NATIONS UNIES **A**

Assemblée générale

Distr. GÉNÉRALE
A/CN.9/454
21 août 1998

FRANÇAIS
Original: ANGLAIS

COMMISSION DES NATIONS UNIES
POUR LE DROIT COMMERCIAL INTERNATIONAL
Trente-deuxième session
Vienne, 17 mai-4 juin 1999

RAPPORT DU GROUPE DE TRAVAIL SUR LE COMMERCE ÉLECTRONIQUE
SUR LES TRAVAUX DE SA TRENTE-TROISIÈME SESSION

(New York, 29 juin-10 juillet 1998)

TABLE DES MATIÈRES

V.98-55439

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 était 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).

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 généralement considéré que le Groupe de travail pourrait utilement envisager l'établissement d'un ensemble minimum de normes que les autorités de certification devraient strictement respecter, en particulier dans les cas de certification transnationale[2].

5. Le Groupe de travail a commencé à élaborer le projet de Règles uniformes en se fondant sur une note établie par le secrétariat (A/CN.9/WG.IV/WP.73). Ce dernier a été prié d'établir, à partir des délibérations et conclusions du Groupe de travail, un ensemble de dispositions révisées avec d'éventuelles variantes pour examen par le Groupe de travail lors d'une future session

6. À sa trente et unième session (1998), la Commission était saisie du rapport du Groupe de travail sur les travaux de sa trente-deuxième session (A/CN.9/446). La Commission a pris note avec satisfaction des efforts déployés par le Groupe de travail lors de l'élaboration du projet de Règles uniformes. On a noté qu'à ses trente et unième et trente-deuxième sessions, le Groupe de travail avait eu manifestement beaucoup de mal à se mettre d'accord sur les nouveaux problèmes juridiques qui découlaient du recours accru aux signatures numériques et autres signatures électroniques. On a également fait observer qu'un consensus restait encore à réaliser sur la manière dont ces problèmes pouvaient être abordés dans un cadre juridique acceptable à l'échelon international.

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

8. La Commission a noté qu'à la fin de la trente-deuxième session du Groupe de travail, il avait été proposé que ce dernier envisage à titre préliminaire d'entreprendre l'élaboration d'une convention internationale fondée sur les dispositions de la Loi type et des Règles uniformes. Le Groupe de travail était convenu que ce sujet devrait peut-être être inscrit à l'ordre du jour de sa prochaine session sur la base de propositions plus détaillées que pourraient faire éventuellement les délégations intéressées. La conclusion préliminaire du Groupe de travail avait 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 tout autre supplément éventuel à la Loi type. En attendant une décision finale quant à la forme des Règles uniformes, la proposition tendant à 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, ni de son hypothèse de travail actuelle selon laquelle les Règles uniformes devraient prendre 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 servir de prétexte pour 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 (A/CN.9/446, par. 212).

9. La Commission a noté qu'une délégation avait présenté une proposition relative à l'élaboration d'une convention, pour examen par le Groupe de travail (A/CN.9/WG.IV/ WP.77). Divers points de vue ont été émis à cet égard. Selon une opinion, une convention fondée sur les dispositions de la Loi type était nécessaire car la Loi type de la CNUDCI sur le commerce électronique risquait de ne pas suffire pour établir un cadre juridique universel pour le commerce électronique. Vu la nature de cet instrument, ses dispositions pouvaient être modifiées par le législateur national qui les promulguait, ce qui nuisait à l'harmonisation recherchée des règles juridiques applicables au commerce international. On a estimé, à l'inverse, qu'en raison de l'évolution rapide des données techniques relatives au commerce électronique, cette question ne se prêtait pas aisément à l'adoption de l'approche rigide que supposait une convention internationale. On a fait observer que la Loi type était particulièrement utile comme recueil de principes qui pouvaient être promulgués dans la législation nationale sous divers libellés pour tenir compte du recours accru au commerce électronique.

10. La plupart des membres de la Commission ont estimé qu'il serait prématuré d'entreprendre l'élaboration de la convention proposée. Plusieurs délégations ont indiqué que des projets de réforme juridique fondés sur les dispositions de la Loi type étaient en cours dans leurs pays. Une délégation a exprimé la crainte que l'élaboration d'une convention internationale fondée sur la Loi type nuise à la promulgation générale de la Loi type elle-même qui, à peine deux ans après son adoption par la Commission, était déjà appliquée dans un grand nombre de pays. En outre, on a généralement estimé que le Groupe de travail ne devrait pas être détourné de sa tâche actuelle qui était d'élaborer le projet de Règles uniformes, comme convenu par la Commission. Une fois sa tâche achevée, il serait loisible au Groupe de travail, dans le cadre de sa fonction consultative générale pour les problèmes relatifs au commerce électronique, de présenter à la Commission des propositions touchant les travaux futurs dans ce domaine. Les partisans d'une convention ont estimé qu'il serait peut-être nécessaire d'examiner la question plus avant à une future session de la Commission ainsi que dans le Groupe de travail, éventuellement par le biais de consultations informelles. On a rappelé que, si les travaux futurs pouvaient inclure l'élaboration d'une convention, d'autres questions avaient également été proposées, telles que les questions de compétence, le droit applicable et le règlement des litiges sur Internet[3].

11. Le Groupe de travail sur le commerce électronique, qui est composé de tous les États membres de la Commission, a tenu sa trente-troisième session à New York du 29 juin au 10 juillet 1998. Ont assisté à cette session les représentants des États membres du Groupe de travail ci-après: Allemagne, Australie, Autriche, Brésil, Cameroun, Chine, Colombie, Égypte, Espagne, États-Unis d'Amérique, Finlande, France, Honduras, Hongrie, Iran (République islamique d'), Italie, Japon, Lituanie, Mexique, Ouganda, Roumanie, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, Singapour et Thaïlande.

12. Y ont également assisté les observateurs des États ci-après: Arabie saoudite, Canada, Danemark, Gabon, Indonésie, Irlande, Madagascar, Panama, Pays-Bas, Pologne, Portugal, République de Corée, République démocratique du Congo, République tchèque, Suède, Suisse, Tunisie et Turquie.

13. Y ont en outre assisté les organisations internationales ci-après: Programme des Nations Unies pour le développement (PNUD), Organisation mondiale de la propriété intellectuelle (OMPI), Banque africaine de développement, Commission européenne, Organisation de coopération et développement économiques (OCDE), Comité maritime international (CMI), Association européenne des étudiants en droit, Grupo Latinoamericano de Abogados para el Comercio Internacional (GRULACI), Instituto Iberoamericano de Derecho Maritimo (INIDIE), Association internationale des ports (AIP), Association internationale du barreau, Chambre de commerce internationale (CCI), Internet Law and Policy Forum (ILPF), Society for Worldwide Interbank Financial Telecommunications (S.W.I.F.T.) et Union internationale des avocats (UIA).

14. Le Groupe de travail a élu les membres du Bureau ci-après:

Président : M. Mads Bryde **Andersen** (Danemark);

Vice-Président : M. **Pang** Khang Chau (Singapour);

Rapporteur : M. Jair Fernando **Imbachi Ceron** (Colombie).

15. Le Groupe de travail était saisi des documents ci-après: ordre du jour provisoire (A/CN.9/WG.IV/WP.75); note du secrétariat contenant le projet de Règles uniformes sur les signatures numériques, les autres signatures électroniques, les autorités de certification et les questions juridiques connexes (A/CN.9/WG.IV/WP.76); et note reproduisant le texte du projet de convention internationale sur les transactions électroniques proposé par les États-Unis d'Amérique (A/CN.9/WG.IV/WP.77).

16. 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: projet de Règles uniformes sur les signatures électroniques.

4. Questions diverses.

5. Adoption du rapport.

I. Débats et décisions

17. Le Groupe de travail a examiné la question des signatures numériques, des autres signatures électroniques, des autorités de certification et des questions juridiques connexes sur la base de la note établie par le Secrétariat (A/CN.9/WG.IV/WP.76). Il est rendu compte de ses débats et conclusions à ce sujet dans la section II ci-dessous. Le secrétariat a été prié d'élaborer, à partir de ces débats et conclusions, un ensemble de dispositions révisées, avec d'éventuelles variantes, pour examen par le Groupe de travail lors d'une session future. Une délégation a proposé de travailler ultérieurement à une convention sur les transactions électroniques. Cette proposition a fait l'objet d'un examen informel dont il est fait état à la section III ci-dessous.

II. Projet de Règles uniformes sur les signatures électroniques

Remarques générales

18. D'emblée, l'ensemble du Groupe de travail a estimé que la structure actuelle des Règles uniformes constituait une base de discussion acceptable. Selon une opinion, cependant, l'association d'une partie de caractère général sur les signatures électroniques et d'une partie énonçant des règles très détaillées sur les signatures numériques pourrait poser des problèmes quant à la relation et à l'interaction entre ces deux parties. Il a été observé que les Règles uniformes pouvaient, dans une large mesure, convenir aux divers types de signatures électroniques qui apparaissaient progressivement sur le marché. Elles pouvaient jouer un rôle important en faisant en sorte que les techniques de signature électronique soient utilisées dans un environnement ouvert, en suscitant la confiance à l'égard de ces techniques et en évitant que certaines d'entre elles ne soient désavantagées. Néanmoins, on a souligné qu'il faudrait peut-être éclaircir un certain nombre de points, notamment la mesure dans laquelle les Règles uniformes reconnaissaient l'autonomie des parties dans le contexte de réseaux fermés ou semi-fermés; la capacité des Règles uniformes à tenir compte des systèmes dans lesquels les autorités de certification fonctionnaient comme des prestataires de services indépendants et de ceux dans lesquels les parties se fient à un certificat émis par une des parties; la mesure dans laquelle les Règles uniformes pouvaient être adaptées à des techniques spécifiques autres que les signatures numériques; la compatibilité des Règles uniformes avec les différentes procédures de sécurité, quel que soit leur niveau.

Chapitre premier. Champ d'application et dispositions générales

19. Le Groupe de travail a décidé de reporter l'examen du chapitre premier jusqu'à ce qu'il ait achevé d'examiner les dispositions de fond des Règles uniformes.

Chapitre II. Signatures électroniques

Section I. Signatures électroniques en général

Article premier. Définitions

20. Le Groupe de travail a décidé de reporter l'examen du projet d'article premier jusqu'à ce qu'il ait achevé d'examiner les dispositions de fond des Règles uniformes.

Article 2. Effet de la signature électronique

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

> "1. Pour ce qui est d'un message de données authentifié à l'aide d'une signature électronique [autre qu'une signature électronique sécurisée], cette signature satisfait à toute exigence légale concernant une signature si sa fiabilité est suffisante au regard de l'objet pour lequel elle a été utilisée, compte tenu de toutes les circonstances, y compris tout accord en la matière.
>
> 2. Le paragraphe 1 s'applique, que l'exigence légale qui y est visée ait la forme d'une obligation ou que la loi prévoie simplement certaines conséquences s'il n'y a pas de signature.
>
> 3. Sauf disposition contraire énoncée expressément dans [les présentes Règles], les signatures électroniques qui ne sont pas des signatures électroniques [renforcées] [sécurisées] ne sont pas soumises à la réglementation aux normes ou aux procédures d'octroi de licences établies par ... *[les organes ou autorités indiqués par l'État dans l'article]* ou aux présomptions créées par les articles 4, 5 et 6.
>
> 4. Les dispositions du présent article ne s'appliquent pas dans les situations suivantes: [...]."

Titre

22. On a exprimé l'avis que le titre, "Effet de la signature électronique", pouvait prêter à confusion. En effet, le projet d'article 2 n'était pas axé sur l'effet de la signature électronique, mais plutôt sur les cas dans lesquels on pouvait considérer qu'une telle signature satisfaisait aux exigences légales, conformément à l'article 7 de la Loi type. Après un débat, il a été décidé que le titre du projet d'article devait être plutôt, par exemple, "Respect des exigences légales".

Paragraphe 1

23. On a exprimé l'avis que le libellé du paragraphe 1 devait être aligné exactement sur celui de l'article 7 de la Loi type. Il a donc été suggéré que ce paragraphe se lise comme suit:

> "1. Pour ce qui est d'un message de données authentifié à l'aide d'une signature électronique [autre qu'une signature électronique sécurisée], cette signature satisfait à toute exigence légale ou règle de preuve

concernant une signature si la fiabilité de la méthode utilisée pour l'apposer est suffisante au regard de l'objet pour lequel le message de données a été créé ou communiqué, compte tenu de toutes les circonstances, y compris de tout accord en la matière."

24. Cette proposition a bénéficié d'un certain appui, mais il a été fait observer que l'expression "toute exigence légale ou règle de preuve" ne concordait pas avec le texte de la Loi type. En effet, l'article 7 de la Loi type stipulait "lorsque la loi exige la signature", ce qui renvoyait à la fois aux exigences légales et à la règle de preuve. Toute discordance à ce sujet entre la Loi type et les Règles uniformes risquait de compliquer l'interprétation des deux instruments. Le Groupe de travail a adopté le texte proposé sous réserve de la suppression des mots "ou règle de preuve".

Paragraphe 2

25. On a estimé que, dans l'ensemble, le paragraphe 2 était acceptable quant au fond. Afin de respecter la terminologie employée dans la Loi type, le Groupe de travail a décidé de supprimer le mot "légale".

Paragraphe 3

26. Il a été observé que le paragraphe 3 ne faisait qu'énoncer une évidence et qu'il valait mieux le supprimer. Néanmoins, selon l'avis qui a prévalu, puisque l'on pouvait s'attendre à ce que la très grande majorité des signatures électroniques utilisées dans la pratique n'entrent pas dans la catégorie étroite des signatures électroniques "renforcées" ou "sécurisées" (dont l'usage était réglementé dans certains pays), les Règles uniformes devaient indiquer très explicitement que la réglementation relative aux signatures électroniques "renforcées" ou "sécurisées" ne s'appliquait pas en général à tous les types de signatures électroniques. Après un débat, il a été décidé de conserver le paragraphe 3 pour plus de clarté.

Paragraphe 4

27. Le Groupe de travail a estimé que, dans l'ensemble, le paragraphe 4 était acceptable quant au fond.

Section II. Signatures électroniques [renforcées] [sécurisées]

Article 3. Présomption de signature

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

"1. Un message de données est présumé avoir été signé [si] [à partir du moment où] une signature électronique [renforcée] [sécurisée] y est apposée.

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

Paragraphe 1

29. Il a été généralement convenu qu'il fallait que les Règles uniformes distinguent un petit éventail de techniques offrant une haute fiabilité des "signatures électroniques" en général. Toutefois, sur le plan de la forme, des doutes ont été exprimés sur le point de savoir si les qualificatifs "renforcée" ou "sécurisée" étaient acceptables. Bien qu'on ait reconnu que le terme "sécurisée" était couramment employé dans le contexte des signatures électroniques, il a été critiqué au motif qu'il introduisait un critère subjectif et impliquait que les signatures qui ne rentraient pas dans la catégorie des signatures "sécurisées" n'étaient par définition pas sûres. On a également objecté que le terme "sécurisée" risquait d'être interprété comme impliquant une fiabilité excessive de la signature visée dans le projet

d'article 3. Quant au terme "renforcée", on a objecté qu'il pouvait s'appliquer à pratiquement n'importe quel attribut d'une signature et qu'il était donc trop vague, en particulier pour servir à déterminer la sécurité offerte par une signature. Si certains ont fait valoir que le mot "renforcée" n'avait pas grand sens dans ce contexte, l'opinion qui a prévalu a été qu'en l'absence d'un terme plus approprié qu'il faudrait rechercher à un stade ultérieur, c'est ce mot qui serait utilisé. Des termes tels que "conforme" et "authentifiée" ont également été suggérés, mais ces propositions n'ont reçu aucun appui.

30. Toujours sur le plan de la forme, on a fait observer que le projet d'article 3 n'envisageait qu'un seul cas de figure, celui de l'"apposition" de la signature, alors que la définition de la signature électronique figurant à l'alinéa a) du projet d'article premier englobait un concept plus large, à savoir celui de données "logiquement associées [à un] message [de données]". On a émis l'avis que le projet d'article 3 devrait reprendre les mêmes termes que ceux utilisés dans le projet d'article premier.

