NATIONS UNIES **A**

Assemblée générale

Distr. GÉNÉRALE
A/CN.9/457
25 février 1999

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-QUATRIÈME SESSION
(Vienne, 8-19 février 1999)

TABLE DES MATIÈRES

V.99-81357

INTRODUCTION

1. À sa vingt-neuvième session (1996), la Commission a décidé d'inscrire à son ordre du jour les questions relatives aux signatures numériques et aux autorités de certification. Le Groupe de travail sur le commerce électronique a été prié de réfléchir à l'opportunité de définir des règles uniformes concernant ces questions. Il a été convenu que les règles uniformes devant être élaborées devraient être consacrées notamment aux questions ci-après: fondement juridique des opérations de certification, y compris les nouvelles techniques d'authentification et de certification numériques; applicabilité de la certification; répartition des risques et des responsabilités entre utilisateurs, fournisseurs et tiers dans le contexte de l'utilisation de techniques de certification; questions spécifiques à la certification sous l'angle de l'utilisation des registres; et incorporation par référence[1].

2. À sa trentième session (1997), la Commission était saisie du rapport du Groupe de travail sur les travaux de sa trente et unième session (A/CN.9/437). Le Groupe de travail a indiqué à la Commission qu'il était parvenu à un consensus quant à l'importance et à la nécessité de travailler à l'harmonisation du droit dans ce domaine. Bien que n'ayant pas pris de décision ferme sur la forme et la teneur de ces travaux, il était arrivé à la conclusion préliminaire qu'il était possible d'entreprendre l'élaboration d'un projet de règles uniformes, du moins sur les questions concernant les signatures numériques et les autorités de certification et peut-être sur des questions connexes. Le Groupe de travail a rappelé que dans le cadre des travaux futurs dans le domaine du commerce électronique, il pourrait être nécessaire de traiter, outre les questions relatives aux signatures numériques et aux autorités de certification, les sujets suivants : techniques autres que la cryptographie à clef publique; questions générales concernant les fonctions exercées par les tiers fournisseurs de services et contrats électroniques (A/CN.9/437, par. 156 et 157).

3. La Commission a approuvé les conclusions du Groupe de travail et lui a confié l'élaboration de règles uniformes sur les questions juridiques relatives aux signatures numériques et aux autorités de certification (dénommées ci-après "les Règles uniformes").

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 que les Règles uniformes devraient être compatibles avec l'approche techniquement neutre adoptée dans la Loi type de la CNUDCI sur le commerce électronique (dénommée ci-après "la Loi type"). Ainsi, les Règles uniformes ne devraient pas décourager l'utilisation d'autres techniques d'authentification. En outre, s'agissant de la cryptographie à clef publique, il pourrait être nécessaire que les Règles uniformes prennent en considération divers niveaux de sécurité et reconnaissent les divers effets juridiques et niveaux de responsabilité correspondant aux différents types de services fournis dans le contexte des signatures numériques. S'agissant des autorités de certification, la Commission a certes reconnu la valeur des normes issues du marché, mais il a été généralement considéré que le Groupe de travail pourrait utilement envisager l'établissement d'un ensemble minimum de normes que les autorités de certification devraient strictement respecter, en particulier dans les cas de certification transnationale[2].

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

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). Elle 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. Toutefois, la Commission a estimé, dans l'ensemble, que les progrès accomplis jusqu'ici montraient que le projet de Règles uniformes sur les signatures électroniques prenait progressivement la forme d'une structure utilisable.

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 et exprimé sa conviction que le Groupe de travail pourrait accomplir de nouveaux progrès à sa trente-troisième session (New York, 29 juin-10 juillet 1998) sur la base du projet révisé établi par le secrétariat (A/CN.9/WG.IV/WP.76). La Commission a également noté avec satisfaction que l'on reconnaissait généralement désormais que le Groupe de travail était une instance internationale particulièrement importante pour échanger des vues sur les problèmes juridiques que posait le commerce électronique et pour chercher des solutions à ces problèmes[3].

8. Le Groupe de travail a poursuivi la révision des Règles uniformes à sa trente-troisième session (juillet 1998) sur la base d'une note établie par le secrétariat (A/CN.9/WG.IV/WP.76). Le rapport sur les travaux de cette session est publié sous la cote A/CN.9/454.

9. Le Groupe de travail sur le commerce électronique, qui est composé de tous les États membres de la Commission, a tenu sa trente-quatrième session à Vienne du 8 au 19 février 1999. Ont assisté à cette session les représentants des États membres du Groupe de travail ci-après: Allemagne, Argentine, Australie, Autriche, Brésil, Burkina Faso, Cameroun, Chine, Colombie, Égypte, Espagne, États-Unis d'Amérique, Fédération de Russie, Finlande, France, Honduras, Hongrie, Inde, Iran (République islamique d'), Italie, Japon, Mexique, Nigéria, Paraguay, Roumanie, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, Singapour et Thaïlande.

