode sûre pour le commerce électronique par le biais de réseaux publics tels que l'Internet, elles avaient recensé trois grands objectifs commerciaux : la solution devait être sûre; elle devait être disponible à tout fournisseur de techniques désireux d'élaborer un produit conforme au protocole défini; et toutes les applications devaient pouvoir fonctionner entre elles. Pour l'industrie des paiements, le terme "sûr"ou "sécurisé" comportait les trois éléments suivants : 1) caractère confidentiel de l'information relative au paiement, y compris l'intitulé du compte du consommateur; 2) intégrité de l'information relative à la commande; et 3) authentification des parties à l'opération. C'est pour offrir le niveau requis de "sécurité" qu'avait été créé le protocole intitulé "Secure Electronic Transaction" (SET). Ce protocole utilisait les signatures numériques (sur la base du modèle X.509) pour remplir les fonctions d'intégrité des données et d'authentification des parties.

102. Une brève description du protocole SET avait été faite. Un consommateur qui décidait d'effectuer une opération de commerce électronique sécurisée au moyen du SET devait d'abord obtenir un logiciel conforme aux procédures énoncées par l'autorité de certification de base du SET. Ce logiciel créait une paire de clefs et un formulaire que le consommateur adressait à l'entité ayant émis la carte de paiement devant être utilisée. Le logiciel plaçait la clef publique dans la demande de certificat et invitait le consommateur à donner des renseignements sur son identité, afin que l'organisme financier puisse vérifier que la personne demandant le certificat était autorisée à le faire. Cette demande était adressée à l'organisme financier par l'Internet. Si la demande était acceptée, l'organisme financier signait numériquement le certificat du consommateur et le lui renvoyait par l'Internet. Le logiciel du consommateur enregistrait le certificat numérique dans l'ordinateur du consommateur. Cette procédure n'était effectuée qu'une fois pour l'obtention du certificat.

103. Le consommateur commençait alors à effectuer ses achats en direct et pouvait entreprendre des opérations sûres avec les commerçants au moyen du logiciel conforme au protocole SET. Durant les premières étapes de l'opération, le logiciel du consommateur demandait au commerçant des informations en vue d'une authentification. Le logiciel authentifiait le commerçant en vérifiant toutes les signatures numériques et certificats numériques adressés par le commerçant. S'il y avait un problème à tout moment du processus d'authentification, le consommateur était averti. Le consommateur identifiait alors les biens ou services qu'il désirait acheter, choisissait la méthode de paiement et effectuait l'opération. Le logiciel du consommateur séparait les informations relatives au paiement et les informations relatives à la commande. Les informations relatives au paiement étaient codées au moyen d'une méthode de cryptographie fiable, de sorte que l'organisme financier du commerçant était seul à même de les décrypter. Les informations relatives à la commande, spécifiant ce qui était commandé et d'autres détails de l'opération, ainsi que les informations codées relatives au paiement, étaient signées numériquement et envoyées au commerçant. Lorsque le commerçant recevait ce message, il séparait les informations codées relatives au paiement, signait numériquement le nouveau message et l'adressait à son organisme financier. Ce dernier vérifiait la signature

numérique du commerçant, décryptait les informations relatives au paiement, puis les soumettait pour traitement à l'infrastructure de paiement utilisée. Il signait numériquement l'autorisation et l'envoyait au commerçant. Le commerçant envoyait alors une réponse signée numériquement au consommateur. Si l'opération était autorisée, le commerçant honorait la commande.

104. Il a été indiqué que le protocole SET était un exemple de l'utilisation de la technologie des signatures numériques pour l'authentification des messages et des parties. Toutefois, il importait de noter que les certificats SET n'étaient pas des certificats d'identité. Ils n'authentifiaient pas l'identité d'une personne et ne pouvaient être utilisés pour cette fonction, comme il était explicitement indiqué dans la déclaration jointe aux certificats. Les certificats SET ne faisaient qu'authentifier le lien entre une clef publique et un intitulé de compte. Le SET utilisait la technologie des signatures numériques pour offrir un surcroît de protection dans le cadre d'une opération, et non pour identifier une personne. En outre, le SET n'utilisait pas de listes d'annulation des certificats pour les certificats de consommateurs ou de commerçants. Dans le cadre du modèle commercial SET, de telles listes n'étaient pas nécessaires. Les opérations devaient toujours être autorisées par l'infrastructure de paiement utilisée, de sorte que l'ajout de listes d'annulation des certificats des titulaires de cartes n'offrirait aucun avantage, tout en augmentant sensiblement le coût de la mise en place et de l'entretien du système.

105. Il a été indiqué que le SET illustrait : 1) l'utilisation des signatures et certificats numériques à des fins autres que l'identification; 2) l'émission de certificats par des autorités de certification non agréées, relevant du marché; 3) l'émission de certificats dans un système où les parties avaient défini par convention leurs droits et responsabilités; et 4) le fait que, dans certains cas, une partie se fiant à un certificat (la banque ayant effectué le paiement sur la base d'informations signées numériquement par le consommateur) pouvait être l'émetteur du certificat. Le SET n'était qu'un exemple de la mise en œuvre de la technologie des signatures numériques. Il a été déclaré que de nombreuses autres utilisations apparaîtraient durant les années à venir et qu'elles se fonderaient sur des technologies et modèles commerciaux qui n'existaient pas encore.

106. Le Groupe de travail s'est félicité des présentations qui avaient été faites. Il a été jugé dans l'ensemble que ces illustrations des techniques actuellement mises en œuvre ou envisagées étaient utiles pour permettre une meilleure compréhension des problèmes juridiques qu'il faudrait traiter dans les Règles uniformes. Le Groupe de travail a exprimé l'espoir que d'autres exposés concernant l'évolution des techniques de signature numérique et des autres techniques d'authentification pourraient être faits lors de sessions ultérieures.

CHAPITRE III. AUTORITÉS DE CERTIFICATION ET QUESTIONS CONNEXES

Article 7. Autorité de certification

107. Le texte du projet d'article examiné par le Groupe de travail était le suivant :

"1. Aux fins des présentes Règles, les termes "autorité de certification" désignent :

a) toute personne ou entité agréée [habilitée] par ... [*l'État adoptant indique l'organe ou l'autorité ayant pouvoir d'agréer les autorités de certification et de promulguer des règles concernant les fonctions des autorités de certification agréées*] pour agir en application des présentes Règles;

b) toute personne ou entité qui, dans le cours ordinaire de ses affaires, délivre des certificats concernant des clefs cryptographiques utilisées pour créer des signatures numériques.

[2. Une autorité de certification peut proposer ou faciliter l'enregistrement et l'horodatage de la transmission et de la réception de messages de données et remplir d'autres fonctions ayant trait aux communications protégées au moyen de signatures numériques.]"

Paragraphe 1

108. Selon un avis, le paragraphe 1 mettait trop l'accent sur le cas où la fonction d'autorité de certification était remplie par un tiers indépendant (souvent désigné sous le nom de "tiers de confiance"), ce qui n'était pas le seul cas envisageable. Il a été noté que, dans la pratique en matière de signature numérique, les parties recouraient de plus en plus à des mécanismes d'autocertification (ou de certification mutuelle), ne faisant intervenir que les expéditeurs et destinataires de messages signés numériquement. De ce fait, la définition d'"autorité de certification" devrait être élargie à tous les types de pratiques. Il a été proposé de remplacer à l'alinéa b) les mots "dans le cours ordinaire de ses affaires" par les mots "dans le cours de ses affaires". Cette suggestion a été jugée dans l'ensemble acceptable.

109. Selon une autre suggestion, il faudrait, outre la définition d'"autorité de certification", traiter également de la définition de l'"autorité d'enregistrement". Cette suggestion n'a pas reçu d'appui, mais il a été jugé dans l'ensemble que la question devrait être réexaminée à un stade ultérieur.

110. Selon une autre suggestion, il faudrait supprimer l'alinéa a), car il ne faisait que traiter d'une sous-catégorie de la catégorie visée à l'alinéa b) et les mots "dans le cours ordinaire de ses affaires", à l'alinéa b) devraient être remplacés par les mots "dans le cours de ses affaires", ou "dans le cadre de ses activités". À l'appui de cette suggestion, il a été déclaré que toute référence à des "autorités de certification agréées" dans les Règles uniformes pourrait être interprétée comme visant à inciter les États adoptants à mettre en place des mécanismes d'agrément, ce qui pourrait être contraire à l'approche "duale" adoptée par le Groupe de travail à sa session précédente (voir A/CN.9/437, par. 69). Il a également été noté que la suppression de l'alinéa a), tout en préservant la souplesse requise, mettrait comme il convient l'accent, dans les Règles uniformes, sur l'utilisation des signatures numériques aux fins d'opérations commerciales internationales, par opposition à l'utilisation des signatures numériques à des fins administratives. Toutefois, selon l'avis qui a prévalu, il faudrait conserver la teneur de l'alinéa a). Il a été noté que, dans certains contextes, les autorités de certification agréées ne fonctionnaient pas toujours comme des "entreprises". En outre, la distinction entre les autorités de certification agréées et celles qui fonctionnaient à titre purement privé était justifiée, compte tenu des régimes juridiques différents pouvant être applicables à ces deux types d'autorités. Un exemple a été donné de ces différences : la législation antitrust pouvant être applicable à des autorités de certification privées ne le serait peut-être pas à des autorités de certification s'acquittant de fonctions publiques. En outre, même si la catégorie traitée à l'alinéa a) était englobée dans l'alinéa b), cet alinéa a) serait quand même utile pour les États désireux d'appliquer un mécanisme d'agrément, ce qui préserverait la neutralité des Règles uniformes.

111. Compte tenu de ce qui précède, il a été décidé de modifier le paragraphe 1 comme suit, en vue d'un examen ultérieur :

"1. Aux fins des présentes Règles, les termes "autorité de certification" désignent toute personne ou entité qui, dans le cours de ses affaires, délivre des certificats concernant des clefs cryptographiques utilisées pour créer des signatures numériques.

2. Le paragraphe 1 s'entend sous réserve de toute loi applicable exigeant qu'une autorité de certification soit agréée ou accréditée, ou qu'elle fonctionne d'une manière spécifiée dans ladite loi."

Paragraphe 2

112. Le maintien du paragraphe 2 a reçu un certain appui. Selon un avis, les diverses fonctions énumérées dans ce paragraphe devraient être complétées par une référence expresse à d'autres fonctions, telles que la création, la gestion, la suspension ou l'annulation des certificats, afin que soit mieux illustré le lien entre les divers services connexes offerts par les autorités de certification et le fonctionnement d'un système de signature numérique, qui constituait l'activité essentielle d'une autorité de certification. Toutefois, selon l'avis qui a largement prévalu, il faudrait supprimer le paragraphe 2 et sa teneur devrait être réexaminée ultérieurement en vue de son inclusion éventuelle dans un guide pour l'incorporation des Règles uniformes, au cas où le Groupe de travail déciderait d'élaborer un tel guide.