31. On a émis l'avis que les mots "[à partir du moment où]" devraient être supprimés. À l'appui de ce point de vue, on a fait valoir que le moment auquel le message était signé n'était pas ce qui importait dans le projet d'article 3 et que l'inclusion de ce membre de phrase risquait d'introduire un élément d'incertitude. On a répondu que le moment auquel le message de données était signé avait d'importantes conséquences juridiques, en particulier pour les tiers, et que le membre de phrase devait donc être maintenu. Après un débat, la majorité des membres du Groupe de travail a estimé que la question du moment auquel le message de données avait été signé ne devait pas être traitée dans le projet d'article 3, mais qu'il faudrait peut-être y revenir à un stade ultérieur de l'élaboration des Règles uniformes.

32. On a émis l'avis que les questions traitées dans les projets d'article 3 et 4 étaient trop proches pour figurer dans des articles distincts. On a fait observer que, dans certains systèmes juridiques, les deux questions étaient indissociables puisqu'un message de données ne pouvait être considéré comme signé que si la signature pouvait être attribuée à un signataire. Pour résoudre cette difficulté, on a suggéré de fusionner les projets d'article 3 et 4. On a rétorqué que dans d'autres systèmes juridiques, la question de savoir si un message de données avait ou non été signé, quelle que soit l'identité du signataire ou lorsque l'identité de l'expéditeur n'était pas un point controversé.

33. Le débat a porté essentiellement sur la question de savoir si le projet d'article 3 devait être supprimé, conservé sous forme d'une présomption ou remanié afin d'énoncer une règle de fond. On a fait valoir qu'une présomption devrait être réfragable et que dans le cas d'une signature il serait difficile d'apporter la preuve contraire. On a répliqué que la présomption soulevait le problème des preuves capables de l'écarter, lesquelles pouvaient être rapportées par des éléments tels que l'intention du signataire ou la fiabilité ou la régularité de la méthode utilisée pour signer le message de données. En stipulant qu'il y avait présomption de signature dans le cas d'une signature électronique renforcée, l'intention était de faire une distinction entre le type de signature électronique "renforcée" visé dans le projet d'article 3 et le type plus général de signature électronique visé dans le projet d'article 2. On a déclaré qu'en acquérant ce statut spécial, la signature électronique renforcée pouvait être considérée comme ayant été soumise à certains contrôles et ne nécessitait donc pas le même degré de vérification que la forme de signature électronique plus générale.

34. Le Groupe de travail a été invité à envisager de remplacer le paragraphe 1 par le nouveau paragraphe ci-après:

"Lorsque la loi exige une signature, cette exigence est satisfaite par une signature électronique renforcée."

35. Le débat s'est poursuivi sur la base de cette proposition. On a déclaré que le texte proposé évitait les problèmes que pourrait susciter la présomption et reconnaissait le principe de non-discrimination consacré à l'article 5 de la Loi type. L'objet de la proposition était d'établir une règle selon laquelle une signature électronique renforcée satisfaisait au critère énoncé à l'article 7 de la Loi type, à savoir que "la fiabilité" de la méthode d'authentification devait être "suffisante".

36. La proposition a reçu un certain appui, mais on a aussi fait observer qu'il ne serait possible de se prononcer à son sujet qu'en fonction de la définition qui serait retenue pour la signature électronique "renforcée". On a suggéré de maintenir la proposition entre crochets en attendant que cette définition ait été examinée. Certains membres ont déclaré estimer, eux aussi, que le libellé de la proposition devrait avoir un lien plus direct avec celui de l'article 7 de la Loi type. Il devait énoncer clairement que par signature électronique renforcée il fallait entendre une signature qui satisfaisait au critère de "la fiabilité ... suffisante" posé dans la Loi type, et qu'elle pouvait dès lors être considérée comme l'équivalent fonctionnel d'une signature manuscrite.

37. On a en outre fait observer que l'article 7 de la Loi type, en mettant l'accent sur la fiabilité suffisante de la méthode, compte tenu de toutes les circonstances, établissait un critère qui laissait à la règle de fond une certaine souplesse. Le texte proposé, en revanche, établissait un critère rigide. On a suggéré d'ajouter un membre de phrase tel que "à moins qu'il ne soit prouvé que la signature électronique sécurisée ne satisfait pas aux exigences de l'article 7 de la Loi type" à la fin du texte proposé afin de maintenir la souplesse voulue. On a rétorqué que la proposition avait pour objet d'aller au-delà du critère énoncé à l'article 7 de la Loi type et de poser comme règle que dans tous les cas où la loi exige une signature, cette exigence serait satisfaite par une signature électronique renforcée, sans que les circonstances particulières à chaque cas d'espèce aient à être prises en considération. Si l'on ajoutait le membre de phrase suggéré, cela jetterait un doute sur le point de savoir si une signature électronique renforcée remplissait toutes les conditions d'une signature. Il ne fallait donc pas ajouter ce membre de phrase.

38. Après délibération, un large appui a été apporté au texte proposé, quant au fond, mais le Groupe de travail a décidé de le placer entre crochets en attendant l'examen de la définition de la signature électronique [renforcée] [sécurisée]. Il a aussi été décidé d'ajouter entre crochets un membre de phrase tel que "à moins qu'il ne soit prouvé que la signature électronique sécurisée ne satisfait pas aux exigences de l'article 7 de la Loi type", afin que le débat sur la question puisse être poursuivi à une session ultérieure.

Paragraphe 2

39. Le Groupe de travail a estimé que le paragraphe 2 était dans l'ensemble acceptable sur le fond.

Article 4. Présomption d'attribution

40. Le texte du projet d'article 4 examiné par le Groupe de travail était le suivant:

"1. Une signature électronique [renforcée] [sécurisée] est réputée être celle de la personne par qui, ou au nom de laquelle, elle est supposée avoir été utilisée,

Variante A sauf si le signataire supposé établit que la signature électronique [renforcée] [sécurisée] a été apposée sans autorisation.

Variante B à condition que la partie se fiant à la signature établisse que la procédure de sécurité ou la combinaison de procédures de sécurité appliquée pour vérifier la signature

a) était commercialement raisonnable eu égard aux circonstances;

b) qu'elle l'avait appliquée de manière fiable; et

c) qu'elle s'y était fiée de manière raisonnable et de bonne foi.

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

Remarques générales

41. Certains se sont demandé si le projet d'article 4 consacré à la présomption d'attribution était utile et approprié. Il a été fait observer que la question qui y était traitée relevait du droit civil général et que, par conséquent, elle ne se prêtait peut-être pas à une harmonisation au moyen d'un instrument international. Il a été suggéré que la question de l'attribution des signatures électroniques soit régie uniquement par le droit interne.

42. Néanmoins, selon l'avis qui a prévalu, il était bien nécessaire d'inclure dans le projet de Règles uniformes un article allant dans le même sens que le projet d'article 4. Bien que les variantes aient suscité quelques objections, le sentiment largement partagé a été non seulement que l'attribution pouvait être cruciale pour déterminer l'effet juridique d'une signature, mais aussi qu'un article de ce type était important pour établir la confiance et la certitude dans le domaine des signatures électroniques.

Paragraphe 1

43. La variante A a reçu un certain appui, de même qu'un projet d'article qui comprendrait à la fois la variante A et la variante B. Il a été fait observer qu'il était difficile d'avoir à choisir entre les deux variantes car elles ne constituaient pas une véritable alternative et portaient sur des aspects différents de la présomption d'attribution. La variante A traitait directement de la signature et des questions de l'attribution et de l'autorisation de la signature, tandis que la variante B déterminait les éléments sur lesquels la partie se fiant à la signature devait s'appuyer pour établir la présomption d'attribution, nonobstant le fait que la signature pouvait avoir été apposée sans autorisation.

44. À l'appui de la variante A, on a jugé qu'elle plaçait, à bon escient, la charge de la preuve sur la partie la plus à même de prouver l'acte de la signature, c'est-à-dire le signataire, alors que les règles énoncées dans la variante B s'appuyaient sur plusieurs critères subjectifs qu'il serait difficile d'appliquer dans la pratique. En outre, il a été fait observer que la variante B imposait, de manière inéquitable, une responsabilité éventuelle au signataire, en dépit du fait que celui-ci pouvait avoir prouvé, conformément à la variante A, que la signature avait été apposée sans autorisation. Dans ce contexte, on a vigoureusement exprimé l'avis qu'une disposition allant dans le sens de la variante B ne conviendrait pas aux transactions dans lesquelles intervenaient des consommateurs. Bien que le Groupe de travail ait décidé de ne pas s'engager, à ce stade, dans un débat général sur la question de savoir si le projet de règles uniformes devait s'appliquer aux transactions dans lesquelles intervenaient des consommateurs, on a en général estimé qu'il devait s'occuper des transactions dans lesquelles intervenaient des utilisateurs de techniques de communication électroniques.

45. À l'appui de l'incorporation de certains éléments de la variante B dans les Règles uniformes, on a déclaré que lorsqu'il s'agissait de déterminer les effets juridiques, il importait que toute partie se fiant à la signature électronique soit tenue de prouver les points énoncés aux alinéas *a* à *c* avant de pouvoir établir une présomption. Selon un avis, les conditions énumérées dans la variante B n'avaient pas leur place dans une disposition permettant d'établir une présomption. À ce propos, il a été suggéré de réexaminer l'emplacement de la variante B, et de se demander non seulement si elle avait sa place dans l'article 4 mais aussi quels étaient ses liens avec les définitions formulées au projet d'article premier ainsi qu'avec les articles de fond des règles uniformes. Par exemple, il a été fait observer que l'alinéa *c* de la variante B était en rapport avec le projet d'article 7 consacré à la responsabilité. Cette suggestion a bénéficié d'un certain appui et il a été décidé qu'il convenait de réexaminer les questions évoquées dans la variante B dans le contexte de la définition de la signature électronique [renforcée] [sécurisée] et des dispositions de fond sur la responsabilité. Après un débat, le Groupe de travail a décidé de supprimer la variante B.

46. Comme dans le cas du projet d'article 3, on s'est demandé s'il était approprié que l'article soit rédigé sous la forme d'une présomption. On s'est notamment interrogé sur la question de savoir s'il s'agissait d'une présomption réfutable et, si oui, par quels moyens elle pouvait être réfutée. On a estimé que cela devait être mentionné explicitement dans le texte de l'article. Il a été fait observer qu'il serait peut-être difficile d'établir une présomption générale applicable à tous les types de transaction car, pour être valable, une telle présomption dépendait d'un certain nombre de variables telles que la fiabilité technique de certaines signatures; l'opinion des parties au sujet du traitement à réserver à certains types de signature; la nature même des transactions. Dans certains types de transaction tels que les transactions financières, il pouvait être approprié d'associer un degré élevé de responsabilité à l'utilisation d'une signature sans autorisation, alors que pour les transactions moins importantes, un tel degré de responsabilité n'était peut-être pas fondé.

47. On s'est également inquiété de savoir si la présomption devait être structurée de manière qu'on puisse la réfuter simplement en niant avoir apposé la signature ou s'il fallait aussi prouver qu'il n'y avait pas eu autorisation.

48. On a critiqué le fait que l'article indique avec tant de précision les actes que les parties devaient accomplir. Les conditions auxquelles devait se plier la partie se fiant à la signature, énoncées aux alinéas *a* à *c* de la variante B, étaient trop contraignantes. De même, il était trop restrictif d'exiger, comme le faisait l'alinéa *b*, que ce soit la partie se fiant à la signature qui doive appliquer la procédure de sécurité. Le projet d'article devait s'en tenir à la question de savoir si une procédure de sécurité raisonnable avait été appliquée, quelles que soient les personnes qui s'en étaient chargées, ou aux faits qu'il fallait prouver. On a formulé la même critique à propos de la variante A, qui exigeait que le signataire supposé établisse qu'il n'y avait pas eu autorisation. De l'avis général, il convenait de dépersonnaliser le libellé du projet d'article 4 pour prendre en compte ces préoccupations.

49. On a également critiqué le fait que le projet d'article traite à la fois de l'autorisation et de l'attribution, deux concepts différents qu'il convenait de traiter séparément. Il a été proposé que le projet d'article 4 soit axé sur l'autorisation plutôt que sur l'attribution. En réponse, il a été observé que le paragraphe 2 de l'article 13 de la Loi type intégrait la notion d'autorisation dans des dispositions consacrées à l'attribution.

50. Le libellé du projet d'article 4 a suscité un certain nombre de préoccupations. Il a été estimé que le projet de Règles uniformes devait respecter le principe de la neutralité quant aux techniques utilisées et au champ d'application, et que tel n'était pas le cas de la variante B. En particulier, l'expression "partie se fiant à la signature" était habituellement utilisée dans le contexte des signatures numériques. Puisqu'elle n'était pas définie dans les Règles uniformes, le projet d'article 4 devait indiquer clairement que l'emploi de cette expression ne signifiait pas que l'on traitait uniquement des signatures numériques certifiées. Compte tenu de la décision de supprimer la variante B, aucune suite n'a été donnée à cette proposition, étant entendu cependant qu'un texte reprenant cette variante quant au fond pourrait être proposé à une session future.

51. D'autres propositions ont été formulées pour améliorer le libellé du projet d'article 4. Il a été suggéré notamment de remplacer le mot "utilisée" (s'agissant de la signature) par des termes tels que "conçue", "produite" ou "créée". Le Groupe de travail a approuvé cette proposition. On a estimé par ailleurs qu'il n'aurait pas été nécessaire d'employer l'expression "une combinaison de procédures de sécurité" dans la variante B supprimée car l'emploi de différentes procédures équivalait à "une procédure de sécurité". Le Groupe de travail a convenu qu'il faudrait examiner plus en détail cette suggestion dans le contexte d'autres projets d'articles où l'expression en question était employée.

52. Afin de prendre en compte la suggestion tendant à dépersonnaliser le libellé du projet d'article 4 et à élargir la catégorie des personnes qui pouvaient se charger des actes nécessaires, il a été proposé de remplacer le paragraphe 1 par le texte suivant:

> "Une signature électronique [renforcée] est réputée être celle de la personne par qui, ou au nom de laquelle, elle est supposée avoir été créée, sauf s'il est établi que la signature électronique [renforcée] n'a été apposée ni par le signataire supposé ni par une personne habilitée à agir en son nom."

Après un débat, le Groupe de travail a adopté le paragraphe 1 ainsi remanié.

Paragraphe 2

53. Le Groupe de travail a jugé que le paragraphe 2 était de manière générale acceptable quant au fond.

Article 5. Présomption d'intégrité

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

> "1. Si le signataire supposé a utilisé une procédure de sécurité capable de prouver [de manière fiable] qu'un message de données ou toute signature [électronique] [électronique [renforcée] [sécurisée]] y étant apposée n'a pas été modifié après l'application de la procédure de sécurité audit message de données ou à toute signature, il est présumé [sauf preuve contraire] que le message de données ou la signature n'a pas été modifié.
>
> 2. Les dispositions du présent article ne s'appliquent pas dans les conditions suivantes: [...]."

Paragraphe 1

55. D'emblée, il a été généralement estimé qu'il était utile d'adopter une disposition allant dans le sens du paragraphe 1 pour clarifier la manière dont les conditions énoncées à l'article 8 de la Loi type devaient être satisfaites. Plusieurs avis ont été exprimés et des suggestions ont été formulées pour améliorer le libellé du paragraphe 1.

56. Le Groupe de travail a examiné la question de savoir si le projet d'article 5 devait traiter à la fois de l'intégrité de la signature et de l'intégrité du message de données. Le sentiment largement partagé était que le libellé actuel du paragraphe 1, qui mentionnait l'intégrité du message de données ou de "toute signature", n'était pas clair et pouvait donner lieu à une interprétation erronée, par exemple en laissant entendre que la vérification de l'intégrité de la signature seulement créerait une présomption quant à l'intégrité du message. Il a été suggéré que le projet d'article 5 traite de l'intégrité de la signature et de l'intégrité du message de données dans des dispositions distinctes. Une autre solution était que l'article 5 traite uniquement des procédures de sécurité capables de prouver à la fois l'intégrité de la signature et celle du message. Néanmoins, après un débat, il a été largement estimé que les Règles uniformes ne devaient porter que sur l'intégrité du message.