10. Y ont également assisté des observateurs des États ci-après: Afrique du Sud, Angola, Arabie saoudite, Bélarus, Belgique, Bolivie, Canada, Croatie, Cuba, Géorgie, Guatemala, Indonésie, Irlande, Koweït, Liban, Maroc, Nouvelle-Zélande, Pays-Bas, Pologne, Portugal, République tchèque, République de Corée, Slovaquie, Suède, Suisse, Turquie et Uruguay.

11. Y ont en outre assisté les organisations internationales ci-après: Conférence des Nations Unies sur le commerce et le développement (CNUCED), Commission économique pour l'Europe de l'Organisation des Nations Unies (CEE/ONU), Organisation des Nations Unies pour l'éducation, la science et la culture (UNESCO), Organisation des Nations Unies pour le développement industriel (ONUDI), Banque africaine de développement, Commission européenne, Organisation de coopération et de développement économiques (OCDE), Union asiatique de compensation, Association européenne des étudiants en droit, Association internationale des ports (AIP), Association internationale du barreau, Chambre de commerce internationale (CCI), International Telecommunications User Group (INTUG),Internet Law and Policy Forum (ILPF), Society for Worldwide Interbank Financial Telecommunications (S.W.I.F.T.) et Union internationale des avocats (UIA).

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

Président: M. Jacques GAUTHIER (Canada, élu à titre personnel);

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

Rapporteur: M. Louis-Paul ENOUGA (Cameroun).

13. Le Groupe de travail était saisi des documents ci-après: ordre du jour provisoire (A/CN.9/WG.IV/WP.78); deux notes du secrétariat contenant un projet révisé de règles uniformes sur les signatures électroniques (A/CN.9/WG.IV/WP.79 et 80); et la note du secrétariat établie pour la trente-troisième session du Groupe de travail

(A/CN.9/WG.IV/WP.76), afin de permettre la poursuite du débat sur les questions relatives à la reconnaissance des signatures électroniques étrangères (projet d'articles 17 à 19).

14. 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

15. Le Groupe de travail a examiné la question des signatures numériques sur la base des notes établies par le secrétariat (A/CN.9/WG.IV/WP.76, 79 et 80). 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.

II. PROJET DE RÈGLES UNIFORMES SUR LES SIGNATURES ÉLECTRONIQUES

A. REMARQUES GÉNÉRALES

16. Les membres du Groupe de travail ont tout d'abord échangé des vues sur les faits nouveaux en matière de réglementation découlant du commerce électronique, y compris l'adoption de la Loi type de la CNUDCI sur le commerce électronique, sur les signatures électroniques et sur les questions relatives à l'infrastructure à clef publique dans le contexte des signatures numériques. Les rapports établis aux niveaux gouvernemental, intergouvernemental et non gouvernemental confirmaient que l'on reconnaissait de plus en plus la nécessité de traiter les aspects juridiques du commerce électronique pour faciliter ce type de commerce et éliminer les obstacles aux échanges. Il a été signalé que plusieurs pays avaient récemment adopté, ou étaient sur le point d'adopter, une législation incorporant la Loi type ou traitant de questions connexes relatives à la facilitation du commerce électronique. Un certain nombre des propositions législatives portaient également sur les questions des signatures électroniques (ou, dans certains cas, plus particulièrement sur les signatures numériques). D'autres pays avaient créé, parfois en étroite collaboration avec le secteur privé, des groupes de travail qui étudiaient les changements à apporter à la législation pour faciliter le commerce électronique, envisageaient activement d'adopter la Loi type, préparaient les textes législatifs nécessaires, et travaillaient sur les questions relatives aux signatures électroniques, y compris la mise en place d'infrastructures à clef publique ou d'autres projets sur des questions étroitement liées à ce sujet.

17. Le Groupe de travail a entamé l'examen des Règles uniformes en rappelant qu'il était à la fois souhaitable et possible d'établir des règles sur les signatures électroniques et qu'il était nécessaire de s'employer à harmoniser la législation dans ce domaine (voir ci-dessus par. 7). On a fait remarquer qu'un certain nombre de références avaient été faites aux travaux entrepris sur les signatures numériques, et la diversité des lois promulguées sur cette technique particulière de signature montrait bien l'importance d'une harmonisation. On a également fait observer que si la Loi type était fondée sur une approche techniquement neutre, l'adoption d'une telle approche dans le projet de Règles

uniformes, qui visaient diverses techniques de signature, était source de tension. Les membres du Groupe de travail s'accordaient sur la nécessité d'assurer une cohérence entre la Loi type et les Règles uniformes, en reconnaissant cependant qu'il fallait, pour rédiger des dispositions attribuant des effets juridiques spécifiques à ces différents types de techniques de signature, parvenir à un équilibre qui pouvait être difficile à trouver. Les Règles uniformes devraient, a-t-on déclaré, mettre l'accent sur plusieurs points: les utilisations des signatures, ce qui pourrait impliquer l'examen des questions de l'équivalence fonctionnelle pour une signature "renforcée" ou à sécurité maximale; les conséquences, pour les parties concernées, de l'utilisation de diverses techniques de signature, y compris la conduite de ces parties (plutôt que d'essayer d'établir un lien entre un effet juridique particulier et l'utilisation de telle ou telle technique de signature électronique); et les questions de reconnaissance internationale.