Article 8. Certificat

113. Le texte du projet d'article 8 examiné par le Groupe de travail était le suivant :

> "Aux fins des présentes Règles, le terme "certificat" désigne un message de données [ou un autre document] qui, au minimum :
>
> a) identifie l'autorité de certification qui l'émet;
>
> b) nomme ou identifie son détenteur ou un dispositif ou un agent électronique sous le contrôle du détenteur;
>
> c) contient une clef publique correspondant à une clef privée dont le détenteur a le contrôle;
>
> d) spécifie sa période d'effet [et, le cas échéant, les restrictions à l'utilisation de la clef publique]; et
>
> e) est signé [numériquement] par l'autorité de certification qui l'émet."

Remarques générales

114. Il a été généralement convenu que l'article 8 devrait être divisé en deux parties (ou en deux articles séparés), l'une donnant une définition générale des certificats visés par les Règles uniformes et l'autre énumérant les éléments minimums que devraient contenir ces certificats, d'après les alinéas a) à e). On a fait observer qu'une telle division permettrait d'élargir utilement le champ d'application des Règles uniformes, qui serait plus limité si tous les éléments énoncés au projet d'article 8 étaient englobés dans la définition du "certificat".

Définition du terme "certificat"

115. Il a été convenu, dès le départ, qu'il ne serait peut-être pas indiqué de donner des définitions techniques des certificats, car ces définitions seraient probablement révisées pour tenir compte de l'évolution des besoins et des technologies. Le Groupe de travail a ensuite examiné une définition du terme "certificat" sur la base du libellé suivant : "Aux fins des présentes Règles, le terme "certificat" désigne un message de données ou un autre document émis par une autorité de certification en vue d'identifier une personne ou une entité détenant une clef privée".

116. On a fait observer qu'une telle définition couvrait uniquement les certificats d'identité et laissait hors du champ d'application des Règles uniformes divers certificats qui étaient largement utilisés et qu'il serait peut-être nécessaire de reconnaître. Des vues divergentes ont été exprimées sur ce point. Selon l'une d'entre elles, seuls les certificats d'identité devraient être traités dans les Règles uniformes. Selon une autre, il faudrait également englober

d'autres types de certificat (par exemple les certificats de pouvoirs). Bien que cette opinion ait bénéficié d'un certain appui, on a exprimé la crainte que, si les Règles uniformes visaient d'autres certificats, les dispositions portant sur les garanties données par une autorité de certification et, en conséquence, sa responsabilité, doivent établir des régimes juridiques différents pour les différents types de certificat émis, ce qui pourrait rendre la tâche du Groupe de travail par trop ambitieuse.

117. S'agissant de la forme, il a été proposé, pour couvrir divers types de certificat, d'élaborer une définition générale s'appliquant à tous les types de certificat, et d'énoncer ensuite dans des dispositions subséquentes les éléments minimums devant figurer dans chaque type de certificat. Pour ce faire, il a été suggéré d'adopter un libellé tel que : "Aux fins des présentes Règles, le terme "certificat" désigne un message de données permettant la vérification d'un message de données correspondant à la clef publique contenue dans le certificat". Il faudrait ensuite énoncer l'objet de chaque type de certificat, par exemple de la façon suivante : "Un certificat d'identité a pour objet de fournir une preuve de l'identité". Pour rendre l'idée que les certificats peuvent remplir diverses fonctions, il a aussi été proposé de modifier la définition en indiquant que le message de données était "supposé vérifier l'identité ou une autre caractéristique importante d'une personne". Il a été suggéré par ailleurs de remplacer par des mots tels que "confirmer", "établir", ou un autre terme analogue le mot "vérifier", auquel on pouvait donner parfois un sens technique précis.

118. Les débats se sont concentrés sur la dernière définition proposée. S'agissant de la formulation exacte de la définition des termes "certificat d'identité", un certain nombre de suggestions ont été faites. Il a été proposé notamment d'éviter les termes "autre document". À l'appui de cette proposition, on a déclaré que l'incorporation du mot "document" dans les Règles uniformes risquait de donner lieu à des problèmes pour l'interprétation de l'article 2 a) de la Loi type. En réponse à cet argument, on a fait observer que ce mot permettrait d'éviter toute incertitude quant à la question de savoir si un certificat uniquement sur papier serait couvert par les Règles uniformes. Il a été aussi proposé, pour éviter des problèmes d'interprétation quant aux intentions subjectives des parties, de remplacer les mots "en vue d'identifier" par les mots "qui identifie".

119. À l'encontre du libellé proposé, on a fait valoir qu'il pourrait engendrer une situation dans laquelle l'autorité de certification serait en mesure d'échapper à sa responsabilité en n'identifiant pas la personne à l'intention de laquelle le certificat était émis. Il fallait donc insérer un libellé tel que "supposé identifier". Selon une autre proposition, le mot "personne" devrait être remplacé par le mot "sujet", terme spécialisé largement utilisé dans la pratique et qui permettrait de prendre dûment en compte les cas dans lesquels le sujet du certificat n'était pas une personne mais "un dispositif ou un agent électronique". Les arguments des opposants à cette suggestion étaient que si l'on utilisait le terme "sujet", il faudrait le définir par référence à une "personne"; que ce serait, en tout état de cause, une personne qui contrôlerait tout "dispositif ou agent électronique", et que le terme "sujet" serait incompatible avec la terminologie employée dans la Loi type ainsi que dans d'autres textes de la CNUDCI. L'emploi du mot "personne" a été jugé acceptable, à condition de préciser qu'il désignait le sujet d'un certificat et englobait également le terme "entité". Quant à ce dernier, il a été convenu de le maintenir jusqu'à ce que le Groupe de travail prenne une décision définitive sur la question de savoir si "un dispositif ou un agent électronique" pouvait être le sujet d'un certificat. Selon une autre proposition encore, il faudrait remplacer les termes "une paire de clefs" par les termes "une clef privée".

120. Après un débat, le Groupe de travail a décidé de reformuler comme suit la définition :

"Certificat [d'identité]

Aux fins des présentes Règles, le terme "certificat" [d'identité] désigne un message de données ou un autre document émis par une autorité de certification et supposé confirmer l'identité [ou une autre caractéristique importante] d'une personne ou d'une entité détenant une paire de clefs particulière".

121. Il a été convenu que les termes “d’identité” et “ou d’une autre caractéristique importante” placés entre crochets permettraient au Groupe de travail d’examiner ultérieurement la question de savoir si les Règles uniformes devaient viser des certificats autres que les certificats d’identité.

Disposition relative au contenu minimum d’un certificat d’identité

122. Le Groupe de travail s’est ensuite penché sur les alinéas a) à e), en se concentrant sur la question de savoir s’ils décrivaient avec exactitude le contenu minimum d’un certificat d’identité.

Remarques générales

123. Il a été généralement convenu que l'objectif pratique d'une disposition énumérant les éléments minimums d'un certificat était d’énoncer les normes qu'une autorité de certification devrait respecter pour remplir sa fonction et éviter d'être tenue responsable d'un préjudice dû au fait qu’elle n’avait pas inclus dans le certificat tous les éléments nécessaires. Le sentiment largement partagé a été qu'aucune décision définitive ne pouvait être prise au sujet du contenu minimum d'un certificat avant qu'ait été clarifiée la question de la responsabilité de l'autorité de certification et celle des types de certificat devant être visés par les Règles uniformes. Le Groupe de travail a décidé d'examiner les alinéas a) à e) en partant du principe qu'un échange de vues préliminaire pourrait faciliter la reprise du débat à un stade ultérieur.

124. Lors du débat, on s'est demandé si un certificat qui ne remplissait pas les conditions minimums énoncées dans le projet d'article 8 devait être considéré comme non valide ou si le projet d'article 8 devait faire fonction de règle par défaut, auquel cas le certificat pourrait être valide, si les parties en décidaient ainsi. Dans le dernier cas, il a été proposé d'insérer au projet d'article 8 une règle s'inspirant du projet d'article 5-2.

Chapeau

125. Il a été convenu qu'un certificat pouvait être émis sous une forme uniquement papier, mais des doutes ont été exprimés quant à l'adéquation de l'expression "ou autres documents" (voir par. 118 ci-dessus).

Alinéa a)

126. L'alinéa a) a été jugé généralement acceptable quant au fond.

Alinéa b)

127. On s'est demandé si le mot "détenteur" désignait la personne à l'intention de laquelle le certificat était émis ou bien la personne détenant une copie dudit certificat et s’y fiant. Il a en outre été déclaré que l'emploi du terme "détenteur" était source d’incertitude car dans le projet d'article 8 il désignait à la fois la personne détenant le certificat et la personne détenant la paire de clefs appropriée. Il a été proposé d'employer plutôt le terme "sujet", mais pour les raisons susmentionnées, le Groupe de travail a exprimé une préférence générale pour le terme "personne" (voir par. 119 ci-dessus). Toutefois, il a été décidé de conserver les deux termes en les mettant entre crochets, en vue d'un examen plus approfondi de la question. Pour ce qui était des termes "un dispositif ou un agent électronique", dont l'emploi, a-t-on déclaré, créait une incertitude, il a été décidé de les placer entre crochets jusqu'à ce que le Groupe de travail étudie plus avant la question (voir par. 119 ci-dessus).

Alinéa c)

128. L’alinéa c) a été jugé généralement acceptable quant au fond. Pour ce qui est du terme “détenteur”, il a été décidé de le remplacer par les mots “sujet” et “personne” placés entre crochets (voir par. 127 ci-dessus).

Alinéa d)

129. Il a été généralement convenu que la période d'effet était un des éléments fondamentaux d'un certificat. En ce qui concerne le champ d'utilisation d'un certificat et toutes restrictions à cet égard, il a été proposé de supprimer le libellé existant ou tout au moins de le modifier afin de préciser que le champ d'utilisation et les restrictions pouvaient être incorporés dans le certificat par référence. Il a été déclaré, à l'appui de cette proposition, qu'il pourrait être impossible d'inclure dans un certificat une liste complète de toutes les restrictions. On a fait observer en outre que l'on pourrait ainsi engager involontairement la responsabilité de l'autorité de certification en cas d'omission d'une des restrictions possibles dans un certificat. À l'encontre de cette proposition, on a fait valoir que le champ d'utilisation et toutes restrictions à cet égard étaient des éléments fondamentaux sur la base desquels on pouvait évaluer la fonction et l'intégrité d'un certificat. En outre, en y faisant référence, on tenait compte de la nécessité d'indiquer que les certificats pouvaient remplir diverses fonctions. Il a donc été proposé d'inclure une telle référence entre crochets dans un nouvel alinéa f), en vue d'un examen plus approfondi de la question par le Groupe de travail. Sous réserve de ce changement, le Groupe de travail a approuvé l'alinéa d) quant au fond.