57. S'agissant de la notion de "procédure de sécurité", on a fait observer qu'une définition était peut-être nécessaire pour clarifier la relation entre une procédure de sécurité et une signature électronique ou une signature électronique "renforcée". Il faudrait peut-être intégrer la notion de "procédure de sécurité renforcée" pour traiter la question de l'intégrité du message, par opposition aux "procédures de sécurité" non qualifiées qui conviendraient peut-être à la question de l'identité du signataire. On a en général estimé que les questions liées à la définition de la "procédure de sécurité" et au niveau de sécurité nécessaire pour établir une présomption seraient peut-être résolues par l'application du projet d'article 6, selon lequel ce qui constituait une "procédure de sécurité" acceptable serait déterminé par une autorité compétente ou par convention entre les parties.

58. Quant à la question de savoir si la procédure de sécurité devait être appliquée par le signataire uniquement, le sentiment largement partagé était qu'il fallait dépersonnaliser le libellé du paragraphe 1. Il a été jugé que l'on rendrait ainsi mieux compte des situations (qui, disait-on, revêtaient une importance considérable dans la pratique) dans lesquelles la procédure de sécurité ne serait pas seulement "appliquée" par le signataire, mais supposerait également l'intervention de la partie se fiant à la signature.

59. S'agissant de l'expression "capable de prouver", on a exprimé l'avis que le paragraphe 1 ne rendait pas suffisamment compte du fait que toute procédure de sécurité devait être appliquée correctement et avec succès afin de pouvoir établir l'intégrité du message de données. À cet effet, il a été proposé de remplacer les mots "capable de prouver de manière fiable" par, par exemple, "garantissant" ou "prouvant de manière fiable". On a fait valoir, à l'encontre de cette proposition, que le fait de stipuler que l'intégrité devait être prouvée pour qu'il puisse y avoir présomption d'intégrité était dénué de sens. Le projet d'article 5 avait précisément pour but de disposer que l'utilisation de certaines procédures de sécurité (qui pouvaient être évaluées selon le projet d'article 6, ou, à un stade ultérieur, par un tribunal, conformément à l'article 8 de la Loi type) permettait d'établir une présomption d'intégrité, étant donné que les procédures en question étaient "capables" de vérifier l'intégrité des messages. Néanmoins, de l'avis général, le projet d'article 5 devait préciser qu'il ne pouvait y avoir présomption d'intégrité que si la procédure de sécurité avait été appliquée correctement et avec succès.

60. S'agissant de l'expression "sauf preuve contraire", placée entre crochets, on a fait observer qu'elle ne constituait qu'une très faible présomption dans la mesure où toute preuve contraire permettrait de la réfuter. Le projet d'article 5 formulait une présomption plus faible que le projet d'article 4, discordance à laquelle il faudrait peut-être remédier. On a aussi fait remarquer que le projet d'article 5 était formulé comme une présomption réfutable mais ne contenait aucune indication concernant la façon dont cette présomption pouvait être réfutée. Il a été suggéré de compléter le libellé du projet d'article en ce sens. Néanmoins, selon l'avis qui a prévalu, il était approprié que le projet d'article 5 établisse une règle de preuve, mais il serait peut-être difficile d'harmoniser plus en détail le degré de la présomption et les moyens par lesquels on pouvait la réfuter. On a généralement estimé que ces questions relevaient plutôt du droit interne applicable.

61. Afin de prendre en compte les vues et préoccupations mentionnées ci-dessus, on a proposé, pour le paragraphe 1, les variantes suivantes:

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

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

62. La variante B a bénéficié d'un appui considérable mais le Groupe de travail a décidé d'intégrer les deux variantes dans le projet révisé de Règles uniformes que le secrétariat devait établir, afin que l'on puisse en discuter à une autre session. On a fait observer qu'en fonction de la décision finale qui serait prise au sujet du contenu du paragraphe 1, il faudrait peut-être réexaminer l'emplacement du projet d'article 5. Si le texte du paragraphe 1 ne faisait aucune allusion à la notion de "signature électronique renforcée", la portée du projet d'article 5 s'en trouverait élargie et il y aurait peut-être lieu d'intégrer la disposition en question dans la section I, qui avait trait aux signatures électroniques en général, ou dans une section séparée des Règles uniformes.

Paragraphe 2

63. On a estimé que le paragraphe 2, dans l'ensemble, était acceptable quant au fond.

Article 6. Prédétermination de la signature électronique [renforcée] [sécurisée]

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

"1. Une procédure de sécurité ou une combinaison de procédures de sécurité satisfait aux exigences d'une signature électronique [renforcée] [sécurisée] si [*l'organe ou l'autorité indiqué par l'État adoptant comme compétent en la matière*] en décide ainsi...

2. Pour ce qui est de la relation entre la personne signant un message de données et toute personne se fiant au message signé, une procédure de sécurité ou une combinaison de procédures de sécurité est supposée satisfaire aux exigences d'une signature électronique [renforcée] [sécurisée] si les parties en conviennent expressément.

3. Les dispositions du paragraphe 2 ne s'appliquent pas dans les situations suivantes: [...]."

Remarques générales

65. De l'avis général, il fallait inclure un article allant dans le sens du projet d'article 6 car la prédétermination de procédures de sécurité agréées contribuerait à la sécurité et à la fiabilité des signatures électroniques et du commerce électronique en général. S'agissant de la question de l'autonomie des parties telle que prévue au paragraphe 2, le principe de la liberté contractuelle a bénéficié d'un large appui, mais l'avis général a été que cette question devait être examinée dans l'optique de l'ensemble du texte afin de déterminer quelles dispositions pouvaient être modifiées par convention (et quelles dispositions ne pouvaient l'être). On a fait observer que si le Groupe de travail décidait que les Règles uniformes devaient être intégrées à la Loi type, il faudrait examiner le rapport entre ces règles et l'article 4, lequel devrait être modifié en conséquence. Le Groupe de travail a décidé d'attendre pour examiner la question des dispositions impératives et non impératives d'avoir achevé l'examen des dispositions de fond des Règles uniformes.

Paragraphe 1

66. Le paragraphe 1 a dans l'ensemble été considéré comme offrant un moyen acceptable d'aider à prédéterminer ce qui constituait une signature électronique [renforcée] [sécurisée]. Un certain nombre de suggestions ont été faites pour en améliorer le libellé et le rendre plus clair.

67. Le Groupe de travail a rappelé qu'il avait été convenu, lors de l'examen du projet d'article 4, de substituer les mots "une procédure de sécurité" aux mots "une procédure de sécurité ou une combinaison de procédures de sécurité".

68. On a fait observer que si la décision visée au paragraphe 1 pouvait être rendue librement, on risquait de saper la confiance dans le commerce électronique, et qu'il faudrait donc exiger qu'elle soit rendue sur la base de normes internationales lorsque celles-ci existaient et étaient pertinentes. Après un débat sur cette proposition, le secrétariat a été prié d'établir un texte qui serait ajouté au paragraphe 1 et qui dirait en substance que la décision devrait être rendue "sur la base de normes techniques internationales reconnues dans la mesure où celles-ci existent".

69. Les membres se sont largement accordés à estimer qu'étant donné l'ampleur des conséquences que pouvait avoir la prédétermination de la signature électronique [renforcée], la décision visée au paragraphe 1 ne devrait pouvoir émaner que d'un organe ou d'une autorité qui se trouvait manifestement en position de rendre une telle décision ou y était manifestement autorisée, qu'il s'agisse d'une autorité publique ou d'une autorité privée désignée par les pouvoirs publics. Afin que le projet d'article indique plus clairement comment on pouvait prédéterminer qu'on avait affaire à une signature électronique "renforcée", on a proposé de remanier le paragraphe 1 en reprenant la même terminologie que dans le titre du projet d'article, c'est-à-dire en remplaçant le mot "décide" par le mot "détermine", et en mentionnant l'autorité chargée de procéder à la détermination au début de la disposition. On aboutirait alors à un libellé tel que le libellé suivant: "*[L'organe ou l'autorité indiqué par l'État adoptant comme compétent en la matière]* peut déterminer qu'une procédure de sécurité satisfait aux exigences d'une signature électronique [renforcée] [sécurisée]". Cette proposition a recueilli un large appui.

Paragraphe 2

70. L'inclusion d'une disposition du type de celle énoncée au paragraphe 2 prévoyant l'autonomie des parties a fait l'unanimité. On a fait observer que le paragraphe 2 traitait de la question de la prédétermination des signatures électroniques [renforcées] en ménageant la souplesse voulue et en tenant compte de l'importance de l'autonomie des parties dans le contexte des systèmes fermés. On a toutefois déclaré craindre que le paragraphe 2 ne permette aux parties de convenir de déroger à des exigences de formes impératives, et on a émis l'avis qu'il faudrait se borner à reconnaître l'autonomie des parties dans les limites du droit national. À cet égard, on a proposé d'ajouter à la fin du paragraphe les mots "dans la mesure où la loi les y autorise" et de supprimer le paragraphe 3. À l'appui de cette proposition, on a fait valoir que le paragraphe 3 exigeait que l'État adoptant s'attache à prendre en compte les exceptions possibles, alors que le libellé proposé réglait la question des restrictions existantes et permettrait de tenir compte des restrictions qui pourraient être imposées à l'avenir. Après avoir délibéré, le Groupe de travail a adopté cette proposition.

71. S'agissant de la forme, on a déclaré craindre que, compte tenu du sens généralement accepté des termes "personne se fiant", figurant au paragraphe 2, ces derniers soient interprétés à tort comme pouvant englober non seulement les parties ayant convenu que telle ou telle procédure satisfaisait aux exigences d'une signature [renforcée], mais aussi un tiers, avec pour résultat fâcheux que les tiers pourraient pâtir de la convention passée entre les parties. L'opinion générale a été que les parties pouvaient convenir entre elles et pour leur propre usage des effets produits par la procédure de sécurité à laquelle elles avaient recours, y compris qu'elle satisfaisait aux exigences d'une signature électronique [renforcée], et qu'il fallait que le paragraphe 2 précise que cette convention ne pouvait pénaliser quiconque n'y était pas partie. On a souligné que l'intention n'était pas que la disposition permette qu'un tiers subisse les conséquences d'une convention entre le signataire et le destinataire du message de données signé. Selon un autre point de vue, il fallait indiquer plus clairement que la disposition s'appliquait uniquement dans un contexte commercial et qu'il ne devait pas s'agir simplement de parties contractantes mais aussi de parties consentantes.

72. On s'est aussi inquiété du rapport entre l'article 7 de la Loi type, qui ne pouvait faire l'objet de dérogations conventionnelles, et le projet d'article 6. On a émis l'avis que les paragraphes 1 et 2 pouvaient donner à croire aux parties qu'en convenant de ce qui constituait une signature électronique [renforcée], elles pouvaient éviter de se conformer aux exigences de l'article 7 concernant l'équivalent fonctionnel d'une signature. Le paragraphe 2 devrait, a-t-on déclaré, disposer qu'une fois qu'une procédure de sécurité a satisfait aux exigences de la signature prévues à l'article 7 de la Loi type, les parties pourraient convenir de ce qui constituerait une signature électronique [renforcée]. On a aussi fait observer qu'en sus des situations envisagées aux paragraphes 1 et 2, il pouvait y avoir une troisième possibilité, à savoir qu'une procédure non visée par l'un de ces paragraphes puisse néanmoins correspondre à la définition d'une signature [renforcée], par exemple si elle était reconnue comme telle par un tribunal. Cette question n'a pas été débattue.

Révision proposée du projet d'article 6

73. Il a été proposé de réviser le projet d'article 6 en tenant compte des remaniements qui avaient été discutés et convenus au sujet du paragraphe 1. Selon cette proposition, le paragraphe 1 devait être scindé en deux parties, la première traitant de la détermination qu'une procédure de sécurité satisfaisait aux exigences d'une signature électronique, et la seconde traitant des procédures de sécurité qui satisfaisaient aux exigences d'intégrité énoncées au projet d'article 5. Un nouveau paragraphe 2 permettrait aux parties de déterminer l'effet juridique de leur signature. Un libellé tel que le libellé ci-après a été proposé:

> "1. *[L'organe ou l'autorité indiqué par l'État adoptant comme compétent en la matière]* peut déterminer :
>
> a) qu'une signature électronique satisfait aux [exigences] de l'alinéa *b* de l'article premier; ou
>
> b) qu'une procédure de sécurité satisfait aux exigences de l'article 5.
>
> 2. Pour ce qui est de la relation entre la personne signant un message de données et toute personne se fiant au message signé, les parties peuvent déterminer l'effet d'une signature ou d'une procédure de sécurité si elles en conviennent expressément, sous réserve des présentes Règles et du droit applicable."

74. Le Groupe de travail a dans l'ensemble accepté le texte proposé, sous réserve de certaines modifications de forme. On a notamment proposé de placer les mots "des présentes Règles et" entre crochets en attendant que le Groupe de travail se prononce sur la question du respect des dispositions impératives des Règles uniformes. Cette proposition a été acceptée, et le Groupe de travail a décidé de reporter le débat concernant la question de la détermination des dispositions des Règles uniformes qui devaient revêtir un caractère impératif ainsi que le débat sur les questions touchant au droit de la protection des consommateurs.

75. On a demandé ce qu'il faudrait entendre par "les parties peuvent déterminer l'effet" de la signature. On a notamment objecté que les parties ne pouvaient convenir de l'effet juridique des signatures, mais qu'elles pouvaient se mettre d'accord sur la façon dont elles devraient signer un message de données. Selon un autre point de vue, les parties ne pouvaient convenir de conférer tel ou tel statut juridique à telle ou telle forme de signature, mais elles pouvaient convenir de l'effet juridique qu'aurait une forme particulière de signature. Selon un autre point de vue encore, la disposition énoncée au paragraphe 2 devrait viser uniquement une forme particulière de signature. Après un débat, il a été décidé de placer les mots "l'effet" entre crochets en attendant que leur signification ait été éclaircie. Le Secrétariat a été prié d'élaborer une version révisée du projet d'article 6 en tenant compte des débats relatés ci-dessus.

Article 7. Responsabilité pour une signature électronique [renforcée] [sécurisée]

76. Le projet d'article 7 examiné par le Groupe de travail était le suivant:

> "*Variante A*
>
> Lorsque l'utilisation d'une signature électronique [renforcée] [sécurisée] n'a pas été autorisée et lorsque le signataire supposé n'a pas exercé un soin raisonnable pour en éviter une utilisation non autorisée et pour empêcher que le destinataire ne s'y fie, le signataire supposé est tenu responsable du préjudice causé [et doit verser des dommages-intérêts à la partie s'étant fiée à sa signature], sauf si la partie s'étant fiée à la signature savait ou aurait dû savoir qu'elle n'était pas celle du signataire supposé.

Variante B

Lorsque l'utilisation d'une signature électronique [renforcée] [sécurisée] n'a pas été autorisée et que le signataire supposé n'a pas exercé un soin raisonnable pour en éviter l'utilisation non autorisée et empêcher que le destinataire ne s'y fie, ladite signature est néanmoins considérée comme la sienne, sauf si la partie qui s'y est fiée savait ou aurait dû savoir qu'elle n'était pas celle du signataire supposé."

77. On a suggéré de remanier le titre du projet d'article afin qu'il indique que l'objet de l'article est l'utilisation d'une signature sans autorisation. On pourrait par exemple intituler le projet d'article : "Responsabilité en cas d'utilisation non autorisée d'une signature électronique [renforcée] [sécurisée]".

78. Quant à la portée de l'article, on a proposé d'étendre la règle régissant la responsabilité en cas d'utilisation non autorisée d'une signature renforcée aux signatures électroniques ordinaires. On a par ailleurs proposé de restructurer l'article 7 pour distinguer entre les cas où: a) l'utilisation non autorisée de la signature résultait de l'intervention frauduleuse d'un pirate informatique; b) la signature était utilisée sans autorisation par un employé ou ancien employé du signataire supposé; ou c) la signature était utilisée par un employé ayant une autorisation, mais à des fins autres que celles autorisées.

79. Des délégations ont dit que, pour éviter toute ingérence dans le droit interne des contrats et de la représentation, c'était le droit interne applicable qui devait réglementer la matière faisant l'objet du projet d'article 7, qui devrait donc être supprimé. Le débat a essentiellement porté sur les variantes A et B.