18. Selon un avis, il était nécessaire de mieux préciser la relation entre l'article 7 de la Loi type et le projet de Règles uniformes. On s'est demandé s'il était vraiment nécessaire et souhaitable de partir de l'article 7 et on a fait observer qu'il pourrait être difficile de trouver un seul raccourci pour satisfaire à l'exigence très souple énoncée au paragraphe 1-b) de cet article, selon laquelle la fiabilité de la méthode d'identification utilisée devrait être "suffisante au regard de l'objet...". Il a été déclaré que la diversité des facteurs énumérés dans le Guide (voir par. 58 du Guide pour l'incorporation de la Loi type de la CNUDCI sur le commerce électronique) était utile pour tout examen de l'objet pour lequel la méthode était utilisée. On a rappelé que le Groupe de travail avait examiné cette question à plusieurs reprises lors de ses précédentes délibérations et que la version actuelle du projet de Règles uniformes n'y apportait pas de réponse. On a aussi exprimé la crainte qu'en examinant une règle sur les types de techniques de signature qui pourraient satisfaire à l'exigence énoncée à l'article 7 on n'aboutisse à un texte dont le champ d'application serait jugé très limité par rapport aux transactions commerciales (qui ne devaient normalement satisfaire à aucune règle de droit particulière quant à la forme).

19. La question de la forme à donner au projet de Règles uniformes a été soulevée et on a noté à cet égard qu'il était important d'examiner la relation entre la forme et le contenu. S'agissant de la forme, différentes approches ont été proposées, à savoir l'adoption de règles contractuelles, de dispositions législatives ou de principes directeurs à l'intention des États envisageant d'adopter une législation sur les signatures électroniques. On a également soulevé, à ce propos, la question de la relation entre les Règles uniformes, en tant que dispositions législatives, et la Loi type. On a reconnu que l'examen, par le Groupe de travail, de l'utilisation de diverses techniques de signature, avait beaucoup contribué à faire progresser l'intelligence des questions pertinentes et que les documents du Groupe donnaient une bonne vue d'ensemble des notions de base. En attendant une décision finale quant à la relation entre les Règles uniformes et la Loi type, les membres du Groupe de travail ont généralement déclaré préférer que les Règles uniformes soient considérées comme un instrument séparé.

20. S'agissant du champ d'application de ces Règles, il a été généralement estimé que les questions relatives aux consommateurs ne devraient pas y être expressément traitées. Néanmoins, étant donné qu'elles pourraient, dans certains cas, être utiles aux consommateurs, il a été proposé d'adopter la formulation figurant dans la note ** relative à l'article premier de la Loi type. On a également estimé qu'en tout état de cause les transactions mettant en jeu des consommateurs, qui seraient visées par les Règles uniformes, devraient être limitées aux transactions commerciales comme indiqué dans la note *** relative à l'article premier de la Loi type (pour la poursuite du débat, voir ci-dessous, par. 56 et 70).

21. Le Groupe de travail a été d'avis que le texte du projet de Règles uniformes publié sous la cote A/CN.9/WG.IV/WP.80 (dénommé ci-après le document WP.80) constituait une base de discussion plus acceptable que celui qui figurait dans le document A/CN.9/WG.IV/WP.79 (dénommé ci-après le document WP.79). On a fait remarquer que le Groupe de travail pourrait utilement examiner le document WP.79 une fois qu'il aurait terminé l'examen du document WP.80 afin de voir s'il restait d'autres questions à traiter.

B. EXAMEN DES PROJETS D'ARTICLES

Article A. Définitions

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

"Aux fins des présentes Règles:

a) Le terme "signature électronique" désigne des données sous forme électronique contenues dans un message de données, ou jointes ou logiquement associées audit message et [pouvant être] utilisées pour [identifier le détenteur de la signature dans le cadre du message de données et indiquer qu'il approuve l'information qui y est contenue].

b) Le terme "signature électronique renforcée" désigne une signature électronique qui [est créée et] peut être vérifiée par l'application d'une procédure de sécurité ou d'une combinaison de procédures de sécurité qui garantit que cette signature électronique:

i) est particulière au détenteur de la signature [aux fins pour lesquelles][dans le contexte où] elle est utilisée;

ii) peut être utilisée pour identifier objectivement le détenteur de la signature dans le cadre du message de données;

iii) a été créée et apposée au message de données par le détenteur de la signature ou à l'aide d'un moyen dont seul ce détenteur a le contrôle.

c) Le terme "détenteur de la signature" désigne une personne par qui, ou au nom de qui, une signature électronique renforcée peut être créée ou apposée à un message de données.