Alinéa e)

130. Il a été généralement convenu que la signature de l'autorité de certification constituait l'un des éléments essentiels d'un certificat, mais les avis ont divergé quant à la question de savoir si cette signature devait être numérique. Selon un avis, cela était nécessaire pour assurer l'intégrité du certificat. Selon un autre avis, si la signature de l'autorité de certification était cryptographique, les parties qui s'y fiaient pourraient ne pas être en mesure de déterminer qu'il s'agissait de la signature d'une autorité de certification donnée, indiquant son intention d'être liée par le certificat. Il a été déclaré en outre que si la signature de l'autorité de certification ne résultait pas d'une procédure transparente, le certificat pourrait ne pas être valide. Le Groupe de travail a convenu qu'il était nécessaire de veiller à ce que la signature de l'autorité de certification soit sûre et la procédure transparente. Il a donc été décidé de conserver le mot "numériquement" en enlevant les crochets et d'ajouter les mots "ou sécurisé de toute autre manière" afin de tenir compte des craintes exprimées concernant le terme "numériquement".

Nouvel alinéa g)

131. Il a été proposé d'ajouter à la liste des éléments minima d'un certificat les algorithmes appliqués par l'autorité de certification. A l'appui de cette suggestion, il a été déclaré que les algorithmes étaient essentiels pour assurer l'identification du signataire et l'intégrité du message de données. À l'encontre de cette suggestion, on a fait valoir que, s'il était nécessaire d'inclure les algorithmes appliqués pour assurer la validité du certificat, l'autorité de certification pourrait dégager sa responsabilité en ne les incluant pas dans le certificat. Il était certes nécessaire d'assurer l'intégrité des données mais on pourrait y parvenir de façon plus satisfaisante en incluant l'élément intégrité des données dans la définition de la signature numérique. Selon un avis contraire, en omettant d'inclure les algorithmes appliqués dans le certificat, l'autorité de certification serait tenue responsable pour l'émission d'un certificat non valide. Après un débat, le Groupe de travail a décidé d'inclure entre crochets une référence aux algorithmes appliqués dans le projet d'article 8 en vue d'un examen plus approfondi de la question à une session future.

Article 9. Déclaration relative aux pratiques d'authentification

132. Le texte de l'article 9 examiné par le Groupe de travail était le suivant :

> "Aux fins des présentes Règles, les termes "déclaration relative aux pratiques d'authentification" désignent une déclaration publiée par une autorité de certification, qui indique les pratiques employées par cette autorité pour émettre et traiter de toute autre manière les certificats."

133. Le Groupe de travail a noté que le projet d'article 9 portait sur un certain nombre de questions traitées dans d'autres dispositions des Règles uniformes, par exemple la question des garanties données au moment de l'émission d'un certificat (projet d'article 10) et celle de la responsabilité de l'autorité de certification (projet d'article 12), et a décidé de reporter l'examen de cet article jusqu'à ce qu'il ait terminé l'examen des Règles uniformes.

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

134. Le texte du projet d'article 10 examiné par le Groupe de travail était le suivant :

"Variante A

1. Lorsqu'elle émet un certificat, une autorité de certification garantit à toute personne qui se fie raisonnablement à ce certificat, ou à une signature numérique vérifiable par la clef publique qui y est indiquée :

a) qu'elle s'est conformée à toutes les conditions applicables prévues dans les présentes Règles pour l'émission du certificat et, si elle a publié le certificat ou l'a mis de toute autre manière à la disposition de cette personne, que le détenteur désigné dans le certificat [et possédant légitimement la clef privée correspondante] l'a accepté;

b) que le détenteur désigné dans le certificat détient [légitimement] la clef privée correspondant à la clef publique indiquée dans le certificat;

c) que la clef publique et la clef privée du détenteur constituent une paire opérationnelle;

d) que toutes les informations données dans le certificat sont exactes à la date de son émission, sauf si l'autorité de certification a déclaré dans le certificat [ou fait savoir par incorporation par référence dans le certificat] que l'exactitude de certaines informations n'est pas confirmée; et

e) qu'à la connaissance de l'autorité de certification, n'a été omis du certificat aucun fait matériel connu qui, s'il était connu, compromettrait la fiabilité des garanties ci-dessus.

2. Sous réserve du paragraphe 1, l'autorité de certification qui émet un certificat garantit à toute personne qui se fie raisonnablement à ce certificat, ou à une signature numérique vérifiable par la clef publique qui y est indiquée, qu'elle a émis le certificat conformément à toute déclaration applicable relative aux pratiques d'authentification [incorporée par référence dans le certificat, ou] dont la personne se fiant au certificat a été avisée.

Variante B

1. Lorsqu'elle émet un certificat, l'autorité de certification garantit au détenteur, et à toute personne se fiant aux informations figurant dans le certificat[, de bonne foi et] pendant la période d'effet du certificat :

a) qu'elle a [traité] [approuvé] [émis] le certificat et le gérera et l'annulera, le cas échéant, conformément :

i) aux présentes Règles;

ii) à toute autre loi applicable régissant l'émission du certificat; et

iii) à toute déclaration applicable relative aux pratiques d'authentification figurant ou incorporée par référence dans le certificat, ou dont la personne a été avisée, le cas échéant;

b) qu'elle a vérifié l'identité du détenteur dans la mesure indiquée dans le certificat ou dans toute déclaration applicable relative aux pratiques d'authentification ou, en l'absence d'une telle déclaration, qu'elle a vérifié l'identité du détenteur de manière fiable;

c) qu'elle a vérifié que la personne demandant le certificat détient la clef privée correspondant à la clef publique indiquée dans le certificat;

d) qu'à sa connaissance, sous réserve de ce qui est stipulé dans le certificat ou toute déclaration applicable relative aux pratiques d'authentification, toutes les autres informations figurant dans le certificat sont exactes à la date d'émission dudit certificat;

e) que, si elle a publié le certificat, le détenteur qui y est désigné l'a accepté.

[2. Si une autorité de certification a émis le certificat conformément aux lois d'une autre juridiction, elle donne également, le cas échéant, toutes les garanties applicables en vertu de la loi régissant la délivrance.]"

135. Il a été proposé de remplacer le titre du projet d'article par un libellé tel que "procédure d'émission d'un certificat". On a noté d'emblée que le projet d'article 10, qui établissait une norme par rapport à laquelle apprécier la responsabilité de l'autorité de certification, était étroitement lié au projet d'article 12, qui prévoyait la sanction par rapport à cette norme. Le Groupe de travail, se fondant sur la variante A, a concentré son attention sur la question de savoir si les garanties énumérées aux alinéas a) à e) du paragraphe 1 devaient être considérées comme des conditions impératives (c'est-à-dire des normes minimales auxquelles les parties ne pouvaient déroger par convention) ou bien comme des règles "par défaut". Quant au sens de ces "règles par défaut" possibles, elles ont été décrites, à divers moments du débat, comme des règles "comblant un vide" (c'est-à-dire des règles contraignantes uniquement en l'absence d'une convention contraire) ou comme des règles à appliquer seulement lorsque n'existait aucun contrat entre les parties.

136. À l'appui de l'option de la règle par défaut, on a avancé les arguments suivants : une règle souple était nécessaire pour tenir compte de l'évolution future de la technologie; imposer en matière de responsabilité une norme rigoureuse aux autorités de certification ne ferait qu'entraver le développement de l'industrie, tout en encourageant l'entrée sur le marché d'autorités de certification moins fiables; l'imposition de normes minimales pour des certificats à sécurité relativement faible pourrait limiter l'utilisation générale de ces certificats dans divers contextes importants; en général, pour ce qui est du contenu du certificat, il ne faudrait déterminer les attentes du détenteur du certificat et des parties qui s'y fient que par référence à ce que l'autorité de certification s'est engagée, dans sa déclaration relative aux pratiques d'authentification ou de toute autre manière, à garantir dans le certificat; et l'adoption de normes impératives minimales pour les certificats pourrait isoler les Règles uniformes de la pratique commerciale sur les principaux marchés. En d'autres termes, il faudrait déterminer la responsabilité de l'autorité de certification uniquement par référence aux obligations que cette dernière avait acceptées de contracter. Une telle approche offrait, a-t-on déclaré, la souplesse nécessaire pour prendre en considération la grande diversité des certificats proposés sur le marché. Il a été suggéré de reformuler comme suit le projet d'article 10, qui pourrait être fusionné avec le projet d'article 12 :

"1. L'autorité de certification énonce explicitement dans le certificat le type de service qu'elle fournit. Si l'obligation de l'autorité de certification n'est pas exprimée dans le certificat, l'autorité de certification est supposée avoir garanti l'identité du détenteur de la clef.

2. Si l'autorité de certification n'a pas fourni les services énoncés dans le certificat ou a garanti de façon négligente l'identité du détenteur de la clef, elle est responsable envers la partie s'étant fiée au certificat du préjudice subi.

3. L'autorité de certification peut limiter son obligation de verser des dommages-intérêts en incluant dans le certificat des dénis de responsabilité explicites.

4. Le présent article s'entend sous réserve de toute convention contraire entre l'autorité de certification et la partie se fiant au certificat."

137. À l'encontre de cette proposition, on a fait valoir que, dans certains systèmes juridiques, il y aurait incompatibilité entre la définition de critères pour la reconnaissance du statut juridique du certificat, d'une part, et la possibilité de recourir à un déni de responsabilité général afin de faire abstraction des éléments essentiels de ces critères. On a également déclaré qu'il n'existerait en général aucune relation contractuelle entre la partie se fiant au certificat et l'autorité de certification. À cet égard, il pourrait être utile, selon une opinion, de préciser si la notion de "partie se fiant au certificat" devait englober le détenteur de la paire de clefs indiqué dans le certificat. On a aussi fait observer que les certificats pourraient être de taille très réduite et qu'il serait donc difficile d'y inclure des dénis de responsabilité explicites. En réponse à cet argument, il a été déclaré que l'établissement d'une norme minimale concernant le contenu supposé d'un certificat répondait à la nécessité de réduire la taille du certificat lui-même.

138. À l'appui du maintien du paragraphe 1 comme norme minimale à laquelle les parties ne devraient pas être autorisées à déroger par convention privée, il a été rappelé que le Groupe de travail, à sa session précédente, avait pris une décision explicite sur ce point. En outre, l'établissement de conditions minimales non seulement protégerait le détenteur du certificat et d'autres parties se fiant à ce certificat, mais renforcerait également la fiabilité et l'acceptabilité commerciale des mécanismes de signature numérique, ce qui serait aussi dans l'intérêt des autorités de certification. En réponse à une objection selon laquelle l'établissement d'une norme minimale imposerait de lourdes obligations aux autorités de certification, on a fait observer que le projet d'article 10 n'avait pas pour objectif d'imposer quelque obligation que ce soit à l'autorité de certification mais simplement de définir un régime juridique particulier pour certains certificats qui, en satisfaisant à certaines conditions, pouvaient bénéficier d'un statut juridique particulier. Une autorité de certification demeurerait libre d'offrir des certificats de moindre qualité qui, cependant, ne produiraient pas les mêmes effets juridiques. Les tenants du maintien d'une norme minimale ont reconnu que les mécanismes limitant la responsabilité au titre du projet d'article 12 compenseraient dûment l'acceptation par les autorités de certification de règles impératives au titre du projet d'article 10. Un parallèle a été établi à cet égard avec le régime de responsabilité qui existait dans l'industrie des transports maritimes où l'interaction de forces du marché sans entraves avait par le passé engendré une incertitude générale d'une ampleur telle que les parties avaient été découragées de s'engager dans des transactions maritimes et qu'il avait été nécessaire d'élaborer des instruments internationaux dans ce domaine, tels que les Règles de La Haye.