Variante A

80. La variante A a bénéficié d'un large appui. On a fait observer qu'une telle disposition était nécessaire pour indiquer clairement que le signataire supposé ne pouvait répudier sa signature en se contentant d'indiquer, en vertu du projet d'article 4, qu'elle avait été utilisée sans autorisation. Outre l'absence d'autorisation visée au projet d'article 4, le signataire supposé devait aux termes de l'article 7 montrer qu'il n'avait pas été négligent s'agissant de protéger sa signature contre les utilisations non autorisées. Dans ce contexte, on a dit que dans le cadre de la variante A, la charge de la preuve n'était peut-être pas appropriée. En effet, aux termes de cette variante, la partie qui se fiait à la signature devrait prouver que le signataire supposé n'avait pas exercé le soin raisonnable nécessaire pour éviter l'utilisation non autorisée de sa signature. On a dit que cette disposition pourrait devoir être remaniée afin d'inverser la charge de la preuve, de telle manière qu'il appartienne au signataire supposé de prouver qu'il a exercé le soin raisonnable nécessaire pour protéger sa signature électronique.

81. À l'appui de la variante A, on a fait observer par ailleurs que cette disposition était, comme il convenait, axée sur les questions de responsabilité, à la différence de la variante B, qui risquait d'être excessivement lourde pour le signataire supposé si on l'interprétait comme liant strictement ce dernier au contenu du message authentifié au moyen d'une signature non autorisée.

82. Des objections ont toutefois été formulées contre la variante A, notamment qu'il n'était peut-être pas approprié de créer une norme de "soin raisonnable" s'agissant de pratiques nouvelles comme les signatures électroniques, qui se développaient dans un environnement technique en mutation rapide et ne pouvaient s'appuyer sur des usages ou pratiques établis. À cet égard, une disposition comme la variante A risquait de décourager l'utilisation des signatures électroniques en fixant une norme trop stricte. La simple référence à la notion de "responsabilité" dans une disposition concernant les signataires supposés et les parties se fiant à une signature risquait de dissuader les utilisateurs potentiels de la signature électronique de s'en servir. À cet égard, la variante B, qui évitait toute mention de la notion de responsabilité, était peut-être plus acceptable (voir ci-après, par. 84).

83. On a répondu à cet argument que, dans de nombreux pays, la norme de soin raisonnable établie dans la variante A était déjà applicable au commerce électronique, étant une règle de conduite généralement applicable en vertu du droit interne. Si les dispositions de la variante A n'étaient peut-être pas nécessaires dans les pays en question, l'harmonisation internationale du droit concernant cette question pourrait être utile. Il serait certes peu judicieux que les règles uniformes tentent d'unifier le droit applicable à l'indemnisation du préjudice purement économique ou interviennent autrement dans le droit des contrats ou de la responsabilité civile, mais le Groupe de travail ne devait pas craindre d'éclaircir les règles de conduite fondamentales qui devaient guider les parties lorsqu'elles utilisaient les signatures électroniques. On a aussi fait observer que le critère de soin raisonnable prévu dans la variante A était suffisamment souple pour faire leur place aux pratiques nouvelles qui se faisaient jour dans le domaine du commerce électronique. En outre, la norme de conduite énoncée dans la variante A était peut-être moins rigoureuse que les normes de conduite applicables dans certains domaines en droit interne. De plus, on a fait observer que, loin de décourager l'utilisation des signatures électroniques, l'existence de normes de conduite uniformes connues accroîtrait vraisemblablement la confiance dans le commerce électronique en général, pourvu que ces normes reflètent suffisamment la pratique des milieux commerciaux.

Variante B

84. La variante B a recueilli un appui limité. On a dit à juste titre que cette variante était axée sur l'attribution de la signature électronique renforcée dans les cas où celle-ci n'était pas autorisée, tout en laissant aux tribunaux le soin de trancher la question de la responsabilité sur la base du droit interne. Dans ce contexte, on a suggéré de remanier la variante B de manière à limiter son application dans le temps, à y inclure un élément de prévisibilité du montant des dommages-intérêts pouvant résulter de l'utilisation non autorisée de la signature, et à indiquer clairement que la perte de bénéfices attendus ne relevait pas du champ d'application du projet d'article 7. On a, à défaut, proposé de la remanier comme suit:

> "Lorsque l'utilisation d'une signature électronique [renforcée] [sécurisée] n'a pas été autorisée et que le signataire supposé n'a pas exercé un soin raisonnable pour en éviter l'utilisation non autorisée et empêcher que le destinataire ne s'y fie, ladite signature est néanmoins considérée comme autorisée, sauf si la partie qui s'y est fiée savait ou aurait dû savoir qu'elle ne l'était pas."

85. De l'avis général, le projet d'article 7 pouvait demeurer entre crochets dans le projet de règles uniformes en attendant la poursuite du débat lors d'une session ultérieure. On estimait généralement qu'il serait peut-être nécessaire de revenir sur la question de la responsabilité du signataire supposé en cas de négligence dans la protection de sa signature électronique à l'occasion de l'examen du projet d'article 13-2, qui énonçait une obligation de révoquer un certificat si la clef privée avait été compromise.

86. Pour tenir compte des diverses opinions et préoccupations exprimées au sujet des variantes A et B, on a proposé ce qui suit comme révision possible du projet d'article 7:

> "Lorsque 1) l'utilisation d'une signature électronique [renforcée] [sécurisée] n'a pas été autorisée; 2) que le destinataire s'est à son détriment fié de bonne foi à la signature; et 3) que le signataire supposé n'a pas exercé un soin raisonnable pour éviter l'utilisation non autorisée de sa signature et empêcher que le destinataire ne s'y fie, la signature est attribuable au signataire supposé aux fins de la responsabilité du coût de rétablir les parties dans la position dans laquelle elles se trouvaient avant l'utilisation non autorisée de la signature. Ce qui précède ne s'applique pas dans la mesure où le destinataire savait ou aurait dû savoir que la signature n'était pas autorisée."

87. On a aussi proposé de remanier ce projet d'article 7 comme suit:

"Lorsque l'utilisation d'une signature électronique [renforcée] [sécurisée] n'a pas été autorisée et que le signataire supposé n'a pas exercé un soin raisonnable pour en éviter une utilisation non autorisée et empêcher que le destinataire ne s'y fie, le signataire supposé ne peut être tenu responsable que du coût du rétablissement des parties dans la situation qui était la leur avant l'utilisation non autorisée de la signature, sauf si la partie qui s'y est fiée savait ou aurait dû savoir que cette signature n'était pas celle du signataire supposé."

88. Après un débat, le Groupe de travail a décidé que les divers textes proposés pour le projet d'article 7 devaient figurer en tant que variantes dans la version révisée des Règles uniformes qui serait établie pour examen lors d'une session ultérieure, en même temps que le texte de la variante A figurant dans la note du Secrétariat.

Section III. Signatures numériques accompagnées de certificats

Article 8. Teneur d'un certificat [renforcé] [sécurisé]

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

"Aux fins des présentes Règles, un certificat [renforcé] [sécurisé] remplit au minimum les fonctions suivantes:

a) il identifie l'autorité de certification qui l'émet;

b) il nomme ou identifie le [signataire] [sujet du certificat] ou un dispositif ou un agent électronique sous le contrôle [du signataire] [du sujet du certificat] [de cette personne];

c) il contient une clef publique correspondant à une clef privée dont [le signataire] [sujet du certificat] a le contrôle;

d) il spécifie sa période d'effet;

e) il est signé numériquement ou sécurisé d'une autre manière par l'autorité de certification qui l'émet;

[f) il spécifie, le cas échéant, les restrictions à l'utilisation de la clef publique;]

g) il identifie l'algorithme à appliquer]."

Remarques générales

90. Au début du débat sur le projet d'article 8, on s'est interrogé sur le rapport entre cet article et la définition d'une signature électronique renforcée figurant à l'alinéa *b* du projet d'article premier. Le Groupe de travail a reconnu que les définitions figurant dans le projet d'article premier des Règles uniformes devraient être examinées lors d'une session ultérieure, une fois que l'élaboration des articles portant sur le fond aurait été terminée, mais il a estimé qu'il faudrait garder à l'esprit la teneur possible des définitions pour déterminer quels éléments devraient nécessairement figurer dans les dispositions de fond.

91. Des questions ont également été soulevées au sujet de la technologie sur laquelle était fondé le projet d'article 8. On a fait observer que celui-ci supposait une triple certification faisant intervenir, outre le signataire et le destinataire d'un message de données, une autorité de certification indépendante. Or, la tendance dans

l'usage commercial était actuellement à la double certification, et l'on a émis l'avis que le projet d'article risquait de ne pas convenir dans ce contexte. À cet égard, on a demandé notamment si l'inclusion d'un article tel que le projet d'article 8 aurait des répercussions négatives sur la double certification, s'il faudrait établir une règle analogue pour cette dernière, ou si celle-ci devrait être spécifiquement exclue du champ d'application du projet d'article 8. On a répondu que si la double certification était largement contractuelle, il y avait des situations dans lesquelles un tiers pouvait se fier à la signature et qu'il importait de sauvegarder ses intérêts. On a émis l'avis que même si ce cas de figure semblait ressembler à la situation d'une partie se fiant à la signature dans le cadre d'une triple certification, il serait difficile d'élaborer une disposition qui puisse s'appliquer à la fois à la double et à la triple certification. La plupart des membres ont estimé que le Groupe de travail devrait attendre pour trancher la question de savoir si le projet d'article 8 devait s'appliquer à la double certification ou si celle-ci devait au contraire être exclue de son champ d'application.

92. On a aussi fait observer que si l'inclusion d'une liste des exigences auxquelles devrait satisfaire l'émetteur d'un certificat pourrait rendre plus sûre l'utilisation des signatures numériques, l'évolution de la technologie était si rapide qu'une telle liste risquerait d'être vite dépassée.

93. On a déclaré qu'on ne voyait pas très bien, à la lecture du projet d'article 8, quelles conséquences entraînerait un certificat qui ne comporterait pas toutes les informations énoncées aux alinéas *a* à *g*, quel était l'objet du projet d'article et comment il s'articulait avec les projets d'articles 9 et 10. On s'est demandé si cet article était même nécessaire. On a fait observer que les obligations qu'imposaient les projets d'articles 9 et 10, qui établissaient le lien entre les clefs publiques et privées et rattachaient les deux clefs à l'identification du signataire, étaient au coeur même de la notion de certificat renforcé accompagnant une signature renforcée et ne pouvaient être dissociées du projet d'article 8. Il a été convenu que ces questions étaient essentielles pour déterminer s'il fallait inclure un article tel que le projet d'article 8 et comment celui-ci devrait être libellé. On s'est aussi interrogé sur le rapport entre le projet d'article 8 et l'article 7 de la Loi type. À cet égard, on a fait observer qu'il ne fallait pas présumer que s'il était satisfait aux exigences du projet d'article 8, il serait aussi automatiquement satisfait à celles de l'article 7. On a aussi fait remarquer que certaines exigences du projet d'article 8, y compris les alinéas *d* à *g*, ne contribuaient pas à établir la fiabilité de la signature en respectant les critères énoncés à l'article 7 de la Loi type. La question du rapport entre les deux articles n'a pas été réglé lors de l'examen du projet d'article 8, mais le Groupe de travail a décidé qu'il y reviendrait dans le cadre de l'examen des projets d'articles 9 et 10.

94. Des opinions divergentes ont été exprimées au sujet des conséquences que pourrait entraîner un certificat qui ne satisferait pas aux exigences du projet d'article 8. Selon une opinion, l'utilisation du certificat pourrait être interdite par les Règles uniformes et les autres dispositions de la section III ne s'appliqueraient pas. On a objecté qu'une telle conséquence serait hors de proportion avec les exigences des alinéas *a* à *g*. Selon une autre opinion, la signature accompagnée du certificat serait toujours considérée comme une signature numérique, mais sans doute plus comme une signature renforcée. Les règles concernant les signatures numériques non accompagnées d'un certificat s'appliqueraient. Selon une autre opinion encore, le certificat ne ferait plus de la signature qu'il accompagne une signature renforcée, mais la signature pourrait tout de même être considérée comme une signature renforcée au sens de l'alinéa *b* du projet d'article premier; les seules différences seraient que les facilités offertes par la section III ne seraient pas applicables et qu'il faudrait apporter la preuve que la signature réunit tous les éléments de la définition figurant à l'alinéa *b* du projet d'article premier. Selon encore une autre opinion, le certificat ne serait pas considéré comme un certificat aux fins des Règles uniformes, ou il le serait, mais son émetteur pourrait voir sa responsabilité engagée pour présentation fallacieuse des faits s'il cherchait à le faire passer pour un certificat faisant d'une signature une signature renforcée. Selon une opinion proche de la précédente, l'autorité de certification ne devrait pas pouvoir se soustraire à sa responsabilité en tirant argument du fait que le certificat qu'elle avait émis ne remplissait pas les conditions d'un certificat renforcé. Dans une telle situation, l'autorité de certification devrait être considérée comme ayant émis un certificat renforcé. Le Groupe de travail n'a pu se mettre d'accord sur les conséquences

qu'entraînerait un certificat qui ne serait pas conforme aux dispositions du projet d'article 8. Il a toutefois estimé qu'il n'était pas nécessaire qu'il parvienne à un tel accord pour le moment, mais qu'il faudrait qu'il revienne sur cette question lorsqu'il examinerait les autres dispositions de la section III.

95. Il a été proposé que puisque le projet d'article 5, tel qu'il avait été révisé par le Groupe de travail, comportait des dispositions applicables aux certificats et signatures à utiliser pour sécuriser l'intégrité du message de données (qui diffère de l'identification), cette distinction devrait être indiquée dans le projet d'article 8. Cette proposition n'a guère été appuyée.

96. Sur le plan de la forme, l'emploi du terme "signataire" a recueilli un certain soutien. Mais on a aussi estimé que ce terme, au contraire, ne convenait pas dans le contexte de l'émission d'un certificat, lorsque les parties étaient l'émetteur et le sujet du certificat. Seulement dans les cas où un certificat avait été émis et où le sujet du certificat avait effectivement signé un document, pouvait-on dire qu'il y avait un "signataire". Selon un autre point de vue, l'emploi du terme "signataire" exclurait potentiellement les agents électroniques. On a également fait observer que lorsqu'il y avait un intermédiaire, le véritable signataire n'était pas le "signataire" au sens de sujet du certificat. On a estimé que l'expression "le sujet du certificat" lèverait l'incertitude associée à l'emploi du terme "signataire". Il a été convenu que le débat sur la terminologie devrait être rouvert à une session future sur la base du projet révisé établi par le Secrétariat.

97. On a estimé qu'il faudrait ajouter une nouvelle disposition après l'alinéa *b* pour couvrir les attributs d'un signataire autres que l'identité. Il a été proposé d'ajouter dans un nouvel alinéa *c* une disposition qui pourrait être ainsi conçue: "il identifie un attribut précis [du signataire] tel que l'adresse, le pouvoir d'agir au nom d'une société, ou l'existence de permis ou licences spécifiques". Cette proposition n'a guère été soutenue.

Chapeau

98. Sur le plan de la forme, il a été proposé d'ajouter le membre de phrase "et dans le contexte des signatures numériques" après le mot "Règles" afin de préciser la portée de cette disposition. Il a également été proposé que le chapeau établisse une obligation positive ayant un caractère contraignant pour l'émetteur du certificat, plutôt qu'une norme fixant des critères minimaux à remplir pour qu'il puisse s'agir d'un certificat renforcé. On a estimé en outre que le projet d'article 8 devrait offrir une possibilité de dérogation par voie d'accord entre les parties. Le texte ci-après a été proposé:

> "Aux fins des présentes Règles et dans le contexte des signatures numériques, l'émetteur d'un certificat [renforcé] [sécurisé] fournit au minimum les informations ci-après dans le certificat, en l'absence d'accord contraire:"

99. Si la proposition tendant à modifier le texte du projet d'article 8 pour que, de norme impersonnelle, il devienne une obligation à caractère contraignant pour l'émetteur, la référence à l'autonomie des parties a été critiquée pour les mêmes raisons que celles évoquées dans le contexte du projet d'article 6 concernant l'effet éventuel d'un accord de ce type sur les tierces parties. On a également émis l'avis que la possibilité de dérogation par voie d'accord aurait pour effet de faire du projet d'article 8 une règle par défaut plutôt qu'une norme minimale. On a fait observer à cet égard que l'objectif initial de cet article était d'établir une norme minimale concernant l'information à fournir sur le certificat et que cela faciliterait l'harmonisation des pratiques d'authentification et renforcerait la confiance dans le commerce électronique. En réponse à ces critiques, il a été proposé de mettre entre crochets l'expression "en l'absence d'accord contraire" en attendant que la question de l'autonomie des parties soit examinée plus avant.