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

Alinéa a) – Définition du terme "signatures électroniques"

23. On a fait valoir que si l'on considérait la question de la définition de la signature électronique d'un point de vue général, une telle définition était superflue puisque la notion de signature électronique était bien connue et bien comprise. Selon un autre avis, il ne fallait pas utiliser le terme "signature" car il laissait entendre que la notion juridique de signature était définie alors que les Règles uniformes visaient uniquement à réglementer l'utilisation de certaines technologies. Le terme "signature électronique", tout comme le terme "signature numérique", représentait une notion technique et ne devait pas être employé comme terme juridique indiquant l'existence d'un effet juridique. Selon un autre avis encore, aucune définition n'était nécessaire puisque la notion de "signature électronique" était suffisamment expliquée à l'article 7 de la Loi type.

24. En réponse aux arguments précédents, on a fait observer que le terme "signature électronique" ne pouvait pas avoir une acception uniquement technique puisqu'il ne faisait référence à aucune technique particulière de signature, mais visait à créer un lien entre diverses techniques et la notion juridique de signature. Pour ce qui était de savoir si l'article 7 de la Loi type traitait suffisamment la question de la définition d'une "signature" dans un environnement électronique, on a fait observer que cet article ne contenait pas de définition. Il avait pour objectif de fournir une règle d'équivalence fonctionnelle pour une série de situations où l'on substituait des dispositifs techniques aux signatures

manuscrites traditionnelles. Selon un avis largement partagé, il faudrait traiter la question de la définition de la "signature électronique" en tenant compte de la structure du document WP.80. On a fait observer qu'une définition était nécessaire à deux titres: parce qu'en vertu du projet d'article B une signature électronique produisait des effets juridiques et pour qu'il soit possible d'établir une définition de la signature électronique renforcée, Après un débat, il a été généralement estimé qu'il fallait prévoir une définition des termes "signature électronique". Toutefois, selon un avis, une définition n'était pas nécessaire, car aucun effet juridique n'y serait attaché (voir ci-dessous par. 48).

25. Diverses suggestions ont été formulées quant à la manière d'améliorer la définition du terme "signature électronique". Selon l'une d'entre elles, largement appuyée, il fallait enlever les crochets entourant les mots "pouvant être". De l'avis général, la définition ne devrait pas uniquement viser le cas où une signature électronique était effectivement utilisée mais indiquer plutôt que cette dernière constituait un dispositif technique de signature.

26. On a également fait valoir que l'emploi du terme "approuve" était trop subjectif et créait une incertitude dans la mesure où l'approbation dépendait des intentions du signataire au moment de la signature. On a suggéré d'employer un libellé plus objectif et proposé comme solution, le texte ci-après, fondé sur un projet de directive du Parlement et du Conseil européens sur un cadre commun pour les signatures électroniques:

> "Le terme «signatures électroniques» désigne des données sous forme électronique jointes ou logiquement associées à d'autres données électroniques et servant de méthode d'authentification."

27. En réponse à cette proposition, on a fait observer que l'emploi du terme "approuve" n'impliquait pas nécessairement une appréciation de l'intention subjective du signataire concernant, par exemple, les effets contractuels ou autres effets juridiques du message. Ce terme se limitait en fait à associer le signataire au message, ce qui constituait un élément nécessaire de la plupart des définitions existantes de tout type de signature, comme le montrait l'utilisation de la notion d'"approbation" à l'article 7 de la Loi type. Le Groupe de travail n'a pas adopté la solution proposée.

28. Afin de tenir compte de certaines des opinions et des craintes exprimées au cours du débat, il a été proposé de formuler plus clairement les éléments nécessaires à la définition d'une signature électronique en employant le libellé suivant:

> "Le terme «signature électronique» désigne des données sous forme électronique qui:
>
> a) sont contenues dans un message de données, ou jointes ou logiquement associées audit message;
>
> b) sont fournies par un signataire comme moyen de s'identifier;
>
> c) sont utilisées par un signataire pour indiquer qu'il approuve l'information contenue dans le message de données; et
>
> d) peuvent être utilisées pour vérifier cette identification".

29. On a fait remarquer que les changements proposés avaient pour but de préciser d'une part que si les données qui constituaient la signature électronique devaient servir de moyen d'identification du signataire, ces données pouvaient n'être utilisées à cette fin qu'un certain temps après la création de la signature, et d'autre part que la vérification des moyens d'identification pouvait être effectuée par le destinataire, le signataire ou un tiers, mais qu'elle devait être possible. Toutefois, compte tenu des observations précédemment formulées au sujet du mot "approbation", il a été suggéré de supprimer l'alinéa c).