139. On a fait valoir qu'en limitant la portée de la disposition par la définition d'un type particulier de certificat (par exemple certificat d'identité émis pour les transactions portant sur des sommes élevées) auquel s'appliquerait le projet d'article 10, on pourrait peut-être rendre la formulation de normes impératives plus acceptable. Une autre solution serait d'adopter une norme impérative restreinte, ce qui contribuerait peut-être faire accepter l'application de l'article 10 à une catégorie plus large de certificats. Pour combiner ces deux suggestions, il a été proposé de ne retenir comme norme minimale que les alinéas a), d) et e) du paragraphe 1. La prise en compte de cette proposition dans la suite du débat a bénéficié d'un appui général mais il a aussi été estimé qu'il fallait clarifier davantage un certain nombre de points.

140. L'un d'entre eux était la catégorie exacte de certificats auxquels s'appliquerait cette norme impérative restreinte. Selon un vis, elle ne devrait s'appliquer qu'à une catégorie limitée de certificats d'identité offrant une sécurité maximale. L'avis selon lequel une norme plus stricte serait nécessaire pour les certificats auxquels

s'attacherait un degré élevé de certitude juridique a bénéficié d'un appui. En particulier, si le certificat avait pour objet de créer une signature juridiquement contraignante, il faudrait prévoir des assurances supplémentaires quant au lien entre le certificat et l'identité du détenteur de la paire de clefs. Toutefois, on a aussi appuyé l'avis selon lequel la norme minimale proposée aux alinéas a), d) et e) était si restreinte qu'elle pourrait s'appliquer à un large éventail de certificats.

141. Un autre point à clarifier était la compatibilité entre le texte proposé pour le paragraphe 1 et d'autres dispositions des Règles uniformes portant sur la fonction d'identification du certificat. On a rappelé que, pour les signatures numériques, la principale fonction du certificat était d'identifier le détenteur de la paire de clefs, raison pour laquelle il avait été proposé auparavant que le Groupe de travail concentre son attention sur la notion de certificat "d'identité". Si la norme restreinte proposée était adoptée, l'autorité de certification ne donnerait plus aucune garantie quant à l'identité du détenteur, mais se contenterait de garantir que la procédure qu'elle avait définie avait été suivie. On a certes reconnu qu'une telle procédure pourrait indirectement conduire à l'identification du détenteur de la paire de clefs, mais il a été suggéré que l'on envisage de conserver la teneur des alinéas b) et c) traitant de l'identification directe (ou "irréfutable") du détenteur, dans les Règles uniformes, en l'insérant éventuellement dans le projet d'article 2.

142. Bien que l'on ait fait valoir que les alinéas a), d) et e) énonçaient une norme pour les certificats d'identité, il a généralement été convenu après un échange de vues, qu'une telle norme restreinte pourrait s'appliquer de manière plus appropriée à un large éventail de certificats. Il a aussi été convenu qu'il faudrait réfléchir davantage à la manière de prendre en considération la fonction d'identification, soit dans le projet d'article 10, soit avant, comme fonction essentielle d'une catégorie plus limitée de certificats pour lesquels il fallait un niveau de fiabilité juridique élevé. De l'avis général, la question devrait être examinée de façon plus approfondie à une prochaine session. Entre-temps, les alinéas a), b) et c) seraient maintenus au paragraphe 1 et les alinéas b) et c) seraient placés entre crochets. Selon un avis, il serait peut-être indiqué de placer entre crochets dans le paragraphe 1 un libellé tiré du paragraphe 1 b) de la variante B aux fins d'examen par le Groupe de travail à une prochaine session. S'agissant de l'alinéa d), il a été largement estimé que la mention d'un éventuel déni de responsabilité de l'autorité de certification quant à l'exactitude de l'information contenue dans le certificat ne serait acceptable que si les alinéas b) et c) étaient inclus dans le paragraphe 1.

143. S'agissant du paragraphe 2, il fallait, de l'avis général, conserver le principe selon lequel une autorité de certification devrait respecter les engagements qu'elle avait pris dans sa déclaration relative aux pratiques d'authentification.

144. Pour tenir compte de l'échange de vues susmentionné, on a proposé la version révisée suivante du projet d'article 10 :

"Lorsqu'un certificat est émis, il est présumé que :

a) la personne ou l'entité émettant le certificat s'est conformée à toutes les conditions applicables prévues dans les présentes Règles;

[b) au moment de l'émission du certificat, la clef privée est celle du détenteur et correspond à la clef publique indiquée dans le certificat;]

[c) la clef publique et la clef privée du détenteur constituent une paire de clefs opérationnelle;]

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

e) à la connaissance de l'autorité de certification, il n'a été omis du certificat aucun fait matériel connu qui, s'il était connu, compromettrait la fiabilité de l'information contenue dans le certificat; et

[f) si l'autorité de certification a publié une déclaration relative aux pratiques d'authentification, le certificat a été émis par l'autorité de certification conformément à cette déclaration.]"

145. Après un échange de vues, le Groupe de travail a demandé au secrétariat d'établir une version révisée du projet d'article 10, en prévoyant des variantes possibles, pour tenir compte du débat susmentionné.

Article 11. Responsabilité contractuelle

146. Le texte du projet d'article 11 examiné par le Groupe de travail était le suivant :

"1. Entre une autorité de certification émettant un certificat et le détenteur de ce certificat [ou toute autre partie ayant une relation contractuelle avec l'autorité de certification], les droits et obligations des parties sont déterminés par convention.

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

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

147. Il a été noté que le paragraphe 1 énonçait à nouveau le principe de l'autonomie des parties concernant le régime de responsabilité applicable à l'autorité de certification. Il a été noté en outre que le paragraphe 2 traitait la question des clauses d'exonération, qui étaient généralement déclarées admissibles, à deux exceptions près. La première découlait d'une référence au projet d'article 10, qui visait à établir une norme minimale à laquelle les autorités de certification ne devaient pas être autorisées à déroger. La seconde, qui était inspirée des principes d'UNIDROIT relatifs aux contrats de commerce international (art. 7.1.6), tentait d'établir une norme uniforme pour l'évaluation de l'acceptabilité générale des clauses d'exonération. Il a été noté par ailleurs que le paragraphe 3 traitait des cas où une faute intentionnelle de l'autorité de certification ou de ses agents entraînerait une perte ou un autre préjudice (inspiré de l'article 18 de la Loi type de la CNUDCI sur les virements internationaux).

148. Le Groupe de travail a examiné tout d'abord la question de savoir s'il fallait conserver le projet d'article 11 dans les Règles uniformes. À l'appui de sa suppression, on a fait valoir qu'il portait sur des questions qui seraient mieux traitées dans le contrat et dans la loi applicable. On a fait en particulier les observations suivantes : le paragraphe 1 était redondant car il reprenait uniquement le principe de l'autonomie des parties, déjà énoncé à l'article 4 de la Loi type; d'autre part, les paragraphes 2 et 3 empiétaient sur la législation nationale pour des questions pouvant ne pas se prêter à une unification. On a fait observer par ailleurs que le projet d'article 10 couvrait suffisamment cette question. On a estimé que le fait de traiter les questions de la responsabilité contractuelle dans le contrat et dans la loi applicable en dehors des Règles uniformes était une alternative acceptable, mais selon l'avis qui a prévalu, il valait la peine de tenter d'établir une certaine unification sur cette question importante.

149. Pour ce qui était de la manière de s'y prendre, un certain nombre de suggestions ont été formulées, tendant notamment à conserver le projet d'article 11 sous sa forme actuelle. À l'appui de cette suggestion, on a fait valoir que le paragraphe 1 semblait peut-être énoncer une évidence, mais que le paragraphe 2 présentait le principe très

important selon lequel il était impossible de se soustraire aux obligations essentielles du contrat par le biais de clauses exonératoires. En outre, on a fait remarquer que le paragraphe 3 était primordial et portait non seulement sur les relations contractuelles mais également sur les relations non contractuelles.

150. Selon une autre proposition, il convenait de mentionner au paragraphe 1 l'impossibilité pour les parties de convenir de conditions "manifestement inéquitables" et de supprimer les paragraphes 2 et 3. La suppression des paragraphes 2 et 3 a bénéficié d'un certain appui mais plusieurs arguments ont été avancés à l'encontre de cette proposition, notamment les suivants : l'emploi des termes "manifestement inéquitables" était inapproprié car inconnu dans de nombreux systèmes juridiques; la protection de la partie la plus faible, qui était le but recherché, devrait être assurée par d'autres textes (par exemple, la loi sur la protection des consommateurs); et la suppression des paragraphes 2 et 3 pourrait conduire, sans que cela soit le but recherché, à autoriser les parties à rendre nul l'effet essentiel du contrat ou à s'exonérer de leur responsabilité en cas de faute intentionnelle.

151. Il a été proposé, dans le même ordre d'idée, d'insérer après les mots "obligations des parties", au paragraphe 1, les mots "et toute restriction à cet égard" et à la fin de la phrase les mots "sous réserve de la loi applicable", et de supprimer les paragraphes 2 et 3. À l'appui de cette proposition, on a déclaré qu'une telle approche donnerait une déclaration générale acceptable, fondée sur l'autonomie des parties et la loi applicable. On a fait observer, cependant, qu'elle ne permettrait aucune unification,.

152. Il a aussi été proposé de remplacer le projet d'article 11 par une disposition énonçant que les normes par rapport auxquelles l'autorité de certification devrait être tenue responsable devraient être celles qui étaient énoncées dans la déclaration relative aux pratiques d'authentification. À l'encontre de cette proposition, on a fait valoir qu'une telle disposition remplacerait à la fois le contrat et les normes minimales énoncées au projet d'article 10 comme point de référence pour apprécier la responsabilité de l'autorité de certification. Selon un avis, cependant, cette proposition pourrait offrir une règle appropriée pour les certificats offrant une faible sécurité, et auxquels les normes minimales prévues au projet d'article 10 ne s'appliqueraient pas.

153. Lors du débat, un certain nombre de suggestions ont été faites quant à la forme. Pour ce qui est du paragraphe 1, on a fait valoir que l'expression entre crochets "toute autre partie" était trop générale et trop vague et devrait être remplacée par les termes "toute autre partie se fiant au certificat". Selon une autre proposition, le paragraphe 1 devrait être modifié pour préciser qu'il n'avait pour objet de baser la relation entre les parties exclusivement sur une convention, ce qui enlèverait tout sens à l'exception au droit des parties de convenir de clauses exonératoires de responsabilité aux paragraphes 2 et 3. S'agissant du paragraphe 2, il a été proposé d'ajouter après le mot "préjudice" les mots "lié au certificat" et de supprimer le reste de la première phrase.