100. Une autre proposition concernant le champ d'application du projet d'article 8 préconisait que ce projet s'applique à tous les certificats et que la référence aux certificats renforcés soit supprimée. Les adversaires de

cette proposition ont fait valoir que le projet d'article 8 avait pour seul objet de valider les signatures renforcées et ont donc proposé le texte ci-après:

> "Aux fins des présentes Règles, un certificat émis pour valider une signature renforcée remplit au minimum les fonctions suivantes:"

Bien que cette proposition n'ait pas été appuyée, ces termes ont été repris dans une proposition ultérieure relative à un nouveau projet d'article 8 (voir plus loin par. 112).

101. Selon une autre proposition encore relative au champ d'application du projet d'article 8, il faudrait peut-être que le terme "émission" ne recouvre que la remise du certificat au sujet du certificat, ce qui supposait une relation contractuelle entre l'autorité de certification et le sujet du certificat et non la divulgation par l'autorité de certification de l'information contenue dans le certificat à toute tierce partie intéressée. Une telle disposition pourrait s'appliquer à n'importe quel type de certificat, qu'il soit renforcé ou non. Pour donner effet à cette proposition, le texte ci-après a été présenté:

> "Une autorité de certification doit s'assurer que, lors de la divulgation à une partie des informations contenues dans un certificat, au minimum les renseignements figurant au paragraphe 2 sont divulgués. La disposition qui précède s'applique sauf convention expressément contraire entre l'autorité de certification et la partie en question."

102. Dans le cadre de cette proposition, on a déclaré que le paragraphe 2 devrait inclure les alinéas *a* à *g* du projet d'article 8. Certaines délégations se sont déclarées favorables à cette inclusion et ces termes ont été repris dans une proposition ultérieure relative à un nouveau projet d'article 8 (voir plus loin par. 114).

Alinéa a)

103. Le Groupe de travail a convenu que la teneur de la disposition énoncée à l'alinéa *a* était généralement acceptable.

Alinéa b)

104. Il a été souligné que les termes "un dispositif ou un agent électronique" représentaient un concept nouveau dans les Règles uniformes et qu'il conviendrait de les définir. Il a été avancé, à l'appui de cette proposition, que les Règles uniformes devaient contenir des dispositions claires relatives aux situations dans lesquelles un système pourrait être mis en marche par un utilisateur puis fonctionner de manière autonome, s'agissant notamment de signer des messages de données et être le destinataire d'un certificat.

Alinéa c)

105. Une préoccupation exprimée au sujet de l'alinéa *c* avait trait au fait qu'il n'était pas nécessaire de faire référence à la clef publique dans le certificat car il existait d'autres moyens d'obtenir les informations. Il a été proposé de remplacer l'expression "contient une clef publique" par "identifie une clef publique".

Alinéa d)

106. Certains membres du Groupe de travail ont reproché à l'alinéa *d* le manque de clarté de l'expression "période d'effet". Il a été proposé de substituer à l'énoncé actuel l'énoncé suivant : "il spécifie la période durant laquelle le certificat peut être utilisé aux fins de la vérification d'une signature numérique"; un avis contraire a été émis, selon lequel la période d'effet d'un certificat était la période au cours de laquelle une

signature numérique valide pouvait être créée. Si une signature devenait caduque, le certificat pourrait toujours être utilisé pour vérifier une signature apposée avant le moment où elle est devenue caduque. Il a été généralement convenu de retenir l'énoncé actuel de l'alinéa *d*.

Alinéa e)

107. Les membres du Groupe de travail se sont généralement accordés sur l'inclusion de l'alinéa *e* dans le projet d'article 8. Pour plus de clarté, et du fait que la validité du certificat dépend de sa signature par celui qui l'émet, il a été proposé d'insérer cet alinéa à la suite du projet d'alinéa *a*.

Alinéa f)

108. L'examen de l'alinéa *f* était axé sur l'incorporation par référence. Les membres du Groupe de travail souhaitaient conserver l'alinéa et supprimer les crochets du fait que l'objet du projet d'article 8 était de fournir des informations à la partie contractante et à la partie se fiant à la signature. De l'avis d'un intervenant, il était donc essentiel que si des restrictions devaient figurer sur le certificat, elles soient clairement imprimées au recto du certificat lui-même. Les partisans de la suppression de l'alinéa *f* ont fait valoir que le certificat pouvait comporter toutes sortes de restrictions figurant dans divers autres documents (déclaration relative aux pratiques d'authentification, par exemple). Étant donné que ces restrictions devraient être spécifiées d'une manière "humainement" lisible à l'intention de l'utilisateur, au lieu d'être incorporées au certificat par référence à des codes d'identification, il pourrait dans certains cas être techniquement impossible d'inclure dans le certificat la quantité d'informations requise par les dispositions de la règle en question.

109. Il a été répondu à cette critique que si des restrictions s'appliquaient au certificat, il suffirait tout simplement d'"indiquer" sur le certificat l'existence de restrictions, plutôt que de spécifier les restrictions elles-mêmes.

110. Il a également été proposé d'ajouter à l'alinéa *f* un alinéa précisant que "lorsque les restrictions ne sont pas spécifiées sur le certificat, le certificat ne peut être utilisé au détriment de tiers". Cette proposition n'a pas été approuvée. Une autre proposition a été faite, selon laquelle il devrait être possible de reconnaître une "version abrégée du certificat" à condition: de préciser sur le certificat lui-même qu'il s'agit d'une version abrégée; d'indiquer sur le certificat où se trouvent les données n'y figurant pas; et de donner à une partie demandant des renseignements la possibilité d'accéder à l'information. Cette proposition a été approuvée par certains membres du Groupe de travail. À l'issue d'un débat approfondi, le Groupe de travail a convenu que la question de l'incorporation par référence soulevait un certain nombre de difficultés qui avaient déjà été examinées au moment de la rédaction de l'article 5 *bis* de la Loi type. Il a été avancé que l'article 5 *bis* stipulait que la question de l'incorporation par référence ne pouvait être résolue dans le contexte du commerce électronique tant qu'elle n'aurait pas été résolue selon le droit général, et que les travaux du Groupe de travail ne permettraient pas d'aboutir à une telle solution. Selon un avis contraire, puisque l'article 5 *bis* ne couvrait pas toutes les questions concernant l'incorporation par référence du fait que son libellé était entièrement négatif, la question devait être traitée dans les Règles uniformes. Après délibération, le Groupe de travail a décidé que la question de l'incorporation par référence devait être résolue selon le droit national.

Alinéa g)

111. Si certains membres étaient partisans de conserver l'alinéa *g*, on a généralement reconnu qu'il n'était pas aussi important que les alinéas *a* à *f*.

Propositions concernant un nouvel article 8

112. En réponse aux objections selon lesquelles le projet d'article 8 était trop détaillé et serait probablement rendu caduc par l'évolution des techniques, le texte ci-après a été proposé comme une autre variante possible pour ce projet d'article:

> "Aux fins des présentes Règles, un certificat renforcé comprend, au minimum, ou [lorsqu'il est techniquement difficile de procéder ainsi] résume et référence, des informations suffisantes pour [satisfaire aux exigences de la procédure de sécurité applicable] remplir la fonction qui lui est assignée]."

Cette proposition n'a reçu qu'un soutien limité.

113. Une autre proposition portant sur un nouveau projet d'article 8 était fondée sur l'idée que les alinéas du projet d'article n'avaient pas tous la même importance et qu'il y avait deux catégories d'éléments, ceux qui devaient être impérativement précisés et ceux pour lesquels une omission n'entraînait pas nécessairement la perte du statut renforcé, mais seulement la perte de l'aptitude à faire valoir ce statut à l'encontre de tiers. Pour défendre cette idée, on a dit que les alinéas *d* à *g* ne prévoyaient pas la nécessité d'établir une identification soit pour les clefs publiques et privées et leur fonction en tant que paire, soit pour le détenteur de la paire de clefs, comme le faisaient les projets d'articles 9 et 10. On a fait observer qu'il pourrait être difficile de satisfaire à ces exigences dans certains cas, compte tenu des pratiques suivies en matière de certification. Par conséquent, les éléments indiqués dans les alinéas *d* à *g* n'étaient pas indispensables pour un certificat renforcé. On a déclaré, en revanche, que les alinéas *a* à *c* étaient essentiels pour l'objet du projet d'article 8, qu'ils formaient la substance des projets d'articles 9 et 10 des Règles uniformes et faisaient apparaître le lien entre le projet d'article 8 et les projets d'articles 9 et 10.

114. Une autre proposition également fondée sur l'idée que les alinéas du projet d'article 8 n'avaient pas tous la même importance était libellée comme suit:

> "1. En communiquant à une quelconque partie les informations contenues dans un certificat, une autorité de certification [ou le sujet d'un certificat] s'assure que lesdites informations comprennent au moins les éléments énumérés au paragraphe 2, sauf dans les cas où l'autorité de certification [ou le sujet, selon le cas] et ladite partie en conviennent expressément autrement.
>
> *Variante A* 2. Les informations visées au paragraphe 1 sont les suivantes:
>
> i) pour tous les certificats, [les éléments a) à c) et e) du projet d'article 8], et
>
> ii) pour les certificats [...], [les éléments d), f) et g) du projet d'article 8].
>
> *Variante B* 2. Les informations visées au paragraphe 1 sont [les éléments a) à c) et e) du projet d'article 8].
>
> 3. Les certificats peuvent également contenir d'autres informations, notamment [les éléments d), f) et g)]."

115. En ce qui concerne la nature des certificats visés à l'alinéa *ii* de la variante A, il n'a pas été possible de parvenir à un accord. Selon un avis largement partagé, cette disposition ne devait ni faire référence aux certificats renforcés ni décrire le certificat par référence à la signature qu'il comportait. On a fait observer que les alinéas *a* à *g* nécessiteraient des remaniements. Il a été proposé de supprimer les mots "l'autorité de certification" et de les remplacer par les mots "l'émetteur du certificat".

116. La révision proposée dans le libellé du projet d'article 8, telle qu'elle est indiquée au paragraphe 26 plus haut, a recueilli une large adhésion, certains exprimant une préférence pour la variante B. Au terme d'un débat, le Groupe de travail a convenu que, pour les travaux à venir, il faudrait inclure dans la version révisée du projet d'article 8 la proposition ci-dessus [y compris les variantes A et B de l'alinéa *ii* et du paragraphe 3] et le texte présenté dans le document A/CN.9/WG.IV/WP.76.

Article 9. Effet des signatures numériques accompagnées de certificats

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

"1. Pour ce qui est de la totalité ou de toute partie d'un message de données, où l'expéditeur est identifié par une signature numérique, ladite signature [est une signature électronique [renforcée] [sécurisée]] [satisfait aux conditions de l'article 7 de la Loi type de la CNUDCI sur le commerce électronique] si:

a) elle a été créée de manière sûre pendant la période d'effet d'un certificat valide et est vérifiée de manière sûre par référence à la clef publique indiquée dans le certificat; et

b) le certificat rattache une clef publique à l'identité [du signataire] [d'une personne] pour les raisons suivantes:

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

iv) des preuves suffisantes font apparaître que le certificat rattache [avec précision] la clef publique à l'identité du [signataire] [sujet].]

[2. Lorsqu'un message de données est signé à l'aide d'une signature numérique [créée pendant la période d'effet d'un certificat] qui ne satisfait pas aux conditions énoncées au paragraphe 1, cette signature est considérée comme une signature électronique [renforcée] [sécurisée] s'il existe des preuves suffisantes montrant que [le certificat] rattache avec précision la clef publique à l'identité du [signataire] [sujet du certificat].]

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

Remarques générales

118. On s'est demandé si cet article était bien à sa place dans la section III et on a proposé d'inverser l'ordre des projets d'articles 8 et 9, les effets des signatures numériques accompagnées de certificats étant présentés avant la disposition relative au contenu des certificats.

Paragraphe 1

Chapeau

119. On a reconnu dès le départ que le sens et l'objet du projet d'article 9 dépendaient des mots placés entre crochets que l'on conserverait dans le chapeau du paragraphe 1. Selon une opinion, les mots entre crochets qui contenaient une référence à l'article 7 de la Loi type auraient un effet juridique, alors que ceux visant une "signature électronique [renforcée] [sécurisée]" aboutiraient à une déclaration quant aux signatures numériques pouvant être considérées comme des signatures électroniques [renforcées] [sécurisées] si les conditions étaient réunies. De l'avis général, il fallait conserver les mots [est une signature [renforcée] [sécurisée]] en supprimant les crochets plutôt que le membre de phrase contenant une référence à l'article 7 de la Loi type.

Alinéa a)

120. Le débat a essentiellement porté sur le point de savoir si l'utilisation de l'expression "de manière sûre", à l'alinéa *a* était justifiée. À l'appui de son maintien, on a rappelé qu'elle avait été insérée dans les Règles uniformes pour mieux rendre compte de la fiabilité nécessaire du processus de signature numérique, ce qui est essentiel dans le cadre de la notion de signature électronique [renforcée] [sécurisée]. On a estimé que les mots "de manière sûre" pourraient être supprimés à l'alinéa *a* si le chapeau contenait une référence à l'article 7 de la Loi type, une telle référence postulant le niveau nécessaire de fiabilité. Comme le Groupe de travail avait décidé que le chapeau du paragraphe 1 ne devait pas viser l'article 7 de la Loi type, il fallait conserver l'expression "de manière sûre" à l'alinéa *a* pour garantir la sûreté de la signature numérique, car toutes les signatures numériques vérifiables par référence à un certificat n'étaient pas nécessairement sûres, notamment en cas d'incertitude quant à l'exactitude de l'identification du signataire ou de la clef publique. Selon une proposition, non seulement il fallait conserver l'expression à l'alinéa *a*, mais il fallait l'expliciter en ajoutant le texte suivant:

> "Une signature numérique est créée de manière sûre et vérifiée de manière sûre si elle est créée au moyen:
>
> a) d'éléments techniques pour la création et la vérification de la signature numérique qui révéleraient de manière fiable une signature numérique contrefaite et des données signées manipulées et qui fournissent une protection contre l'utilisation non autorisée de clefs privées de signature; et
>
> b) d'éléments techniques pour la présentation des données à signer qui indiquent clairement à l'avance la création de signatures numériques et permettent d'identifier les données auxquelles une signature numérique s'applique; et
>
> c) ces éléments techniques doivent avoir été adéquatement testés compte tenu des normes actuelles d'ingénierie."

121. Nombre de délégations ont estimé que cette proposition était trop détaillée pour figurer dans le corps des Règles uniformes. Toutefois, des explications telles que celles y figurant pouvaient être très utiles dans le cadre d'un guide d'application des Règles uniformes.

122. La proposition de supprimer les mots "de manière sûre" à l'alinéa *a* a été vigoureusement appuyée. On a dit que l'utilisation de cette expression introduisait, en ce qui concerne la création et la vérification d'une signature numérique, une nouvelle notion qui était incertaine et ambiguë.

123. Du point de vue de la rédaction, on a dit que le texte de l'alinéa *a* devait indiquer clairement que tant la création de la signature que sa vérification devaient avoir lieu durant la période d'effet d'un certificat. Selon une opinion contraire, la période d'effet ne concernait que la vérification d'une signature numérique et l'alinéa *a* devait être révisé: il fallait supprimer les mots "de manière sûre" en ce qui concerne la vérification et ajouter les mots "et durant la période pendant laquelle la vérification est autorisée" à la fin de l'alinéa.