30. Le texte proposé a bénéficié d'un certain appui mais des doutes ont été exprimés quant à l'utilité de l'alinéa d). Cet alinéa impliquait la participation possible de tiers à la vérification de la signature et n'était donc pas directement lié à la signature effective. En outre, il n'était peut-être pas nécessaire pour la catégorie générale des signatures électronique puisque cette catégorie pouvait inclure des types de signature où une vérification n'aurait pas grand sens.

31. Il a été proposé, pour aligner la définition figurant dans le document WP.80 avec l'article 7 de la Loi type, de remplacer les mots "des données sous forme électronique contenues dans un message de données, ou jointes ou logiquement associées auxdits messages et" par les mots "toute méthode dans le cadre d'un message de données", de manière à ce que le libellé se lise comme suit:

> "Le terme «signature électronique» désigne toute méthode dans le cadre d'un message de données pouvant être utilisée pour [identifier le détenteur de la signature dans le cadre du message de données et indiquer qu'il approuve l'information qui y est contenue]."

32. Après un débat, le Groupe de travail a décidé de conserver la définition énoncée à l'alinéa a) en enlevant tous les crochets. Il a également décidé qu'il fallait, pour permettre la poursuite du débat à un stade ultérieur, établir un projet de variante basé sur le libellé proposé ci-dessus (voir par. 31), qui faisait référence à l'utilisation d'une "méthode" comme dans l'article 7 de la Loi type.

Alinéa b) – Définition du terme "signature électronique renforcée"

33. Il a été proposé de remplacer la notion de "signature électronique renforcée" par celle de "signature électronique certifiée" qui, a~~t~~on déclaré, correspondait mieux à la pratique des signatures numériques. Cett e proposition a bénéficié d'un appui mais il a été généralement estimé que la notion de signature "renforcée" était préférable dans la mesure où l'intervention d'un tiers pour certifier la signature ne serait pas toujours nécessaire.

34. Pour mieux exprimer l'idée que la signature électronique renforcée devait être à la fois unique en tant que signature et particulière au signataire, il a été proposé de remplacer l'alinéa b) par le libellé suivant:

> "Le terme «signature électronique renforcée» désigne une signature électronique dont on peut démontrer, par l'application d'une procédure de sécurité:
>
> i) qu'elle était unique dans le contexte dans lequel elle a été utilisée; et
>
> ii) qu'elle n'a été utilisée par nulle autre personne que le signataire".

35. Cette proposition a bénéficié d'un certain appui. Toutefois, on s'est demandé si les éléments de la définition contenus dans la nouvelle proposition ou dans les alinéas i) à iii) originaux ne créaient pas une différence de fond entre une "signature électronique" et une "signature électronique renforcée". Il a été proposé, pour exprimer la spécificité d'une "signature électronique renforcée", d'ajouter à l'alinéa b) un libellé supplémentaire s'inspirant de l'alinéa b) iv) figurant dans le document WP.79, à savoir:

> "iv) a été créée et est liée au message de données auquel elle se rapporte d'une manière telle que tout changement apporté audit message apparaîtrait".

36. L'ajout proposé a bénéficié d'un large appui, car il créait un lien nécessaire (et par ailleurs manquant) entre la signature renforcée et l'information contenue dans le message de données. On a déclaré que l'application d'une "signature électronique renforcée" devrait rendre plus difficile toute altération ultérieure du message, à peu près de la même façon que l'apposition d'une signature manuscrite rendait plus difficile la modification du contenu d'un

document papier. On a en outre fait observer que, même si la fonction décrite à l'alinéa iv) était analogue à la "fonction de hachage" qu'offraient les signatures numériques, toute autre technique de signature (par exemple les techniques d'authentification fondées sur la dynamique des signatures) devrait pouvoir offrir le même niveau de fiabilité quant à l'intégrité du message. Une garantie à cet égard était d'autant plus nécessaire qu'il était facile d'apporter des changements indétectables à des documents électroniques.

37. On a fait valoir, à l'encontre de ce qui précède, que toutes les signatures électroniques offrant un degré élevé de sécurité n'assureraient pas la fonction mentionnée à l'alinéa iv), qui était caractéristique de certains types de signatures numériques seulement. Quant à un éventuel parallèle entre la fonction de hachage et la signature manuscrite, on a fait observer qu'une signature manuscrite n'offrait pas en elle-même une grande sécurité contre l'altération du document. S'agissant de la différence entre une "signature électronique" au sens de l'alinéa a) et une "signature renforcée" au sens de l'alinéa b) i) à iii), on a déclaré que seule la signature "renforcée" impliquait intrinsèquement l'utilisation de procédures de sécurité pouvant donner de bonnes garanties objectives quant à l'identité du signataire. Selon une opinion, il fallait faire une distinction entre une telle fonction d'identification et la fonction de vérification de l'intégrité du message, qui pourrait n'être nécessaire que lorsque la loi exigeait un document original. S'agissant de la forme, on a déclaré que le libellé de l'alinéa iv) risquait de donner lieu à une interprétation erronée, en particulier si la disposition selon laquelle toute altération du message de données devrait "apparaître" impliquait que la nature exacte de la modification serait explicite. Il a été proposé, si l'on conservait l'alinéa iv), d'employer un libellé fondé sur le texte de l'article 8-1 a) de la Loi type (par exemple "offre une garantie raisonnable quant à l'intégrité du message").