154. Au terme d'un échange de vues, le Groupe de travail n'a pu parvenir à un accord sur la formulation du projet d'article 11 et a prié le secrétariat d'élaborer des variantes tenant compte des diverses vues exprimées, aux fins d'examen à une future session.

Article 12. Responsabilité de l'autorité de certification envers les parties se fiant aux certificats

155. Le texte du projet d'article 12 examiné par le Groupe de travail était le suivant :

> "1. Sauf convention contraire, une autorité de certification qui émet un certificat est responsable envers toute personne se fiant raisonnablement à ce certificat dans les cas suivants :
>
> a) [rupture de la garantie au titre de l'article 10] [négligence par fausse présentation de l'exactitude des renseignements donnés dans le certificat];

b) enregistrement de l'annulation d'un certificat promptement après réception de la notification de l'annulation dudit certificat; et

c) [conséquences de la non] [négligence dans l'] application :
i) de toute procédure énoncée dans la déclaration relative aux pratiques d'authentification publiée par l'autorité de certification; ou

ii) de toute procédure énoncée dans la loi applicable.

2. Nonobstant le paragraphe 1, une autorité de certification n'est pas responsable si elle peut démontrer qu'elle-même ou ses agents ont pris toutes les mesures nécessaires pour éviter des erreurs dans le certificat ou qu'il était impossible, à elle-même ou à ses agents, de prendre de telles mesures.

3. Nonobstant le paragraphe 1, une autorité de certification peut limiter, dans le certificat [ou de toute autre manière], l'objet dudit certificat. L'autorité de certification n'est pas tenue responsable du préjudice découlant de l'utilisation du certificat pour tout autre objet.

4. Nonobstant le paragraphe 1, une autorité de certification peut limiter, dans le certificat [ou de toute autre manière], la valeur des opérations pour lesquelles le certificat est valide. Elle n'est pas tenue responsable du préjudice dépassant cette limite."

Observations générales

156. Un large appui a été exprimé en faveur d'une disposition traitant de la question de la responsabilité de l'autorité de certification envers les parties se fiant aux certificats comme le faisait le projet d'article 12. Toutefois, on a estimé en général que la portée d'une telle disposition devrait être limitée aux cas dans lesquels l'autorité de certification garantissait l'identité du détenteur de la clef et l'intégrité des messages de données signés par ce dernier. Une telle approche pouvait faciliter certaines pratiques où de strictes normes de sécurité étaient nécessaires, sans pour autant affecter d'autres pratiques où de telles normes en matière de sécurité et de responsabilité ne conviendraient peut-être pas.

157. Cependant, certains doutes ont été exprimés sur la question de savoir si un régime de responsabilité particulier pouvait ou devait être établi. On a indiqué que l'adoption d'un tel régime pourrait nuire à certaines pratiques de certification s'il ne s'accompagnait pas d'une quantification raisonnable des risques associés à la prestation des services de certification, dans la mesure où les autorités de certification seraient exposées à des risques contre lesquels elles ne pourraient s'assurer. En outre, on a fait observer qu'il ne serait peut-être pas nécessaire, étant entendu qu'en l'absence d'un régime spécifique, les principes généraux de la législation sur les délits civils s'appliqueraient. On a indiqué, toutefois, que dans certaines juridictions où la responsabilité des autorités de certification n'était pas expressément réglementée, celles-ci ne seraient pas en principe responsables envers les parties se fiant aux certificats. Par ailleurs, on a fait valoir qu'il ne serait pas judicieux d'abandonner cette question à la loi applicable pour un certain nombre de raisons, notamment les suivantes : les incertitudes existant dans de nombreuses juridictions pourraient avoir des conséquences négatives sur le développement du commerce électronique; l'absence de toute responsabilité pourrait avoir pour effet involontaire d'empêcher les parties de faire appel aux services des autorités de certification; la détermination de la loi applicable soulèverait des questions très difficiles à résoudre. S'agissant de la forme du produit des travaux, on a signalé qu'un régime de responsabilité uniforme pourrait être appliqué plus efficacement par une convention que par une loi type (voir par. 212 ci-après).

158. Après un échange de vues, le Groupe de travail a décidé que tout devait être mis en œuvre pour aborder la question de la responsabilité des autorités de certification envers les parties se fiant aux certificats dans les Règles uniformes et il a procédé à un examen détaillé du projet d'article 12. Il pourrait, a-t-on proposé, inclure dans

l'examen futur de ce projet d'article les questions de la nature et de la prévisibilité du préjudice subi par la partie se fiant au certificat.

Paragraphe 1

Chapeau

159. Différentes opinions ont été exprimées sur la question de savoir s'il convenait de maintenir les premiers mots du chapeau. Selon un avis, si le projet d'article 10 fixait des règles minimales auxquelles l'autorité de certification devait se conformer, il fallait supprimer les premiers mots du chapeau. Selon un autre avis, ces mots étaient utiles et il fallait les maintenir dans la mesure où ils permettaient aux parties de négocier leurs responsabilités. On a répondu que les parties ne pouvaient pas négocier, puisque le projet d'article 12 avait trait à la responsabilité extracontractuelle dans les cas où, en général, il n'y avait pas de convention. On a fait observer, toutefois, que les parties se fiant aux certificats dans des systèmes de communication fermés concluraient normalement une convention, sous une forme ou une autre, avec l'autorité de certification. En outre, on a indiqué que les conditions de la responsabilité négociées entre les autorités de certification et les détenteurs de clefs pourraient être incorporées dans les contrats passés entre les détenteurs de clefs et les parties se fiant aux certificats.

160. Selon l'avis qui a prévalu, les cas mentionnés étaient exceptionnels et ne devaient pas aller à l'encontre de l'objet principal du projet d'article 12 qui était de réglementer la responsabilité extracontractuelle des autorités de certification envers les tiers. On a donc proposé que la nécessité subsidiaire de tenir compte des conventions contraires entre les autorités de certification et leurs clients ou les parties se fiant aux certificats, lorsque de telles conventions existaient, fasse l'objet d'un libellé approprié à la fin du projet d'article 12.

Alinéas a) à c)

161. On a fait observer que le deuxième membre de phrase entre crochets aux alinéas a) et c) semblait renvoyer au principe de la responsabilité objective et devrait être supprimé. On a indiqué qu'il était à craindre que l'emploi de la notion de "fausse présentation" ("misrepresentation") ne soulève des difficultés car cette notion avait un sens précis dans certains système juridiques, mais elle était inconnue dans d'autres. Il a été proposé de remplacer ces termes par "fausse déclaration".

Paragraphe 2

162. Différentes opinions ont été exprimées sur la question de savoir si la charge de la preuve en cas de négligence devait être imputée à l'autorité de certification ou à la partie se fiant au certificat. Selon un avis, la charge de la preuve devait être imputée à la partie se fiant au certificat. À l'appui de cette thèse, on a fait valoir que cette partie pouvait prouver la négligence dans la mesure où il lui était facile d'établir si l'autorité de certification avait manifesté la diligence voulue aux termes du projet d'article 10. En outre, on a fait observer qu'il ne serait indiqué de renverser la charge de la preuve et de l'imputer à l'autorité de certification que si le Groupe de travail adoptait le principe de la responsabilité objective. Selon un autre avis, s'il convenait que la responsabilité soit fondée sur la négligence, la charge de la preuve devait être imputée à l'autorité de certification dans la mesure où cette dernière avait la maîtrise de toutes les preuves pertinentes. On a fait observer que cela serait le cas, en particulier, si le certificat mentionnait non l'identité du détenteur de la clef mais la procédure suivie par l'autorité de certification pour déterminer l'identité du détenteur de la clef.

Paragraphes 3 et 4

163. Un soutien a été exprimé en faveur du principe de la limitation de la responsabilité de l'autorité de certification énoncé aux paragraphes 3 et 4. Toutefois, selon un avis, ces limites de responsabilité ne convenaient que dans le

cas d'un régime fondé sur une responsabilité objective de l'autorité de certification, par opposition au régime de responsabilité fondé sur la négligence.

164. S'agissant des types de limites qui pouvaient être retenus, on a fait valoir qu'une limite monétaire par opération ne protégeait pas suffisamment les autorités de certification, en particulier dans le cas des certificats d'identité puisque, indépendamment de la limite de responsabilité, ces certificats pouvaient être utilisés plusieurs fois dans un très bref délai sans qu'il soit possible de déterminer si la limite de responsabilité avait été dépassée. Il a donc été proposé qu'une disposition introduisant une limite globale de responsabilité soit insérée dans le projet d'article 12 et qu'elle soit libellée comme suit : "Une autorité de certification peut, dans le certificat ou de toute autre manière, prévoir une limite de responsabilité pendant la durée de vie du certificat pour tous les incidents liés à la confiance, pour un montant égal à une valeur globale du certificat. L'autorité de certification n'est pas tenue responsable du préjudice dépassant cette limite globale, indépendamment du nombre de plaintes dont le certificat a fait l'objet". Selon un avis, toutefois, cette limite globale ne pouvait fonctionner puisqu'une partie se fiant au certificat n'aurait aucun moyen de savoir, en l'état actuel des applications technologiques, si une certaine limite avait été atteinte.

Propositions relatives à un nouveau projet d'article 12

165. Afin de répondre aux préoccupations exprimées ci-dessus, diverses propositions ont été faites présentant un nouveau libellé pour le projet d'article 12. Selon une proposition, ce projet d'article devrait être libellé comme suit :

> "1. Lorsqu'une autorité de certification émet un certificat, elle est responsable envers toute personne qui se fie raisonnablement au certificat, si elle fait preuve de négligence :
>
> a) en fournissant des informations contradictoires dans le certificat;
>
> b) en manquant à [notifier ou] publier l'annulation [ou la suspension] du certificat promptement après avoir pris conscience de la nécessité de l'annuler [ou de le suspendre] [; ou
>
> c) en manquant à suivre une procédure énoncée dans une déclaration relative aux pratiques en matière de certification qui a été publiée par l'autorité de certification et dont a été avisée la personne se fiant au certificat].
>
> 2. L'autorité de certification peut énoncer dans le certificat [ou ailleurs] une limitation quant à l'objet ou aux objets pour lesquels le certificat peut être utilisé et elle n'est pas responsable du préjudice subi du fait de l'utilisation du certificat pour tout autre objet.
>
> 3. L'autorité de certification peut énoncer dans le certificat [ou ailleurs] une limite quant à la valeur des opérations pour lesquelles le certificat est valide et elle n'est pas responsable du préjudice subi au-delà de cette limite.
>
> [4. Le paragraphe 1 du présent article ne s'applique pas si, et dans la mesure où, un accord entre l'autorité de certification et la personne se fiant au certificat comporte des conditions contraires.]"

166. Selon une autre proposition, le projet d'article 12 devrait être modifié comme suit :

> "1. À moins qu'elle ne prouve qu'elle-même ou ses agents ont pris toutes les mesures raisonnables pour éviter des erreurs dans le certificat, l'autorité de certification est responsable envers toute personne qui se fie raisonnablement à un certificat émis par elle dans les cas suivants :

[insérer les alinéas a) à c)]

2. Nonobstant les dispositions du paragraphe 1, il n'est pas raisonnable de se fier à un certificat dans la mesure où cela est contraire aux informations contenues dans ledit certificat."