124. Après un débat, le Groupe de travail n'a pu parvenir à un consensus en ce qui concerne l'emploi de l'expression "de manière sûre" à l'alinéa *a*. Il a été décidé que dans les variantes du projet d'article 9 qui seraient établies en vue de la poursuite du débat à une session ultérieure, la possibilité de conserver ou de supprimer les mots "de manière sûre" devait être prévue (voir ci-après, par. 133).

Alinéa b)

Chapeau

125. Le membre de phrase liminaire de l'alinéa *b* a fait l'unanimité.

Sous-alinéas i) et ii)

126. Les sous-alinéas i et ii ont fait l'unanimité sur le fond; des éclaircissements ont cependant été demandés au sujet du caractère contraignant des termes "agréée" et "habilitée". On a répondu que si le terme "agréée" suggérait un système obligatoire de contrôle des autorités de certification, appliqué par les pouvoirs publics, et le terme "habilitée" un système non obligatoire, appliqué sur la base du volontariat, ces systèmes n'étaient pas ceux qui importait le plus dans la création d'une signature numérique sûre. La sécurité devait s'apprécier par référence à des critères qualitatifs objectifs, et non pas par référence au processus de création d'une signature sûre. Ce point de vue n'a pas trouvé d'écho, et il a été décidé de maintenir les sous-alinéas i et ii tels quels.

Sous-alinéa iii)

127. On a émis l'avis que les mots "de toute autre manière" figurant au sous-alinéa iii n'étaient pas suffisamment clairs et risquaient de susciter des difficultés d'application. On a donc proposé à la place de commencer les sous-alinéas i et ii par un membre de phrase tel que : "le certificat a été émis conformément à des normes commercialement appropriées et internationalement reconnues par une autorité de certification agréée par ...".

128. À l'appui du maintien du sous-alinéa iii sous sa forme actuelle, on a fait valoir que celui-ci offrait, avec le sous-alinéa iv, ce qu'on pourrait appeler un moyen "moins direct" d'apporter la preuve qu'une clef publique était rattachée à l'identité d'une personne dans les cas où le certificat n'avait pas été émis conformément aux dispositions des sous-alinéas i ou ii. À l'encontre de la proposition exposée au paragraphe 11 ci-dessus, on a fait valoir qu'elle éliminerait les "raccourcis" qu'offraient les sous-alinéas i et ii pour établir le rattachement de la clef publique à l'identité du signataire, en exigeant la preuve que les normes prescrites avaient été suivies.

S'il ressortait clairement du texte que l'autorité de certification devait avoir été agréée ou habilitée dans des conditions qui offraient des garanties de fiabilité, il n'était pas nécessaire d'exiger que des normes garantissant la fiabilité aient aussi été suivies pour l'émission de certificats par des organes dûment agréés ou habilités.

129. S'agissant de la forme, on a émis la crainte que l'expression "normes commercialement appropriées et internationalement reconnues" pose des problèmes d'interprétation dans certaines langues. On a proposé d'utiliser à la place l'expression "commercialement raisonnables" et de préciser l'origine des normes en ajoutant les mots "issues du marché". On a aussi proposé de remplacer le mot "normes" par les mots "usages et pratiques". À l'encontre de cette proposition, on a fait observer que le terme "usage" avait une signification technique dans un certain nombre de systèmes juridiques qui exigeaient qu'il corresponde à des pratiques largement suivies, et ce de longue date. Il ne convenait donc pas dans le contexte du commerce électronique, puisqu'il s'agissait d'un domaine dans lequel ni les Règles uniformes ni aucun autre usage n'étaient suffisamment établis pour être applicables. Pour résoudre cette difficulté, on a proposé d'inclure à la fois une référence aux "normes techniques internationales" et une référence aux "pratiques et usages commerciaux"

130. En vue de concilier les propositions susmentionnées, on a suggéré que le sous-alinéa iii dispose que le certificat devait avoir été émis "conformément à des normes internationales et à des pratiques ou usages commerciaux notoires et communément suivis par la profession effectuant l'opération". La plupart des membres ont estimé que le libellé suggéré pourrait constituer une base acceptable pour poursuivre la discussion. On s'est toutefois demandé s'il était pleinement compatible avec d'autres références aux usages et pratiques (ou aux normes techniques) que pourraient déjà comporter d'autres instruments internationaux en vigueur dans le domaine du droit commercial international. Après un débat, il a été convenu de placer entre crochets le libellé proposé dans les variantes du projet d'article 9 qui seraient soumises ultérieurement à l'examen du Groupe de travail.

Sous-alinéa iv)

131. À l'appui de la suppression de ce sous-alinéa, on a fait valoir qu'il n'était pas nécessaire de préciser que le certificat rattachait la clef publique à l'identité du signataire si la preuve pouvait en être rapportée, ce qui serait normalement le cas, que le projet d'article 9 comporte ou non une disposition à ce sujet. À l'appui du maintien du sous-alinéa iv, on a fait valoir qu'au cas où il ne serait pas possible d'établir le rattachement de la clef publique en appliquant les sous-alinéas i ou ii, qui n'offraient que des méthodes très limitées et pas toujours disponibles, ou le sous-alinéa iii, qui risquait au début de n'être que rarement applicable dans le domaine du commerce électronique, il fallait indiquer d'autres moyens d'apporter la preuve que la clef publique était bien rattachée à l'identité du signataire. Le sous-alinéa iv avait donc pour objet de compléter les sous-alinéas i, ii et iii et de conférer au projet d'article 9 la souplesse voulue.

Paragraphe 2

132. On a fait valoir, pour justifier le maintien du paragraphe 2, les mêmes arguments que ceux avancés à propos du sous-alinéa iv. On a cependant admis qu'il ne serait peut-être pas nécessaire de maintenir à la fois ce sous-alinéa et le paragraphe 2 puisqu'ils avaient essentiellement la même fonction.

Nouveau texte proposé pour le projet d'article 9

133. Afin de prendre en compte les diverses propositions et suggestions formulées à propos du projet d'article 9, le projet révisé ci-après a été proposé:

"1. *Variante A*

Pour ce qui est de la totalité ou de toute partie d'un message de données, où l'expéditeur est identifié par une signature numérique, ladite signature est une signature électronique [renforcée] [sécurisée] si:

a) elle a été créée de manière sûre pendant la période d'effet d'un certificat valide et vérifiée [correctement] par référence à la clef publique indiquée dans le certificat;

b) le certificat a été émis dans le but de rattacher une clef publique à l'identité [du signataire] [d'une personne];

c) le certificat a été émis pour accompagner les signatures numériques qui sont des signatures électroniques [renforcées] [sécurisées]; et

d) le certificat a été émis:

i) par une autorité de certification agrée 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 ou agréées*]; ou

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

[iii) conformément à des normes commercialement appropriées et internationalement reconnues.]

Variante B

Pour ce qui est de la totalité ou de toute partie d'un message de données, où l'expéditeur est identifié par une signature numérique, ladite signature est une signature électronique [renforcée] [sécurisée] si:

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

b) le certificat rattache une clef publique à l'identité de la personne conformément aux procédures établies par:

i) [*l'État adoptant indique l'organe ou l'autorité ayant pouvoir d'agréer les autorités de certification et de promulguer des règles concernant les fonctions des autorités de certification agréées*]; ou

ii) un organe d'habilitation responsable appliquant des normes commercialement appropriées et internationalement reconnues concernant la fiabilité de la technologie, des pratiques et d'autres caractéristiques pertinentes de l'autorité de certification; ou

iii) [des normes internationales et des pratiques ou usages commerciaux bien connus et habituellement observés dans le commerce concerné].

2. Une signature numérique qui ne satisfait pas aux conditions énoncées au paragraphe 1 est considérée comme une signature électronique [renforcée] [sécurisée] si:

a) il existe des preuves suffisantes montrant que:

i) le certificat rattache avec précision la clef publique à l'identité du sujet du certificat;

ii) la signature numérique a été créée correctement et vérifiée par une procédure sûre et fiable; ou

b) elle satisfait aux critères définissant les signatures électroniques [renforcées] [sécurisées] énoncés dans les autres dispositions des présentes Règles."

134. Pour expliquer cette proposition, il a été déclaré que le terme "correctement" employé à l'alinéa *a* de la variante A signifiait que la signature avait été créée pendant la période d'effet du certificat. L'alinéa *b* n'exigeait pas qu'il soit prouvé que le certificat rattache effectivement la clef publique à l'identité du signataire mais stipulait qu'il devait avoir été émis dans ce but. Le sous-alinéa iii de l'alinéa *d* avait été placé entre crochets pour rendre compte des délibérations concernant la référence aux normes, pratiques et usages faite aux sous-alinéas i et ii.

135. On a émis la crainte que le terme "correctement" employé à l'alinéa *a* du paragraphe 1 ne soit pas suffisamment clair pour indiquer que la vérification devait être effectuée durant la période d'effet du certificat. Le Secrétariat a été prié de compléter le libellé de manière appropriée pour prendre en compte cette préoccupation.

136. Après un débat, le Groupe de travail a convenu que le Secrétariat devait prendre en compte les variantes A et B dans la version révisée des Règles uniformes qu'il devait établir pour les prochaines sessions.

137. Ayant achevé son examen du chapitre II et avant d'entamer l'examen du chapitre III des Règles uniformes, le Groupe de travail a été invité par une délégation à reconsidérer l'objet des Règles uniformes. On a déclaré que ces Règles devraient avoir pour objet de poser des principes fondamentaux de droit afin d'assurer une harmonisation et une convergence sur le plan international. Étant donné qu'un instrument de caractère international, tel que les Règles uniformes, ne pouvait pas, par nature, être sujet à de fréquentes révisions, les Règles ne devraient pas avoir pour objectif de créer des normes et des règles détaillées sur la question des signatures numériques. Une réglementation détaillée ne serait en effet pas suffisamment souple pour pouvoir s'adapter à l'évolution rapide des techniques dans le domaine du commerce électronique. S'il était opportun que la CNUDCI codifie certains usages et certaines pratiques du commerce international, il convenait, en élaborant les Règles uniformes, de ne pas perdre de vue que de tels usages et pratiques n'existaient pas à l'heure actuelle en ce qui concerne les signatures électroniques et qu'il serait illusoire de tenter d'aborder dans les Règles uniformes les multiples questions techniques et commerciales qui seraient susceptibles de surgir dans le contexte des nouvelles pratiques en la matière. Il serait préférable de laisser à des entités telles que l'ISO ou la CCI le soin de s'occuper de telles questions. Le champ d'application des Règles uniformes devrait être recentré pour mettre l'accent sur la définition d'un cadre juridique fondamental dans lequel toutes les signatures électroniques pourraient en principe se développer. À cette fin, les Règles pourraient éviter d'établir des distinctions entre divers types de signatures (par exemple, entre les signatures électroniques ordinaires et les signatures électroniques [renforcées] [sécurisées]), et être restructurées en trois parties comme suit: a) introduction consacrant le principe de l'autonomie des parties; b) ensemble de règles régissant les relations

entre les parties qui communiquent entre elles (fondées sur les dispositions relatives aux présomptions et à la responsabilité qui figurent actuellement dans les Règles uniformes); c) ensemble de dispositions traitant de la responsabilité des prestataires de services qui s'engagent à faciliter l'identification des parties dans un environnement électronique (fondées également sur les dispositions relatives à la responsabilité qui figurent dans les Règles uniformes). Les Règles uniformes ne devraient pas comporter de dispositions relatives aux autorités de certification ou à d'autres prestataires de services d'identification, sauf dans la mesure où cela est nécessaire pour donner des conseils généraux sur la façon dont ces entités devraient s'acquitter de leurs fonctions d'identification. Elles devraient éviter de faire référence au contexte technique (par exemple l'utilisation de techniques de chiffrement, le recours à la cryptographie à clef publique, la dynamique des signatures ou d'autres dispositif biométriques) et devraient plutôt instituer une règle très générale tendant à faire reconnaître la responsabilité des prestataires de services d'identification vis-à-vis des personnes qui se sont fiées à l'identification dans la mesure où cette confiance était raisonnable.

138. L'idée qu'il pourrait être souhaitable de simplifier légèrement les Règles uniformes et que celles-ci devraient continuer de mettre l'accent sur les dispositions relatives à leur application générale dans un contexte techniquement neutre a recueilli un certain appui. Le sentiment général était néanmoins que la structure des Règles uniformes était dans l'ensemble appropriée et qu'il n'était pas nécessaire de la revoir au stade actuel. En particulier, la distinction établie entre divers niveaux de sécurité des signatures électroniques était adéquate. On a fait observer que les Règles, telles qu'elles étaient actuellement rédigées, traduisaient déjà la volonté de régler les questions pratiques complexes liées à l'authentification électronique au moyen de dispositions simples et de portée générale. On a généralement estimé que l'approche sur laquelle les Règles uniformes étaient fondées devait être maintenue.

Chapitre III. Autorités de certification et questions connexes

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

139. Le texte du projet d'article 10, tel que le Groupe de travail l'a examiné, était ainsi conçu:

"1. Lorsqu'elle émet un certificat, l'autorité de certification garantit [à toute personne qui se fie raisonnablement à ce certificat]:

a) qu'elle s'est conformée à toutes les conditions applicables [prévues dans les présentes Règles];

b) que toutes les informations données dans le certificat 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];

c) qu'à sa connaissance, n'a été omis du certificat aucun fait matériel connu qui compromettrait la fiabilité des informations y étant contenues; et

[d) que si elle a publié une déclaration relative aux pratiques d'authentification, elle s'est conformée à cette déclaration pour l'émission du certificat.]

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

a) que la clef publique et la clef privée du [signataire] [sujet] indiquées dans le certificat constituent une paire de clefs opérationnelle, et

b) qu'à la date de l'émission du certificat, la clef privée:

i) est celle du [signataire] [sujet] indiqué dans le certificat; et

ii) correspond à la clef publique donnée dans le certificat.

Paragraphe 1

140. Des opinions diverses ont été exprimées quant à l'utilité et au champ d'application du paragraphe 1 du projet d'article 10. Selon une opinion, le paragraphe 1 (et éventuellement le projet d'article 10 dans sa totalité) devait être supprimé car il était superflu et entrait trop dans le détail. On a déclaré en particulier que la norme relative à la diligence dont l'autorité de certification devait faire preuve pour tous les certificats, figurant au paragraphe 1, était trop complexe et pouvait être simplement considérée comme une obligation imposée à ces autorités d'agir de manière raisonnable et de bonne foi. Ainsi, le paragraphe 1 se bornait à énoncer une évidence et pourrait être soit supprimé soit intégré dans d'autres dispositions des Règles uniformes. On a répondu à cela que, indépendamment de son contenu et de son emplacement, la disposition instituant une norme de conduite était indispensable car elle constituait une étape logique pour assurer l'application des dispositions des Règles uniformes traitant de la responsabilité des autorités de certification. On a fait observer qu'il y aurait peut-être lieu de clarifier les rapports entre le projet d'article 10 et les projets d'articles 11 et 12 afin de bien faire ressortir que, en cas de non-respect des conditions fixées par le projet d'article 10, la responsabilité de l'autorité de certification serait engagée. Il a été suggéré de fusionner les dispositions du projet d'article 10 avec celles du projet d'article 12. Au cours de ce débat, on a également émis l'idée que, outre les dispositions traitant de la responsabilité des autorités de certification, les Règles uniformes devraient peut-être comporter des indications plus détaillées sur les normes que les parties se fiant à la signature devaient respecter en matière de diligence. Une autre suggestion portait sur la possibilité de reformuler les dispositions relatives à la diligence en les présentant sous la forme d'une obligation qui serait faite aux autorités de certification et aux parties se fiant à la signature d'agir de manière raisonnable.