38. On a exprimé la crainte que l'ajout de l'alinéa iv) dans la définition du terme "signature électronique renforcée" ne conduise à s'interroger sur la cohérence entre les Règles uniformes et l'article 8 de la Loi type. L'article 8, en effet, prévoyait que l'intégrité devait être garantie "à compter du moment où [l'information] a été créée pour la première fois sous sa forme définitive", alors que l'alinéa iv) n'exigerait l'intégrité qu'à partir du moment où la signature était apposée. On a répondu, à ce propos, que la définition du terme "signature électronique renforcée" ne visait pas à traiter l'équivalence fonctionnelle entre un message de données et un document original à toutes les fins juridiques. En fait, elle avait pour but de veiller à ce qu'une signature électronique renforcée puisse identifier de façon fiable un message donné comme étant le message qui avait bien été envoyé.

39. Après un débat, le Groupe de travail a décidé qu'un texte allant dans le sens de l'alinéa iv) proposé devrait être ajouté entre crochets au texte de l'alinéa b) ou, en tant que variante, au texte proposé au paragraphe 34 ci-dessus, pour que le débat puisse se poursuivre une fois qu'il aurait examiné les dispositions de fond du projet de Règles uniformes. Il pourrait être nécessaire, a-t-on estimé, de réexaminer la définition des termes "signature électronique renforcée" en même temps que l'architecture générale des Règles uniformes, une fois que l'on aurait clarifié l'objectif de la prise en considération de deux catégories de signature électronique, notamment en ce qui concernait leurs effets juridiques. Il pourrait être justifié de traiter les signatures électroniques offrant un degré élevé de fiabilité uniquement si les Règles uniformes prévoyaient un équivalent fonctionnel pour des utilisations spécifiques des signatures manuscrites (par exemple les actes notariés, les signatures certifiées par des témoins et d'autres types de signatures certifiées). Cependant, on a fait également observer que l'unification ou l'harmonisation internationale de telles utilisations spécifiques des signatures manuscrites pourrait être particulièrement difficile sans pour autant être d'une grande utilité pour l'immense majorité des transactions commerciales internationales. Si, pour ces raisons, de telles exigences de forme devaient demeurer en dehors du champ d'application des Règles uniformes, il faudrait peut-être préciser l'avantage supplémentaire à attendre de l'utilisation d'une "signature électronique renforcée" par rapport à une simple "signature électronique", éventuellement dans le contexte du projet d'article B. Le Groupe de travail est convenu qu'il serait peut-être nécessaire de rouvrir le débat sur cette question à un stade ultérieur.

Alinéa c) – Définition de l'expression "détenteur de la signature"

40. L'alinéa c) a bénéficié quant au fond d'un appui général, mais il a été demandé si la définition de l'expression "détenteur de la signature" remplacerait simplement la définition du mot "signataire" figurant dans le document WP.79. On a fait valoir que, même si le détenteur de la signature et le signataire étaient dans la plupart des cas la même personne, il pourrait être nécessaire d'utiliser ces deux notions pour établir une distinction entre l'acte de signature et la simple possession d'un dispositif de signature. Les discussions ont été axées sur la définition de l'expression "détenteur de la signature", mais il a été largement admis qu'il pourrait être nécessaire de rouvrir le débat ultérieurement sur la définition qui pourrait être donnée du mot "signataire".

41. Plusieurs avis ont été exprimés quant à la formulation exacte de l'alinéa c). Selon un avis, la définition ne devrait pas uniquement viser les cas où une "signature électronique renforcée" était utilisée mais elle devrait être étendue aux cas où des dispositifs de signature étaient employés dans le cadre de simples "signatures électroniques". Dans la mesure où le "détenteur de la signature" pouvait avoir des droits et des obligations en vertu des projets d'articles E, F et G, il n'y avait pas de raisons pour que les mêmes droits et obligations ne soient pas applicables aux utilisateurs des "signatures électroniques" en général. On a toutefois mis en garde contre le fait d'imposer à tous les utilisateurs de signatures électroniques les obligations créées pour le détenteur de la signature en vertu de ces articles. Par exemple, conformément à la législation de certains pays, le simple fait de dactylographier le nom du signataire à la fin d'un message électronique pourrait suffire pour constituer une "signature". Cependant, il n'était peut-être pas opportun de prévoir que le signataire devrait protéger ces "signatures" dans la même mesure que le "détenteur de la signature" devrait protéger le "dispositif de signature" contenant une clef privée dans le cadre d'une infrastructure à clef publique. Il a été généralement convenu que cette question devrait être examinée plus à fond dans le contexte des projets d'articles E à G.