167. La première proposition a suscité un certain intérêt, mais le Groupe de travail a axé sa discussion sur la deuxième. Il a été déclaré que le paragraphe 1 avait pour objet d'établir la responsabilité en cas d'erreur dans le certificat, sous réserve du principe de la "confiance raisonnable", en évitant toute référence aux garanties données et à la négligence. En outre, il a été noté que le paragraphe 2 avait pour objet de permettre à l'autorité de certification d'énoncer dans le certificat les critères à l'aune desquels le caractère raisonnable de la confiance pourrait être vérifié. Il a été expliqué que le paragraphe 2 ne visait pas à énoncer une liste exhaustive de tous les cas où la confiance ne serait pas raisonnable. Les paragraphes 1 et 2 ont été jugés dans l'ensemble acceptables, en tant que base d'une discussion ultérieure, mais diverses préoccupations et suggestions ont été émises.

Nouveau paragraphe 1

168. Selon un avis, il serait quasi impossible à une autorité de certification, dans la pratique, de prendre "toutes les mesures raisonnables" de manière rentable et en temps utile. Afin de répondre à cette préoccupation, plusieurs suggestions ont été faites. Selon un avis, il faudrait remplacer le mot "toutes" par le mot "commercialement". À l'appui de cet avis, il a été déclaré qu'une référence aux "mesures commercialement raisonnables" engloberait ce qui était possible dans des circonstances particulières. En outre, une telle référence serait conforme à la terminologie utilisée dans d'autres textes de la CNUDCI (par exemple, l'article 5-2 a) de la Loi type de la CNUDCI sur les virements internationaux). Selon un avis contraire, cette suggestion pourrait être source d'incertitude, car il n'existait pas d'interprétation universelle de ce qui était "commercialement raisonnable". Selon un autre avis, le mot "toutes" devrait être purement et simplement supprimé. On s'est également opposé à cette suggestion, au motif que cela risquerait d'avoir pour conséquence d'assouplir de manière inappropriée la norme de diligence que devaient respecter les autorités de certification. Selon une autre suggestion encore, il faudrait retenir le libellé utilisé à l'article 7-1 b) de la Loi type dans le nouveau paragraphe 1.

169. On a craint également que le nouveau paragraphe 1 ne traite pas des erreurs faites par l'autorité de certification lors de l'émission du certificat. Afin de répondre à cette préoccupation, il a été proposé d'ajouter après le mot "certificat", au nouveau paragraphe 1, les mots "ou dans son émission". Il a été déclaré que les informations contenues dans une liste d'annulation du certificat ou dans une liste similaire seraient également régies par le paragraphe 2.

170. Il a été convenu, qu'en attendant que soit déterminée la question de la fonction des déclarations relatives aux pratiques en matière de certification, l'alinéa c) serait placé entre crochets.

Nouveau paragraphe 2

171. Pour ce qui est de la rédaction, il a été proposé de supprimer le premier membre de phrase et d'insérer les mots "Sous réserve des dispositions du paragraphe 2" au début du nouveau paragraphe 1. On a craint que le nouveau paragraphe 2 n'ait pour résultat non souhaité de limiter à l'excès les motifs pour lesquels le caractère raisonnable de la confiance en le certificat pourrait être mis en doute. Selon une autre préoccupation, le nouveau paragraphe 2 ne traitait peut-être pas du cas où l'on pourrait se fier au certificat dans une opération de valeur excessive, car cette valeur n'était peut-être pas englobée dans le terme "informations". Afin de répondre à cette préoccupation, il a été proposé que les paragraphes 3 et 4 du projet d'article 12 constituent des exemples des cas où la confiance ne serait pas raisonnable. Dans la même veine, il a été proposé que d'autres exemples similaires soient donnés à propos, par exemple, des cas où l'autorité de certification pourrait indiquer dans le certificat quelles parties ou quels types de parties désignés pourraient se fier au certificat. En outre, il a été proposé que l'autorité de certification ne soit pas

habilitée à invoquer de limites de la responsabilité si le préjudice résultait d'un comportement intentionnel ou téméraire de sa part.

172. Selon une autre préoccupation, en faisant référence aux informations "contenues" dans le certificat, le nouveau paragraphe 2 risquerait d'avoir pour résultat d'augmenter de manière inappropriée le volume des informations à inclure dans un certificat. Afin de répondre à cette préoccupation, il a été proposé d'autoriser l'incorporation par référence de ces informations dans le certificat. On s'est opposé à cette suggestion au motif qu'il serait injuste de soumettre les droits de tiers à des conditions incorporées dans un accord entre l'autorité de certification et le détenteur de la clef, accord dont les conditions ne seraient sans doute pas aisément accessibles aux tiers.

173. Après un débat, le Groupe de travail a décidé de modifier comme suit le projet d'article 12 :

"1. Sous réserve des dispositions du paragraphe 2, à moins qu'elle ne prouve qu'elle ou ses agents ont pris toutes les mesures [raisonnables] [commercialement raisonnables] [qui étaient appropriées compte tenu de la fin pour laquelle le certificat avait été émis, au vu de toutes les circonstances,] pour éviter des erreurs dans le certificat [ou dans son émission], l'autorité de certification est responsable envers toute personne se fiant raisonnablement à un certificat émis par elle :

a) des erreurs dans le certificat; [ou]

b) de l'enregistrement de l'annulation du certificat promptement après réception de l'avis d'annulation du certificat[; ou

c) des conséquences imputables au non-respect :

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

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

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

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

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

c) [...].]"

Selon un avis, le projet d'article 12 devrait s'appliquer uniquement aux autorités de certification émettant des certificats d'identification.

Articles 13 à 16

174. Faute de temps, le Groupe de travail a reporté l'examen des projets d'articles 13 à 16 à une future session. Selon une opinion, ces projets d'articles ne devraient s'appliquer qu'aux autorités de certification émettant des certificats d'identification. Selon une autre opinion, le Groupe de travail devrait examiner la question de savoir si les Règles uniformes devraient s'appliquer uniquement aux certificats d'identification ou à tout autre type de certificat.

CHAPITRE IV. RECONNAISSANCE DES SIGNATURES ÉLECTRONIQUES ÉTRANGÈRES

Article 17. Autorités de certification étrangères offrant des services en vertu des présentes Règles

175. Le texte du projet d'article 17 examiné par le Groupe de travail était le suivant :

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

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

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

Variante B Le ... [*l'État adoptant indique l'organe ou l'autorité de certification ayant pouvoir d'établir des règles concernant l'approbation des certificats étrangers]* est autorisé à approuver les certificats étrangers et à établir des règles spécifiques régissant cette approbation."

Observations générales

176. S'agissant du titre du chapitre IV, on a fait observer que la référence à la reconnaissance des signatures électroniques étrangères n'était pas appropriée, dans la mesure où ce chapitre avait trait à la fourniture de services par des autorités de certification étrangères (à savoir le projet d'article 17), à l'approbation des certificats étrangers par les autorités de certification nationales (projet d'article 18) et à la reconnaissance des certificats étrangers (projet d'article 19). Le Groupe de travail a brièvement passé en revue un certain nombre de propositions qui avaient été faites pour mieux cibler dans le titre du chapitre la question traitée (par exemple, "certification transfrontière des certificats", "reconnaissance des signatures électroniques et des certificats", "reconnaissance des autorités de certification et des certificats étrangers"). Toutefois, il a été convenu d'une manière générale que l'examen d'un titre approprié pour le chapitre IV devrait être reporté, après que le Groupe de travail aurait étudié plus en détail les effets juridiques des certificats.

177. S'agissant des deux variantes proposées dans le projet d'article 17, on a estimé en général que la variante B, qui laissait à un organe indiqué par l'État adoptant le soin d'établir des règles concernant l'approbation des certificats étrangers, n'offrait pas une base satisfaisante pour les Règles uniformes. Il a été convenu que la variante B devrait être supprimée et que le Groupe de travail devrait faire porter ses délibérations sur la variante A.

Champ d'application du projet d'article 17

178. On a fait observer que l'objectif du projet d'article 17 était double. Premièrement, il reconnaissait le droit d'une autorité de certification étrangère de s'établir localement, dans les conditions qui y étaient mentionnées; deuxièmement, il donnait aux autorités de certification étrangères le droit de fournir des services dans l'État adoptant sans avoir une implantation locale. En tant que tel, il visait des questions de politique commerciale, à savoir la mesure dans laquelle l'État adoptant lèverait les restrictions à l'établissement d'autorités de certification étrangères et à la fourniture de services par ces autorités. Il a été proposé que le Groupe de travail s'emploie plutôt à élaborer des dispositions types concernant les effets juridiques des certificats étrangers et la relation entre les détenteurs de

certificats et les autorités de certification. Plusieurs interventions sont venues conforter ce point de vue. On a estimé que les questions de politique commerciale relevaient de la compétence d'autres instances et qu'il ne serait pas opportun de les aborder dans le projet de Règles uniformes.

179. En réponse aux vues exprimées, on a fait observer qu'en autorisant des entités étrangères à s'établir comme autorités de certification, le projet d'article 17 énonçait simplement le principe selon lequel ces entités ne devaient pas faire l'objet d'une discrimination, à condition qu'elles satisfassent aux normes applicables aux autorités de certification locales. Ce principe a été jugé particulièrement utile pour les autorités de certification, dans la mesure où celles-ci pouvaient mener leur activité sans avoir nécessairement une implantation matérielle ou un autre type d'établissement dans le pays où elles menaient cette activité. On a en outre indiqué que la Loi type elle-même abordait un certain nombre de questions transfrontières dont on pouvait penser qu'elles soulevaient des problèmes de politique commerciale.

180. Ayant entendu les divers avis exprimés, et pour faire progresser l'examen des Règles uniformes, le Groupe de travail a examiné un certain nombre d'amendements concernant le projet d'article 17, sans préjudice des réserves qui avaient été formulées quant au fond de ce projet d'article.

Paragraphe 1

181. On a demandé si le paragraphe 1 prévoyait uniquement la reconnaissance des autorités de certification qui menaient leur activité conformément à une approbation donnée par un organe ou un organisme public de l'État adoptant. En réponse à cette question, on a fait observer que, sous sa forme actuelle, le paragraphe 1 n'abordait pas la question de savoir si une autorité de certification avait besoin de l'approbation des pouvoirs publics dans l'État adoptant. Toutefois, on a également signalé qu'une disposition comme le projet d'article 17 devait se fonder sur un régime d'agrément, conformément aux prescriptions d'ordre législatif.