141. Selon un autre point de vue, les éléments spécifiques énumérés au paragraphe 1 étaient nécessaires pour tous les types de certificats. Il fallait donc conserver le paragraphe 1, en supprimant éventuellement les alinéas *b* et *d*, les questions abordées dans ces alinéas pouvant être traitées dans le cadre des dispositions relatives à l'autonomie des parties. Sur le plan de la rédaction, il a été avancé que, si les Règles uniformes fixaient des conditions pour tous les certificats, celles-ci devraient être définies en fonction de la pratique internationale et des usages établis. Il a aussi été suggéré de réviser le membre de phrase "Lorsqu'elle émet un certificat" afin de faire clairement ressortir que la norme de conduite définie dans l'article s'appliquait à la fois à l'"émission" du certificat que l'autorité de certification adresse à son client et à la "communication" des informations relatives au certificat à une partie quelconque qui se fie à la signature par l'autorité de certification. Au cours de ce débat, on a constaté que la question de savoir si le signataire ou le sujet d'un certificat devait être considéré comme une partie se fiant à la signature demeurait irrésolue. S'agissant de l'alinéa *c*, on a émis l'opinion qu'il serait peut-être souhaitable de préciser plus clairement dans cette disposition les faits qui ne doivent pas être omis du certificat. Selon un autre point de vue, la responsabilité de l'entité qui délivre le certificat ne devrait être engagée que dans la mesure où elle garantit la fiabilité des informations afférentes à l'objet du certificat, les autres informations susceptibles de figurer dans le certificat étant exclues. À cet effet, il a été suggéré d'insérer le membre de phrase "pour l'usage auquel il est destiné" à la fin de l'alinéa *c*.

142. Selon une opinion largement partagée, le champ d'application du projet d'article 10 devrait être restreint de manière à couvrir un éventail limité de certificats et, peut-être, uniquement ceux qui ont été émis pour étayer

des signatures électroniques [renforcées] [sécurisées]. On a déclaré qu'il n'était peut-être pas judicieux de fixer une norme de conduite obligatoire pour tous les certificats compte tenu des nombreux types de certificats (et des nombreuses utilisations) qui pourraient surgir, outre ceux qui étaient nécessaires pour les signatures électroniques renforcées, et en dehors du cadre des Règles uniformes. On a suggéré de revoir éventuellement la teneur du paragraphe 2 pour insérer dans l'introduction une référence générale à l'obligation qui incombe à l'autorité de certification d'agir de manière raisonnable.

Paragraphe 2

143. Sur le plan de la rédaction, on a proposé pour l'alinéa *b* i une formule du genre "correspond au [signataire] [sujet] indiqué dans le certificat". Cela permettrait d'éviter que l'autorité de certification se trouve impliqué par inadvertance dans des questions touchant la propriété de la clef.

144. À l'issue d'un débat, le Groupe de travail a décidé de surseoir à sa décision sur le projet d'article 10 en attendant d'avoir achevé l'examen du projet d'article 12. Il a été convenu que, pour la poursuite des travaux lors d'une session future, le Secrétariat devrait établir une version révisée du projet d'article 10 en restreignant son champ d'application comme il a été suggéré plus haut.

Article 11. Responsabilité contractuelle

145. Le texte de l'article 11 examiné par le Groupe de travail était le suivant:

"*Variante A*

1. Entre une autorité de certification émettant un certificat et le détenteur de ce certificat [ou toute autre partie se fiant au certificat, qui a une relation contractuelle avec l'autorité de certification], les droits et obligations des parties [et toute restriction à cet égard] sont déterminés par convention [sous réserve de la loi applicable].

[2. Sous réserve de l'article 10, une autorité de certification peut, par convention, s'exonérer de sa responsabilité en cas de préjudice [dû au fait qu'une personne s'est fiée au certificat] [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 d'un acte ou omission de ladite autorité agissant avec l'intention de causer un préjudice ou témérairement et en sachant qu'un préjudice pourrait en résulter.]

Variante B

Conformément à la loi applicable, les droits et obligations d'une autorité de certification, d'un [signataire] [sujet] indiqué dans un certificat, et de toute autre partie sont régis par la ou les conventions conclues par ces parties dans la mesure où ces conventions traitent de ces droits et obligations et de toute restriction à cet égard.

Variante C

Lorsqu'une autorité de certification, un [signataire] [sujet] identifié dans le certificat, ou toute autre partie, concluent des conventions, les droits et obligations de ces parties, et toute restriction à cet égard, visés dans les conventions sont régis par ces dernières conformément à la loi applicable et dans la mesure permise par elle."

Remarques générales

146. Au début des travaux, des doutes ont été exprimés quant à l'utilité d'un article sur la responsabilité contractuelle dans les Règles uniformes. S'agissant de l'article 11 en particulier, il a été avancé que le paragraphe 1 de la variante A, ainsi que les variantes B et C, faisaient simplement mention de l'application du droit national, laquelle se produirait sans l'inclusion d'une disposition telle que l'article 11 dans les Règles uniformes. Les dispositions dudit article ont été qualifiées de "dispositions provisoires" dont la seule fonction était de rappeler aux lecteurs des Règles uniformes qu'en matière de responsabilité contractuelle, il fallait se référer à la loi applicable; ces dispositions ne visaient ni à établir des règles de fond ni à imposer des obligations en la matière. Il a également été souligné que les paragraphes 2 et 3 de la variante A ne pouvaient être considérés comme des dispositions provisoires et qu'ils établissaient bel et bien des règles de fond sur les questions d'iniquité et de faute intentionnelle. Ces questions étaient néanmoins généralement sujettes à controverse, tant à l'échelle nationale qu'à l'échelle internationale, du fait qu'elles avaient trait à la protection des intérêts du consommateur.

147. Une opinion contraire a été exprimée, selon laquelle l'article 11 introduisait utilement l'article 12. Le projet d'article 12 traitait des règles relatives à la responsabilité autre que la responsabilité contractuelle et ne contenait pas de dispositions relatives à l'autonomie des parties ou d'autres dispositions relatives à la limitation des responsabilités liées au contrat. Afin d'établir clairement que les Règles uniformes ne tendaient pas à exclure la possibilité d'un accord entre les parties sur la limitation des responsabilités découlant du contrat, il a été suggéré qu'une disposition correspondant à celles du projet d'article 11 était nécessaire.

148. De l'avis d'un autre intervenant, étant donné que le rôle de la CNUDCI était d'harmoniser et d'unifier les règles du droit commercial international, il importait de s'entendre sur les principes fondamentaux en matière de responsabilité à intégrer aux Règles uniformes. On a en outre fait valoir que certains systèmes juridiques pourraient ne pas admettre que les parties s'accordent à moduler leurs responsabilités, et que s'en remettre au droit national pour résoudre la question ne servirait donc pas les intérêts du commerce électronique.

149. Les membres du Groupe de travail se sont généralement accordés à reconnaître qu'il conviendrait de conserver dans les Règles uniformes une disposition correspondant à celles du projet d'article 11. Les débats ont porté sur les variantes A, B et C du projet d'article 11. L'emploi des termes "sous réserve de la loi applicable" a été remis en question dans chacune des variantes. De l'avis de l'un des participants, l'emploi de ces termes conduirait à une application extrêmement restreinte des Règles uniformes dans les systèmes qui ne reconnaîtraient pas le droit des parties à décider de moduler leurs responsabilités. D'un autre côté, la suppression des termes "sous réserve de la loi applicable" impliquerait une capacité illimitée à restreindre ou exclure la responsabilité. En conséquence, il a été suggéré que le Groupe de travail étudie soigneusement l'emploi de ces termes dans le projet d'article 11. Il a été proposé de traiter la responsabilité contractuelle – dans la mesure où des dispositions en ce sens s'imposaient – dans le cadre de l'article 12, en insérant une disposition relative à l'autonomie des parties.

Variante A

150. La variante A a recueilli une large adhésion, malgré des réserves d'ordre général qui portaient notamment sur la signification du paragraphe 2.

Paragraphe 1

151. Une question soulevée au sujet du paragraphe 1 avait trait au fait que son champ d'application était limité aux relations spécifiques entre des parties spécifiées à un contrat particulier, au lieu d'englober toutes les parties contractantes. Sous réserve de cette question, la teneur du paragraphe 1 a été jugée généralement satisfaisante et il a été convenu de l'adopter en tant que point de départ de futures discussions.

Paragraphe 2

152. On a fait valoir que, en instituant une règle pour pénaliser un comportement manifestement inéquitable, le paragraphe 2 soulevait une question qui pourrait être difficile à appréhender dans le contexte des systèmes juridiques de certains pays. On a rappelé au Groupe de travail que le paragraphe 2 était inspiré des principes d'UNIDROIT relatifs aux contrats de commerce international (art. 7.1.6), et qu'il tentait d'établir une norme uniforme pour l'évaluation de l'acceptabilité générale des clauses d'exonération. Le fait d'indiquer que la limitation ou l'exclusion de la responsabilité peut être "manifestement inéquitable" dénotait une approche souple en la matière, qui avait pour but de promouvoir une reconnaissance des clauses limitatives et exclusives plus large que cela ne serait le cas si les Règles uniformes mentionnaient uniquement la loi applicable en dehors d'elles (A/CN.9/WG.IV/WP.73, par. 64). L'idée d'inclure la norme en reprenant les termes forgés par UNIDROIT, qui étaient connus et bien compris dans un certain nombre de systèmes juridiques, a recueilli un certain appui, mais on a également formulé des propositions pour améliorer la rédaction et exprimer plus clairement le principe en jeu. Une de ces propositions préconisait de remplacer les termes "manifestement inéquitable" par une formulation qui décrirait ce principe. Selon une autre proposition, le principe devait être interprété dans les Règles uniformes de la même manière que dans les dispositions d'UNIDROIT et il faudrait inclure des explications complémentaires dans un guide d'application. On a demandé au Secrétariat d'envisager de remanier le paragraphe 2 pour tenir compte des propositions qui avaient été faites au sujet de la norme relative aux limitations et aux exclusions "manifestement inéquitables".

153. L'insertion du membre de phrase "Sous réserve de l'article 10" au début du paragraphe 2 de l'article 11 a également suscité des observations. On a fait valoir que, puisque le Groupe de travail n'était pas parvenu à un accord sur le projet d'article 10, la signification de ce membre de phrase était difficile à saisir. Il a été décidé de la placer entre crochets en attendant que l'article 10 soit examiné plus avant.

154. En ce qui concerne les mots placés entre crochets au paragraphe 2, on était généralement partisan de conserver le membre de phrase "dû au fait qu'une personne s'est fiée au certificat" en enlevant les crochets, et de supprimer le membre de phrase "dû à des erreurs dans les informations contenues dans le certificat, à des défaillances techniques ou à d'autres circonstances de même nature". En outre, les participants ont généralement considéré qu'il faudrait garder la dernière phrase du paragraphe 2 en la modifiant comme suit: "Toutefois, la clause limitant ou excluant la responsabilité de l'autorité de certification ne peut être invoquée dans la mesure où l'exclusion ou la limitation de la responsabilité contractuelle serait manifestement inéquitable eu égard à l'objet du contrat et à d'autres circonstances pertinentes". Pour justifier l'insertion du membre de phrase "et à d'autres circonstances pertinentes", les auteurs de la proposition ont fait valoir que, pour déterminer si une limitation ou une exclusion était manifestement inéquitable, il faudrait toujours se référer à toutes les circonstances propres à chaque cas particulier et pas simplement au contrat qui contenait une telle limitation ou une telle exclusion.

155. Le Groupe de travail a décidé de conserver les paragraphes 1 et 2 de la variante A, sous réserve d'une révision pour tenir compte des modifications proposées plus haut.

Paragraphe 3

156. Il a été proposé de supprimer le paragraphe 3 compte tenu du fait que le traitement de la responsabilité, lorsqu'il y a intention de causer un préjudice ou un comportement téméraire ou délibéré, serait régi par le paragraphe 2. Cette proposition a été généralement acceptée.

Variantes B et C

157. Un appui a été exprimé en faveur du maintien de la variante C, en tant que texte susceptible de remplacer la variante A. On a déclaré que, puisque la variante C se bornait à faire référence à la loi applicable, il n'y aurait aucun risque d'incompatibilité avec des règles applicables relatives à la responsabilité contractuelle, quelles qu'elles soient. À l'issue du débat, on avait généralement le sentiment que, pour les raisons indiquées plus haut, la variante A était préférable. La variante B n'a pas été défendue. Le Groupe de travail a finalement décidé de supprimer les variantes B et C.

Article 12. Responsabilité de l'autorité de certification envers les parties se fiant au certificat

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

"1. Sous réserve des dispositions du paragraphe 2, lorsqu'une autorité de certification émet un certificat, elle est responsable envers toute personne se fiant raisonnablement à ce certificat:

a) des erreurs y figurant, sauf si elle prouve qu'elle ou ses agents ont pris [toutes] les mesures [raisonnables] [commercialement raisonnables] [qui étaient appropriées compte tenu de l'objet pour lequel le certificat avait été émis, au vu de toutes les circonstances] pour éviter des erreurs dans le certificat;

b) du non-enregistrement de l'annulation du certificat, sauf si elle prouve qu'elle ou ses agents ont pris [toutes] les mesures [raisonnables] [commercialement raisonnables] [qui étaient appropriées compte tenu de l'objet pour lequel le certificat avait été émis, au vu de toutes les circonstances] pour enregistrer l'annulation promptement après réception de l'avis d'annulation]; et

c) des conséquences imputables au non-respect:

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

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) [...].]"

Remarques générales

159. Si l'on a jugé que, dans l'ensemble, le projet d'article 12 était acceptable quant au fond, certaines délégations ont estimé qu'il serait préférable de ne pas inclure de règle précise sur la responsabilité d'une autorité de certification envers les parties se fiant au certificat. Le Groupe de travail a convenu qu'il faudrait examiner conjointement les projets d'articles 10, 11 et 12, lors d'une séance future, pour veiller à ce que les obligations imposées aux autorités de certification correspondent aux règles de responsabilité énoncées dans les Règles uniformes et à ce que les questions liées à l'autonomie des parties soient correctement réglées. Il a également été observé qu'il convenait de maintenir une certaine cohérence entre les trois projets d'articles, notamment en ce qui concernait la question de savoir si les dispositions devaient être axées sur l'exactitude du résultat visé ou la procédure à suivre.

Paragraphe 1

Alinéa a)

160. Plusieurs suggestions concernant le libellé ont été formulées. Il a été décidé de conserver les mots "toutes" et "raisonnables" sans les crochets et de supprimer le reste du texte figurant entre crochets. S'agissant de l'alinéa *a*, il a été proposé de mentionner, outre les erreurs, les "omissions" apparaissant dans le certificat et de supprimer la partie du texte stipulant que l'autorité de certification devait prouver qu'elle avait pris des mesures raisonnables pour éviter des erreurs. On a proposé le texte suivant : "*a* des erreurs ou omissions apparaissant dans le certificat et dues au fait que l'autorité de certification n'a pas pris toutes les mesures raisonnables pour éviter des erreurs ou des omissions dans le certificat". Il a également été proposé de renverser l'ordre de la phrase afin de mettre l'accent sur le fait que l'autorité de certification n'avait pas exercé un soin raisonnable et d'introduire l'idée de permettre à l'autorité de certification de prendre des mesures pour corriger les erreurs ou les inexactitudes apparaissant dans le certificat. On a proposé le texte suivant : "a) de n'avoir pas pris toutes les mesures raisonnables pour éviter ou corriger les erreurs ou les inexactitudes apparaissant dans le certificat". Les auteurs de cette proposition craignaient que la référence à des omissions n'ait de sens que dans le contexte d'une obligation d'inclure des informations spécifiques dans le certificat, dont le non-respect donnerait naissance à une responsabilité. Cette notion serait pertinente dans le contexte des projets d'articles 8 et 10, sur lesquels il faudrait s'aligner. On a également émis la crainte que la proposition tendant à renverser l'ordre de l'alinéa *a* et à supprimer les mots ayant trait à l'obligation de l'autorité de certification de prouver qu'elle avait pris toutes les mesures raisonnables déplace la charge de la preuve à l'intérieur de l'alinéa. Il était acceptable de mentionner les omissions mais, de l'avis général, il ne fallait pas déplacer la charge de la preuve de cette manière.

Alinéa b)

161. Il a été observé que l'alinéa *b* était trop détaillé et qu'il convenait de le supprimer. Néanmoins, on a généralement estimé qu'il ne serait acceptable de supprimer l'alinéa *b* que si les dispositions qu'il contenait étaient incluses dans une version révisée et enrichie de l'alinéa *a*. Dans l'attente des délibérations sur l'harmonisation des projets d'articles 8, 10 et 12, l'alinéa *b* devait être conservé dans les Règles uniformes. En ce qui concernait le libellé, il a été décidé de conserver les mots "toutes" et "raisonnables" sans crochets et de supprimer le reste du texte figurant entre crochets.