42. Selon un avis largement partagé, il faudrait que l'alinéa c) ne s'applique qu'au détenteur "légitime" du dispositif de signature, à savoir la personne dont les droits et obligations étaient mentionnés dans les articles suivants des Règles uniformes. Ainsi, toute personne entrant en possession d'un dispositif de signature de façon frauduleuse ne devait pas être protégée par ces Règles.

43. On a craint que les mots "au nom de qui" ne soulèvent des questions concernant le droit de la représentation des entités juridiques, sur lequel les Règles uniformes ne devraient pas empiéter. En réponse à cette observation, il a été indiqué qu'un libellé analogue avait été introduit dans la définition du mot "expéditeur" conformément à la Loi type, étant entendu que toute incidence concernant la représentation serait traitée par référence au droit applicable en dehors de la Loi type. De l'avis général, la même hypothèse devrait être retenue dans le cadre des Règles uniformes (voir ci-dessous par. 90).

44. On a craint également que la notion de "détenteur de la signature" ne soit incompatible avec la notion d'"expéditeur" au sens de la Loi type. En réponse à cette observation, il a été indiqué que, même si le détenteur de la signature et l'expéditeur pouvait être la même personne, il était justifié de conserver deux définitions, compte tenu de leur objet distinct. La notion d'expéditeur était utilisée pour déterminer la personne à laquelle le message était attribuable, alors que le détenteur de la signature devait être identifié pour déterminer la personne à qui incombaient les obligations concernant la gestion du dispositif de signature.

45. D'un point de vue rédactionnel, on a estimé que la notion de "détenteur du dispositif de signature" était plus judicieuse, mais certainement plus difficile à manier, que la notion de "détenteur de la signature".

46. Pour tenir compte de certains des avis et préoccupations qui avaient été exprimés, il a été proposé d'examiner un nouveau texte pour l'alinéa c) libellé comme suit:

> "Le terme «signataire» désigne une personne qui détient légitimement un dispositif de création de signature et agit soit en son nom propre, soit au nom de l'entité qu'il représente".

47. Le Groupe de travail n'a pas conclu ses délibérations sur l'alinéa c). Au cours de l'échange de vues auquel a donné lieu la définition de l'expression "détenteur de la signature", on a estimé que le champ d'application de la définition (de même que le champ d'application du projet de Règles uniformes en général) était trop large et que de ce fait les différentes règles qui y figuraient étaient trop générales pour régler efficacement les difficultés rencontrées dans la pratique en ce qui concerne les infrastructures à clefs publiques dans le cadre desquelles les signatures numériques étaient utilisées (pour la poursuite du débat, voir ci-dessous par. 66).

48. Le Groupe de travail a engagé un débat général sur le champ d'application des Règles uniformes. Compte tenu des diverses observations et préoccupations exprimées précédemment au cours des discussions, il a été proposé que les notions de signature électronique et de signature électronique renforcée ne soient pas utilisées dans les Règles uniformes car elles n'étaient pas en fait des "signatures", mais plutôt des techniques qui permettaient d'identifier l'expéditeur d'un message de données et d'identifier les messages qui étaient envoyés. En conséquence, il n'y avait pas de raison d'utiliser le mot "signature" pour décrire ces techniques et, en fait, si on l'utilisait, cela pourrait créer des confusions en ce sens que le mot "signature" avait des significations étroitement associées à son utilisation dans l'environnement papier et aux effets juridiques de cette utilisation dans cet environnement (voir ci-dessus par. 23 et 24). Il a été proposé que l'article 7 de la Loi type renferme une règle, pour autant qu'une telle règle soit nécessaire, qui traiterait suffisamment de l'équivalent fonctionnel des signatures dans les environnements papier et électronique. Formuler une règle indiquant quelles techniques de signature satisferaient au critère prévu à l'article 7 n'était pas judicieux compte tenu de ces facteurs et aussi des difficultés rencontrées pour faire en sorte que des technologies qui n'avaient pas encore été élaborées puissent entrer dans le champ d'application d'une telle disposition. En outre, selon un avis, il n'y avait pas lieu d'adopter une règle unique pour indiquer quelle technique de signature satisferait aux dispositions de l'article 7 de la Loi type, compte tenu de la diversité de la notion de "signature" dans les différentes traditions juridiques.