182. Selon un avis, certaines des difficultés qu'avait soulevées le paragraphe 1 découlaient du fait que cette disposition semblait faire une trop large place à la reconnaissance de l'autorité de certification proprement dite par rapport à l'aptitude de l'autorité de certification à émettre des certificats qui seraient utilisés dans l'État adoptant. En outre, le membre de phrase "satisfont aux mêmes normes objectives et suivent les mêmes procédures que les entités et personnes locales pouvant devenir des autorités de certification" risquait de faire obstacle à l'application de nouvelles technologies, dans la mesure où l'on pouvait penser que cette disposition donnait des moyens d'interdire la reconnaissance des autorités de certification étrangères qui suivraient des procédures technologiquement plus avancées que celles employées dans l'État adoptant. Au lieu de la formulation actuelle, on a estimé qu'il serait préférable de faire référence à des "conditions objectives" auxquelles devraient satisfaire les autorités de certification dans l'État adoptant. On devrait également mettre les mots "et suivent les mêmes procédures" entre crochets.

183. S'agissant des conditions auxquelles devait satisfaire une autorité de certification étrangère, on a fait observer que l'objet du projet de paragraphe 1 était de faire en sorte que ces conditions soient essentiellement les mêmes que celles s'appliquant aux autorités de certification nationales. Il a donc été proposé de modifier le paragraphe 1 de manière à ce que la reconnaissance des autorités de certification étrangères soit soumise aux lois de l'État adoptant. Les questions relatives à la définition des normes auxquelles devrait se conformer l'autorité de certification étrangère pourraient être examinées ultérieurement par le Groupe de travail. Une telle modification permettrait en outre de bien préciser que la reconnaissance était également soumise à toute exclusion en vigueur dans l'État adoptant, ce qui rendrait inutile l'une ou l'autre des variantes du paragraphe 2. Le texte proposé était le suivant :

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

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

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

184. En réponse à cette proposition, on a fait observer que la référence aux lois nationales n'apportait pas de solution satisfaisante dans la mesure où la législation de l'État adoptant pouvait renfermer des dispositions discriminatoires qui risquaient de nuire à l'esprit du projet d'article 17. En outre, l'amendement proposé soulevait diverses questions quant au point de savoir qui, dans l'État adoptant, déterminerait que l'autorité de certification étrangère satisfaisait aux mêmes normes objectives et suivait les mêmes procédures que les entités et personnes locales et par quel moyen une telle détermination serait effectuée.

185. Selon un avis, dans sa formulation actuelle, le paragraphe 1 semblait impliquer que les autorités de certification étrangères devaient non seulement être approuvées en vertu de leur propre législation mais devaient en outre satisfaire aux conditions de l'État adoptant. On a estimé qu'une telle règle aurait des effets restrictifs non souhaitables et ne contribuerait pas à promouvoir le commerce électronique. Suite à cette dernière observation, on a proposé de préciser le sens du paragraphe 1 en en faisant une règle non discriminatoire dans les termes ci-après :

"1. Les [personnes] [entités] étrangères ne peuvent se voir refuser le droit de s'établir localement ou de fournir des services d'authentification au seul motif qu'elles sont étrangères si elles satisfont aux mêmes normes objectives et suivent les mêmes procédures que les entités et personnes locales pouvant devenir des autorités de certification."

186. On a objecté que la règle de non-discrimination proposée suscitait globalement les mêmes préoccupations que celles exposées dans les observations générales concernant le champ d'application du projet d'article 17 (voir ci-dessus par. 178 à 180).

187. Ayant examiné les diverses propositions et pris en compte les différentes vues exprimées, le Groupe de travail a estimé qu'il faudrait consacrer plus de temps à l'examen des questions visées au paragraphe 1. Le secrétariat a été prié de proposer une version révisée de ce paragraphe, avec d'éventuelles variantes tenant compte du débat ci-dessus, afin que le Groupe de travail puisse l'examiner ultérieurement.

Paragraphe 2

188. S'agissant des deux variantes sur les exclusions proposées au paragraphe 2, on a fait valoir que la variante X devait être supprimée car elle pourrait fournir un mécanisme non directif pour limiter le champ d'application du paragraphe 1. Conformément à cet avis, si une exclusion était permise, elle ne devrait l'être que pour des raisons de sécurité nationale, comme mentionné sous la variante Y. Toutefois, on s'est accordé à penser qu'il était préférable de conserver la variante X, selon laquelle il incomberait à l'État adoptant de formuler des exceptions à la règle générale du paragraphe 1. Certes, la variante Y offrait l'avantage de limiter les exclusions éventuelles à celles qui avaient trait à la sécurité nationale, mais on a estimé que les États voudraient peut-être inclure dans leur législation d'autres motifs d'exclusion relevant de l'ordre public. Après un échange de vues, il a été décidé de conserver les deux variantes en les plaçant entre crochets en vue d'un examen futur.

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

189. Le texte du projet d'article 18 examiné par le Groupe de travail était le suivant :

"Les certificats émis par les autorités de certification d'un autre pays peuvent être utilisés pour des signatures numériques selon les mêmes modalités que les certificats soumis aux présentes Règles s'ils sont reconnus par une autorité de certification se conformant à .... *[la loi de l'État adoptant]*, et si celle-ci garantit,

à l'instar de ce qu'elle fait pour ses propres certificats, que les détails figurant dans le certificat sont exacts et, en outre, que le certificat est valide et en vigueur."

190. Sur le plan général, on a déclaré que l'inclusion de dispositions traitant de la reconnaissance internationale représentait un progrès considérable pour l'amélioration de la fiabilité des certificats. Ces derniers étaient en effet de plus en plus utilisés dans la pratique commerciale et l'adhésion à des normes internationales pourrait contribuer à accroître la confiance dans cette nouvelle technologie. Le Groupe de travail a été invité à examiner les mécanismes internationaux d'habilitation des autorités de certification qui se conformaient à des normes internationales. L'idée d'inclure le sujet proposé parmi les questions devant être examinées par le Groupe de travail à un stade ultérieur a été appuyée. On a noté toutefois que ce sujet ne se limitait pas aux questions soulevées dans le projet d'article 18 et qu'il pourrait être examiné par le Groupe de travail par exemple quand celui-ci reprendrait l'examen de la question de l'enregistrement des certificats.

191. S'agissant du projet d'article 18 lui-même, il a été noté que la règle qui y figurait avait simplement pour objet de permettre à une autorité de certification locale de garantir, à l'instar de ce qu'elle faisait pour ses propres certificats, que les données figurant dans le certificat étranger étaient exactes et que ce dernier était valable et valide. En vertu de ce projet d'article, c'était l'autorité de certification locale ayant fourni une telle garantie qui était tenue responsable en cas de vices du certificat étranger. Toutefois, l'existence d'une garantie, conformément au projet d'article 18, n'était pas un préalable à la reconnaissance d'un certificat émis par des autorités de certification étrangères qui remplissait par ailleurs les conditions énoncées au projet d'article 19. On a fait valoir que dans la mesure où la fourniture d'une garantie au titre du projet d'article 18 était purement volontaire, cet article n'était pas nécessaire et pouvait être supprimé. On a estimé en outre qu'il faudrait laisser à l'État adoptant le soin de décider si les autorités de certification locales pouvaient fournir une telle garantie pour des certificats émis par des autorités de certification étrangères, et à quelles conditions. On pourrait faire référence à l'émission de garanties du type envisagé dans le projet d'article 18 dans un guide sur l'incorporation des Règles uniformes ou dans des notes explicatives accompagnant ces Règles, selon la nature de l'instrument qui serait en fin de compte adopté.

192. Il a été rappelé au Groupe de travail qu'au cours de sa trente et unième session, il avait examiné les différents niveaux de fiabilité que pouvait offrir une autorité de certification locale par rapport à une autorité de certification étrangère. On a noté qu'au niveau le plus élevé, l'autorité de certification locale garantissait, à la demande de la partie se fiant à un certificat étranger, la teneur dudit certificat sur la base de sa connaissance déclarée des procédures ayant abouti à l'émission du certificat, assumant ainsi l'entière responsabilité de toute erreur ou de toute autre irrégularité dans le certificat. Au niveau de fiabilité le plus bas, l'autorité de certification locale se contenterait de garantir l'identité de l'autorité de certification étrangère, en vérifiant sa clef publique et sa signature numérique (voir A/CN.9/437, par. 81 et 82). On a fait observer que le projet d'article 18 ne faisait pas suffisamment apparaître ces différents niveaux de fiabilité et que, si la disposition était retenue, il faudrait préciser qu'elle n'excluait pas les arrangements autres qu'une garantie totale de l'exactitude et de la validité d'un certificat émis par une autorité de certification étrangère.

193. En réponse à des observations, il a été déclaré que le projet d'article 18 était utile en ce qu'il permettait la circulation et l'utilisation internationale des certificats, sans qu'il soit besoin de recourir à des accords internationaux bilatéraux ou multilatéraux sur leur reconnaissance, ce que certains États pourraient juger nécessaire pour accorder la reconnaissance au titre du projet d'article 19. En outre, puisque le Groupe de travail avait décidé de mentionner dans les Règles uniformes non seulement les autorités de certification agréées par des entités publiques mais aussi celles qui se situaient en dehors de ce système d'agrément (voir A/CN.9/437, par. 48 à 50), le projet d'article 18 avait pour avantage supplémentaire d'offrir une solution commerciale dans les cas où la reconnaissance au titre du projet d'article 19 ne serait pas automatique. Il a été proposé, à cet égard, de préciser la portée de l'article 18 en le reformulant comme suit :

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

194. On a appuyé le maintien dans les Règles uniformes d'une disposition autorisant une autorité de certification locale à donner des garanties pour des certificats émis par des autorités de certification étrangères. Une telle disposition pourrait être fondée sur le projet d'article 18, compte tenu des propositions formulées dans le Groupe de travail. On a fait valoir, cependant, que l'insertion du projet d'article 18 au chapitre IV était inappropriée, car la disposition ne portait pas sur la reconnaissance des certificats émis à l'étrangers.

195. Après délibération, le Groupe de travail est convenu de conserver le projet d'article 18 entre crochets, avec les amendements proposés, et a prié le secrétariat d'élaborer d'autres versions de cette disposition en tenant compte des vues qui avaient été exprimées, aux fins d'un examen futur par le Groupe de travail.

Article 19. Reconnaissance de certificats étrangers

196. Le texte du projet d'article 19 examiné par le Groupe de travail était le suivant :

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

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

3. Il est donné effet [par les tribunaux ou d'autres juges des faits] aux signatures numériques vérifiées par référence à un certificat émis par une autorité de certification étrangère si le certificat est aussi fiable que nécessaire au vu de l'objet pour lequel il a été émis, compte tenu de toutes les circonstances.

4. Nonobstant le paragraphe précédent, les organismes publics peuvent spécifier [par publication] qu'il est nécessaire de recourir à une autorité de certification, une catégorie d'autorités de certification ou une catégorie de certificats particuliers pour les messages ou les signatures qui leur sont soumis."

Paragraphes 1 et 2

197. On a fait observer que les paragraphes 1 et 2 portaient sur les manières d'établir la fiabilité des certificats et des signatures étrangers avant qu'une transaction n'ait lieu (et avant que surgisse un conflit concernant le niveau de fiabilité d'une signature). À cette fin, ces paragraphes énonçaient les critères qui pourraient être appliqués dans l'État adoptant pour reconnaître les certificats émis par des autorités de certification étrangères, ainsi que les signatures et documents conformes aux lois d'un autre État.