Alinéa c)

162. S'agissant de la disposition énoncée au sous-alinéa ii de l'alinéa *c*, on a émis la crainte qu'il soit difficile, pour une autorité de certification, de savoir quelle était la loi applicable dans un cas donné. La référence à "toute procédure" énoncée dans une déclaration relative aux pratiques d'authentification ou dans la loi

applicable risquait d'avoir une portée trop vaste car toutes les procédures en question ne visaient pas à protéger les parties se fiant au certificat et il valait mieux que le projet d'article 12 s'en tienne à la responsabilité des autorités de certification à l'égard des parties en question. On a généralement estimé que le sous-alinéa ii devait être supprimé. On a décidé de conserver le sous-alinéa i, qui évoquait la responsabilité de l'autorité de certification pour le non-respect de sa propre déclaration relative aux pratiques d'authentification.

Paragraphe 2

163. Des suggestions ont été formulées pour clarifier le libellé du paragraphe 2. On a proposé notamment de modifier l'alinéa *a* pour qu'il se lise comme suit : "L'objet de cette démarche est contraire à l'objet pour lequel le certificat a été émis." De même, l'alinéa *b* devrait être modifié pour se lire comme suit: "Il s'agit d'une transaction dont la valeur dépasse la valeur pour laquelle le certificat est valide." On a également suggéré que le texte précise clairement qu'il n'était pas raisonnable de se fier à un certificat en vertu du paragraphe 2 "dans la mesure" où cela n'était fondé ni sur l'objet pour lequel le certificat avait été émis ni sur la valeur pour laquelle le certificat était valide. On a généralement estimé qu'il faudrait réviser le libellé du paragraphe 2 pour prendre en compte ces suggestions.

Articles 13 à 15

164. Faute de temps, le Groupe de travail n'a pu procéder qu'à un examen préliminaire des projets d'articles 13, 14 et 15. Le texte dont le Groupe de travail était saisi était le suivant:

Article 13. Annulation d'un certificat

"1. Pendant la période d'effet d'un certificat, l'autorité de certification qui l'a émis doit l'annuler conformément aux politiques et procédures régissant l'annulation énoncées dans la déclaration applicable relative aux pratiques d'authentification ou, en l'absence de telles politiques et procédures, promptement après:

a) réception d'une demande d'annulation par le [signataire] [sujet] indiqué dans le certificat, et confirmation que la personne demandant l'annulation en est le [signataire] [sujet] [légitime], ou est un agent du [signataire] [sujet] habilité à demander l'annulation;

b) réception d'une preuve fiable du décès du [signataire] [sujet] si ce dernier est une personne physique; ou

c) réception d'une preuve fiable que le [signataire] [sujet] a été dissous ou a cessé d'exister, lorsqu'il s'agit d'une personne morale.

2. Le [signataire] [sujet] titulaire d'une paire de clefs certifiée est tenu d'annuler le certificat correspondant ou d'en demander l'annulation lorsqu'il sait que la clef privée a été perdue, compromise ou risque d'être utilisée à mauvais escient à d'autres égards. Si le [signataire] [sujet] n'annule pas le certificat dans un tel cas, il est responsable de tout préjudice encouru par une personne s'étant fiée à un message du fait qu'il a failli à son obligation d'annuler le certificat.

3. Que le [signataire] [sujet] indiqué dans le certificat consente ou non à l'annulation, l'autorité de certification qui a émis le certificat doit l'annuler rapidement après avoir appris:

a) qu'un fait matériel présenté dans le certificat est faux;

b) que la clef privée ou le système informatique de l'autorité de certification a été compromis d'une manière qui compromet la fiabilité du certificat; ou

c) que la clef privée ou le système informatique du [signataire] [sujet] a été compromis.

4. Lors de l'annulation d'un certificat en vertu du paragraphe 3, l'autorité de certification doit aviser le [signataire] [sujet] et les parties se fiant au certificat conformément aux politiques et aux procédures qui régissent la notification des annulations énoncées dans la déclaration applicable relative aux pratiques d'authentification ou, en l'absence de telles politiques et procédures, il doit aviser rapidement le [signataire] [sujet] et publier dans les meilleurs délais un avis d'annulation si le certificat a été publié, et en informer par ailleurs, sur demande, toute partie s'étant fiée au certificat.

5. [Entre le [signataire] [sujet] et l'autorité de certification,] l'annulation prend effet à partir du moment où elle est [reçue] [enregistrée] par l'autorité de certification.

[6. Entre l'autorité de certification et toute autre partie se fiant au certificat, l'annulation prend effet à partir du moment où elle est [enregistrée] [publiée] par l'autorité de certification.]"

Article 14. Suspension d'un certificat

"Pendant la période d'effet d'un certificat, l'autorité de certification l'ayant émis doit le suspendre conformément aux politiques et procédures régissant la suspension énoncées dans la déclaration applicable relative aux pratiques d'authentification ou, en l'absence de telles politiques et procédures, dans les meilleurs délais après réception d'une demande à cet effet émanant d'une personne dont l'autorité de certification peut raisonnablement penser qu'elle est le [signataire] [sujet] désigné dans le certificat ou une personne autorisée à agir en son nom."

Article 15. Registre des certificats

"1. L'autorité de certification tient un registre électronique des certificats émis accessible au public et indiquant la date d'expiration de chaque certificat, ou la date de suspension ou d'annulation.

2. Le registre est tenu par l'autorité de certification

Variante A pendant au moins [30] [10] [5] ans

Variante B pendant ... [*l'État adoptant spécifie la période pendant laquelle les renseignements pertinents doivent être conservés dans le registre*]

à compter de la date d'annulation ou d'expiration de la période d'effet de tout certificat émis par l'autorité de certification.

Variante C conformément aux politiques et procédures spécifiées par l'autorité de certification dans la déclaration applicable relative aux pratiques d'authentification."

Remarques générales

165. On a exprimé des doutes quant à la nécessité d'inclure les projets d'articles 13 à 15 dans les Règles uniformes. On a proposé de les supprimer au motif qu'ils étaient trop précis, trop détaillés et d'application trop

limitée, qu'ils reposaient sur des hypothèses générales quant à la manière dont certains modèles pourraient ou non fonctionner en pratique, et qu'il était peu probable qu'ils soient largement adoptés. Toutefois, il a été généralement admis au sein du Groupe de travail qu'il serait prématuré de supprimer ces projets d'articles sans les examiner plus avant.

166. Un certain nombre de délégations ont estimé que les projets d'articles 13 et 14 traitaient de questions qu'il était important d'envisager dans les Règles uniformes, en fonction de la manière dont un certain nombre de questions laissées en suspens par le Groupe de travail à sa session actuelle pourraient finalement être réglées dans le cadre des Règles uniformes. On a estimé d'une manière générale que ces projets d'articles devaient être simplifiés, éventuellement ramenés à un seul article ou incorporés à d'autres articles de la section III du chapitre II. On a proposé, comme il était clair qu'il fallait des autorités de certification pour les signatures numériques, que ces trois articles soient limités dans leur application aux signatures numériques et les Règles uniformes réorganisées pour refléter cette limitation. Selon une proposition connexe, il était important d'examiner comment les pratiques commerciales concernant les signatures autres que des signatures numériques se développaient pour déterminer comment structurer les Règles uniformes.

167. Quant au fond, on a estimé que les projets d'articles 13 et 14 concernaient les principales obligations des autorités de certification et qu'il était nécessaire de déterminer quelles devaient être ces obligations avant de pouvoir régler les questions de responsabilité. S'agissant de l'article 13, on a dit qu'il offrait la possibilité de réaliser un équilibre dans les Règles uniformes entre les obligations imposées à l'autorité de certification et celles qui étaient à la charge du signataire ou sujet du certificat.

168. Selon une opinion, le projet d'article 15 soulevait des questions difficiles de confidentialité des données et pouvait être supprimé. Il risquait en outre de ne pas être applicable dans certains systèmes de certification. À l'appui de son maintien, on a fait observer qu'il avait trait à la responsabilité de l'autorité de certification en vertu du projet d'article 12 et qu'il devrait être réexaminé lorsqu'on examinerait ce projet d'article 12.

169. Le Groupe de travail a décidé de conserver les articles 13, 14 et 15 entre crochets pour examen futur. Le Secrétariat a été prié d'en revoir le libellé pour rendre compte des opinions exprimées et voir s'il était possible de simplifier ces articles.

Article 16. Relations entre les parties se fiant aux certificats et l'autorité de certification

170. Le texte du projet d'article 16 examiné par le Groupe de travail était le suivant:

"[1. Une autorité de certification n'est autorisée à demander que les renseignements qui lui sont nécessaires pour identifier l'utilisateur.

2. Sur demande, l'autorité de certification divulgue les renseignements suivants:

a) les conditions dans lesquelles le certificat peut être utilisé;

b) les conditions déterminant l'utilisation des signatures numériques;

c) le coût des services fournis par l'autorité de certification;

d) la politique ou les pratiques de l'autorité de certification concernant l'utilisation, la conservation et la communication de renseignements d'ordre personnel;

e) les prescriptions techniques de l'autorité de certification concernant le matériel de communication devant être utilisé par les parties se fiant aux certificats;

f) les conditions dans lesquelles l'autorité de certification met en garde les parties se fiant aux certificats en cas d'irrégularité ou de défaut de fonctionnement du matériel de communication;

g) toute limite de la responsabilité de l'autorité de certification;

h) toutes restrictions imposées par l'autorité de certification à l'utilisation du certificat;

i) les conditions dans lesquelles le [signataire] [sujet] est autorisé à restreindre l'utilisation du certificat.

3. Les renseignements énumérés au paragraphe 1 sont communiqués au [signataire] [sujet] potentiel avant la conclusion définitive d'un accord de certification. Ces renseignements peuvent être communiqués par l'autorité de certification dans le cadre d'une déclaration relative aux pratiques d'authentification.

4. Avec préavis [d'un mois], le [signataire] [sujet] peut mettre fin à l'accord établissant une connexion avec l'autorité de certification. L'avis prend effet dès qu'il est reçu par l'autorité de certification.

5. Avec préavis [de trois mois], l'autorité de certification peut mettre fin à l'accord établissant une connexion avec elle. L'avis prend effet dès qu'il est reçu.]"

171. De l'avis général, l'article 16 devait être supprimé parce qu'il envisageait des questions précontractuelles qu'il fallait laisser aux parties au contrat de certification le soin de régler entre elles. S'il pouvait être utile d'envisager certaines des questions qui y étaient traitées pour exposer la meilleure pratique à l'intention des autorités de certification, un tel exposé n'avait pas sa place dans les Règles uniformes, mais pourrait figurer dans un guide explicatif.

172. Une préoccupation a été exprimée au sujet de la question des déclarations relatives aux pratiques d'authentification visées au paragraphe 3. On a dit que ces déclarations constituaient un élément important de la relation entre autorités de certification, signataires et parties se fiant aux signatures, et que toutes les autorités de certification devraient être tenues de délivrer une déclaration relative aux pratiques d'authentification. Le Groupe de travail a décidé qu'il reviendrait sur cette question à une session ultérieure lorsqu'il examinerait les projets d'articles 10, 11 et 12.

Chapitre IV. Signatures électroniques étrangères

Articles 17 à 19

173. Faute de temps, le Groupe de travail a renvoyé l'examen des projets d'articles 17 à 19 à une session ultérieure.

III. Travaux futurs proposés dans le domaine du commerce électronique

174. Au cours de la session du Groupe de travail, des consultations officieuses se sont tenues au sujet du projet de convention internationale sur les transactions électroniques (voir document A/CN.9/WG.IV/WP.77)[4]. Une délégation a décrit l'objet de la proposition et a expliqué que celle-ci avait un double objectif: a) éliminer les obstacles aux transactions électroniques liés à l'utilisation du support papier en adoptant des dispositions de la Loi type, et b) traiter certaines questions touchant à l'authentification électronique (dans la mesure où ces questions ne font pas déjà l'objet des travaux en cours sur le projet de Règles uniformes) d'une manière qui, tout en tenant compte des différentes approches que les pays pourraient adopter dans leur droit interne, garantirait néanmoins une reconnaissance et une application larges des clauses contractuelles privées portant sur l'authentification des signatures électroniques. Il a été noté que le texte de la proposition avait été préparé pour la discussion et n'employait pas la terminologie propre aux conventions.

175. En ce qui concerne les obstacles liés à l'utilisation du support papier, la proposition portait sur les principales questions relatives aux transactions électroniques. La convention proposée inclurait des éléments fondamentaux de la Loi type, par exemple la disposition selon laquelle la validité ou la force exécutoire d'un contrat formé par des moyens électroniques ne devait pas être contestée au seul motif que ledit contrat avait été formé électroniquement. Cette partie de la convention définirait également les caractéristiques d'un écrit électronique valide et d'un document original et favoriserait l'admission des preuves informatiques. On y reconnaîtrait en outre l'acceptabilité des signatures électroniques à des fins juridiques et commerciales. Les partisans de la convention ont estimé que ces dispositions faisaient l'objet d'un assez large consensus international, bien qu'il ait été indiqué que, dans les consultations informelles, plusieurs délégations avaient fait savoir qu'elles souhaitaient conserver une marge de manœuvre lors de l'application de ces dispositions dans leurs droits nationaux.

176. Une délégation a fait rapport oralement au Groupe de travail sur diverses autres questions examinées informellement par plusieurs délégations. Il a été indiqué que, selon une opinion, formulée de manière informelle, l'éventuelle élaboration d'une convention ne devrait pas impliquer la reprise des travaux sur le contenu de la Loi type. La proposition relative à l'élaboration d'une convention devait plutôt être considérée comme une suggestion visant à promouvoir la Loi type. Il a aussi été indiqué que la question de savoir dans quelle mesure les dispositions de la Loi type devraient être intégrées à la convention proposée avait été débattue. On a aussi fait savoir que, selon une opinion, le texte intégral de la Loi type devrait figurer en annexe à la convention. Selon un autre avis, certaines dispositions de la Loi type étaient peut-être moins pertinentes que d'autres. Une autre idée signalée était la possibilité de moduler le libellé du projet de convention afin que les États parties puissent entreprendre de mettre en œuvre les principes énoncés dans les dispositions pertinentes de la Loi type.

177. S'agissant de la section de la convention consacrée à l'authentification électronique, on a indiqué que plusieurs questions avaient été examinées de manière informelle. Une délégation avait souligné que, dans le contexte de l'authentification électronique, la convention proposée devrait préserver la liberté des pays d'adopter différentes approches, en fonction de leur droit national. La convention devrait également établir clairement que, nonobstant la nature exacte de tout cadre réglementaire régissant l'authentification électronique, les termes d'un accord (y compris les accords en système fermé) conclu entre les parties devraient être respectés dans toute la mesure du possible. On a indiqué que, selon une opinion, la nécessité de concilier une large reconnaissance de l'autonomie des parties, d'une part, et la volonté des États de préserver leur cadre législatif et réglementaire national, d'autre part, risquait d'être l'une des principales difficultés à résoudre.

178. D'autres questions avaient été débattues informellement qui touchaient aux autres dispositions relatives à l'authentification. Outre la neutralité quant à la technologie et quant à l'application, la convention proposée

stipulait que les parties devraient être autorisées à tenter de prouver l'authenticité de leurs transactions, que la technique d'authentification ou la méthode commerciale à laquelle elles recourent soit ou non expressément visée dans la législation ou la réglementation. Enfin, la convention proposée engageait les États à adopter une approche non discriminatoire des mécanismes d'authentification mis en oeuvre dans les autres pays. Cette disposition a été examinée en tant que principe du droit commercial et à la lumière des principes du commerce international.

179. Il a été convenu que le débat informel sur la convention proposée pourrait se poursuivre avant et pendant la session suivante du Groupe de travail.

* * *

Notes

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

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

[3]Ibid., *cinquante-troisième session, Supplément n° 17* (A/53/17), par. 209 à 211.

[4]En ce qui concerne l'examen préliminaire de cette proposition par la Commission, voir *Documents officiels de l'Assemblée générale, cinquante-troisième session, Supplément n° 17* (A/53/17), par. 209 à 211.