198. Diverses questions ont été soulevées au sujet de la portée de la reconnaissance au titre des paragraphes 1 et 2. À propos du paragraphe 1, il a été déclaré que la notion d'équivalence juridique entre les certificats émis par des

autorités de certification étrangères et des certificats émis par des autorités de certification dont les activités étaient soumises aux règles de l'État adoptant n'était pas suffisamment claire. On a fait observer que la "reconnaissance", tel que ce terme était couramment employé en droit international privé, impliquait que les actes effectués dans une autre juridiction produisaient des effets juridiques. Toutefois, cette notion ne pouvait s'appliquer dans le contexte du paragraphe 1, puisqu'un certificat était un instrument qui ne faisait qu'énoncer des faits. En outre, en vertu du paragraphe 1 comme du paragraphe 2, l'État adoptant devait appliquer ses propres lois pour déterminer la fiabilité des certificats émis par des autorités de certification étrangères ainsi que les signatures et documents conformes aux lois d'un autre État. En conséquence, il a été dit que les paragraphes 1 et 2 ne correspondaient pas aux principes généraux du droit international privé selon lesquels la validité d'actes accomplis à l'étranger devait être déterminée conformément à la loi applicable dans la juridiction où ils avaient été accomplis. En outre, on a fait remarquer que l'article 13 de la Loi type et les projets d'article 3 et 5 des Règles uniformes comportaient déjà des règles concernant l'attribution des messages de données et la détermination de la fiabilité d'une signature électronique.

199. En réponse à ces observations, on a fait remarquer que les paragraphes 1 et 2 étaient utiles pour les régimes réglementaires nationaux exigeant l'utilisation de certaines catégories de certificats offrant un niveau de fiabilité élevé pour la réalisation de certaines transactions. Dans les États adoptants ayant de tels régimes, le paragraphe 1 offrait des normes minimales pour la reconnaissance des certificats émis par des autorités de certification étrangères utilisés dans le cadre de transactions autres que celles pour lesquelles était exigée une certaine catégorie de certificat. Le paragraphe 2 offrait en même temps à ces États adoptants une règle par défaut qui créait une présomption de validité pour les signatures et les documents conformes aux lois d'un autre État, dont on estimait qu'elles fournissaient un niveau de sécurité raisonnable pour tous les cas où les lois de l'État adoptant n'imposaient pas de conditions plus strictes. Le Groupe de travail a été instamment prié de faire en sorte de ne pas laisser régler entièrement la question des normes minimales s'appliquant à un certificat étranger par les règles de conflit de l'État adoptant.

200. Le Groupe de travail a examiné des amendements possibles aux paragraphes 1 et 2 afin de répondre aux craintes qui avaient été exprimées. Il a été en particulier proposé de combiner les deux paragraphes et de les reformuler afin d'en faire une règle de non-discrimination formulée comme suit :

> "Les certificats émis par des autorités de certification étrangères ne peuvent pas ne pas être reconnus comme les certificats émis par des autorités de certification locales au motif qu'ils ont été émis par des autorités de certification étrangères."

201. Des objections ont cependant été soulevées à l'encontre de cette formulation négative car elle n'offrait pas de normes sur lesquelles baser la reconnaissance. En outre, on a fait observer que cette règle pourrait donner lieu aux mêmes réserves que celles qui avaient été émises à propos du projet d'article 17 (voir par. 185 et 186 ci-dessus).

202. Après délibération, il a été généralement estimé qu'il serait souhaitable de formuler une règle de fond offrant une méthode permettant d'établir la fiabilité des certificats et des signatures étrangers avant la transaction. Le secrétariat a été prié d'élaborer une version révisée des paragraphes 1 et 2, comportant plusieurs variantes tenant compte des vues exprimées, et dont une combinerait les deux paragraphes.

Paragraphe 3

203. On a fait observer que le paragraphe 3 visait à établir la norme par rapport à laquelle les signatures et certificats étrangers pourraient être appréciés en l'absence de toute détermination préalable de leur fiabilité. On a toutefois indiqué que, telle qu'elle était actuellement rédigée, cette disposition n'était peut-être pas nécessaire, car elle réaffirmait simplement le principe selon lequel, en cas de litige concernant l'authenticité d'une signature et la fiabilité d'un certificat émis par une autorité de certification étrangère, les tribunaux de l'État adoptant devaient donner à cette signature ou à ce certificat la force probante, qui était appropriée en l'espèce.

204. En réponse à ces observations, il a été noté que le paragraphe 3, qui s'inspirait de l'article 7 de la Loi type, fournissait des indications utiles aux tribunaux de l'État adoptant pour apprécier la fiabilité d'un certificat étranger. Il était souhaitable d'énoncer de nouveau ce principe important dans les Règles uniformes étant donné qu'un État adoptant ces dernières n'aurait pas nécessairement incorporé l'article 7 de la Loi type dans son droit interne. Pour que son objet apparaisse plus clairement, il a été proposé de modifier comme suit le libellé du paragraphe 3 :

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

205. Après délibération, le Groupe de travail a décidé qu'il examinerait de façon plus approfondie la teneur du paragraphe 3 à un stade ultérieur.

Paragraphe 4

206. On s'est interrogé sur la nécessité d'une disposition comme le paragraphe 4, qui préservait le droit des organismes publics de déterminer les procédures à utiliser dans les communications électroniques avec eux. D'un côté, la crainte a été exprimée que ce paragraphe ait des effets restrictifs indésirables et risque d'être interprété comme signifiant que des personnes ou des entités autres que des organismes publics n'avaient pas le droit de choisir l'autorité de certification, la catégorie d'autorités de certification ou la catégorie de certificats particuliers auxquelles elles souhaitaient recourir pour les messages ou les signatures qu'elles recevaient. Une telle situation a été jugée incompatible avec le principe de l'autonomie des parties consacré dans diverses dispositions de la Loi type. D'un autre côté, si l'objet du paragraphe 4 était d'établir une prérogative spéciale pour les organismes publics, il faudrait peut-être préciser encore la disposition, car elle pourrait être interprétée comme signifiant que, si un organisme public n'indiquait pas clairement l'autorité de certification, la catégorie d'autorités de certification ou la catégorie de certificats auxquelles il souhaitait recourir pour les messages ou les signatures qui lui étaient soumis, il était tenu d'accepter quelque catégorie d'autorités de certification ou de certificats que ce soit.

207. L'avis général a été que le droit de choisir l'autorité de certification, la catégorie d'autorités de certification ou la catégorie de certificats, auxquelles elles souhaitaient recourir pour les messages ou les signatures qu'elles recevaient devrait être reconnu aux parties à des transactions commerciales et autres, et non aux seuls organismes publics. Le Groupe de travail a prié le secrétariat de modifier le libellé du paragraphe 4 de façon qu'il reflète ce point de vue et a décidé d'examiner ultérieurement l'endroit où il conviendrait d'insérer la disposition révisée.

IV. COORDINATION DES TRAVAUX

208. Le Groupe de travail a entendu des déclarations concernant les travaux entrepris par l'Organisation des Nations Unies pour l'éducation, la science et la culture (UNESCO) et la Conférence des Nations Unies pour le commerce et le développement (CNUCED) dans le domaine du commerce électronique.

209. Il a été déclaré que, à sa 29ème Conférence générale, l'UNESCO avait été chargée d'entreprendre l'élaboration d'un instrument juridique international relatif à l'utilisation du cyberespace. À cet égard, l'opinion a été exprimée qu'il était nécessaire que l'UNESCO et la CNUDCI unissent leurs efforts dans le domaine du commerce électronique. On a fait observer que ces efforts devraient être guidés par la nécessité de promouvoir le commerce électronique d'une manière qui serait avantageuse à la fois pour les pays développés et les pays en développement et qui garantirait en même temps les droits fondamentaux de l'être humain, y compris le droit au respect de la vie privée. Il a été souligné que les questions de l'attribution de messages de données à leurs initiateurs,

de l'intégrité de tels messages et de la responsabilité de parties engagées dans le commerce électronique devraient être au cœur des efforts du Groupe de travail sur les signatures numériques et autres signatures électroniques.

210. Dans une déclaration concernant les travaux de la CNUCED, on a fait observer qu'un Réseau global des pôles commerciaux avait été mis en place en vue d'aider les pays en développement dans les efforts qu'ils déployaient pour bénéficier des progrès faits dans le domaine des communications électroniques. En outre, il a été annoncé que la CNUCED organisait une exposition des fabricants de matériel, des producteurs de logiciels et des prestataires de services dans le commerce électronique (Lyon, 8-13 novembre 1998). On a indiqué que cette exposition comporterait une série d'exposés sur de nombreuses questions liées au commerce électronique.

211. Le Groupe de travail a pris note des déclarations et s'est félicité de la participation d'organisations intéressées à ses travaux. Le secrétariat a été prié de continuer à suivre l'évolution de la situation en ce qui concernait les aspects juridiques du commerce électronique, tels qu'ils étaient traités par d'autres organisations internationales et de faire rapport au Groupe de travail sur ce sujet.

V. TRAVAUX FUTURS

212. À la fin de la session, il a été proposé que le Groupe de travail envisage à titre préliminaire d'entreprendre l'élaboration d'une convention internationale fondée sur les dispositions de la Loi type et des Règles uniformes. Il a été convenu que ce sujet devrait peut-être être inscrit à l'ordre du jour de la prochaine session du Groupe de travail sur la base de propositions plus détaillées que pourraient faire éventuellement les délégations intéressées. La conclusion préliminaire du Groupe de travail a toutefois été que l'élaboration d'une convention devrait en tout état de cause être considérée comme un projet distinct à la fois de l'élaboration des Règles uniformes et de toute autre supplément éventuel à la Loi type. En attendant une décision finale quant à la forme des Règles uniformes, la proposition d'élaborer une convention à un stade ultérieur ne devrait pas détourner le Groupe de travail de sa tâche actuelle, qui était de se concentrer sur l'élaboration d'un projet de Règles uniformes sur les signatures numériques et autres signatures électroniques, ni de son hypothèse de travail actuelle selon laquelle les Règles uniformes prendraient la forme d'un projet de dispositions législatives. Il a aussi été généralement entendu que l'élaboration éventuelle d'un projet de convention ne devrait pas être utilisée comme moyen de revenir sur des questions réglées dans la Loi type, ce qui risquerait d'avoir un effet négatif sur l'usage croissant de cet instrument déjà couronné de succès.

213. Il a été noté que la prochaine session du Groupe de travail devrait normalement se tenir à New York du 29 juin au 10 juillet 1998, sous réserve de la confirmation de ces dates par la Commission à sa trente et unième session (New York, 1er-12 juin 1998).

Notes

[1]*Documents officiels de l'Assemblée générale, cinquante et unième session, Supplément nº 17* (A/51/17), par. 223 et 224.

[2]Ibid., *Cinquante-deuxième session, Supplément nº 17* (A/52/17), par. 249 à 251.

* * *