49. Selon une autre proposition, le Groupe de travail devrait envisager les technologies qui avaient été mises au point et qui étaient actuellement utilisées dans les transactions commerciales, comme les techniques de signature numérique dans une infrastructure à clef publique. Lorsque les règles régissant les infrastructures à clef publique auraient été arrêtées, il serait possible d'envisager si ces règles peuvent s'appliquer plus largement. Cela étant, il a été proposé que le Groupe de travail n'examine pas les projets d'articles A à D du document WP.80 mais fasse porter son attention sur les projets d'articles F à H du même document, dans le cadre des infrastructures à clef publique (voir ci-dessus par. 4).

50. Cette proposition a été largement appuyée, mais on a craint qu'un examen axé essentiellement sur les infrastructures à clef publique ne soit trop restrictif et risque de porter préjudice à d'autres technologies. On a estimé qu'il ne faudrait pas écarter les projets d'articles A à D sans les examiner de façon plus approfondie, mais que cet examen pourrait être reporté après le débat sur les projets d'articles F à H. On a fait observer que le projet d'article B, en particulier, pourrait jouer un rôle important dans la définition du champ d'application des articles F à H. En outre, on a fait valoir que l'article E, qui traitait du principe de l'autonomie des parties, serait important pour aborder l'examen des obligations des parties dans les articles F à H. Selon une autre proposition, la question de la reconnaissance internationale des signatures numériques et certificats étrangers, traitée dans les projets d'articles 17 à 19 du document A/CN.9/WG.IV/WP.76, devrait aussi être examinée dans le cadre des règles régissant les infrastructures à clef publique. Il a également été indiqué que le document WP.79 pourrait jouer un rôle utile pour déterminer s'il y avait d'autres questions (outre celles évoquées dans les projets d'articles E à H et les questions de reconnaissance internationale) qui pourraient être examinées dans le cadre des règles régissant les infrastructures à clef publique.

51. Il a été généralement convenu que le Groupe de travail devrait poursuivre l'examen de ces questions, étant entendu qu'il concentrerait tout d'abord son attention sur les règles applicables aux infrastructures à clef publique exposées dans les projets d'articles E à H du document WP.80, et qu'il pourrait peut-être envisager d'étendre ces règles une fois qu'elles auraient été arrêtées; que la question de la neutralité quant aux techniques utilisables et des

effets juridiques des infrastructures à clef publique ne serait pas examinée plus avant à ce stade mais qu'il en serait tenu compte ultérieurement dans la poursuite des débats; et que les questions relatives à la reconnaissance internationale viendraient s'ajouter aux thèmes à examiner. Il a été admis que dans la mesure où le document WP.80 n'avait pas été rédigé dans cette optique, il devrait être uniquement considéré comme point de départ des discussions. S'agissant de la forme des Règles uniformes, puisque aucune décision finale ne pouvait être arrêtée à ce stade, le Groupe de travail a retenu comme hypothèse de travail que les dispositions en cours d'élaboration seraient des règles juridiques assorties de commentaires, et non simplement des principes directeurs (pour la poursuite du débat, voir ci-dessous par. 72).

52. Le Groupe de travail est ensuite passé à l'examen quant au fond des projets d'articles E à G.

Article E. Liberté contractuelle

53. Le texte de l'article E examiné par le Groupe de travail était le suivant:

> "Le détenteur d'une signature ou toute personne qui peut se fier à la signature électronique dudit détenteur peut déterminer qu'entre eux, la signature électronique doit être traitée comme une signature électronique renforcée".

54. Puisque le Groupe de travail devait examiner la question de l'autonomie des parties dans le cadre de l'infrastructure à clef publique, on a estimé que le projet d'article E était peut-être trop étroitement circonscrit et qu'il fallait replacer la question dans un contexte plus large. Si, de l'avis général, toutes les parties commerciales devraient être libres de contracter et de répartir les risques entre elles, il pourrait être néanmoins nécessaire d'énoncer certaines limites, par exemple en ce qui concernait la protection des consommateurs ou d'autres questions d'ordre public.

55. Pour faciliter le débat sur une notion plus large de l'autonomie des parties, le texte suivant a été proposé:

> "1. Les présentes Règles visent uniquement les relations commerciales et ne sont pas appliquées de manière à être en conflit avec une loi relative à la protection des consommateurs.
>
> 2. Les parties commerciales sont libres, par convention expresse ou tacite, de modifier tout aspect des présentes Règles ou de s'en écarter.
>
> (Le Commentaire indiquerait qu'«Aucune des dispositions des présentes Règles n'est impérative».)
> (Le Commentaire indiquerait que cette disposition sur l'autonomie des parties se rapporte uniquement aux présentes Règles, et qu'elle n'a pas d'incidences sur les dispositions d'ordre public ou sur les dispositions impératives applicables aux contrats, telles que les dispositions relatives aux contrats léonins.)
>
> 3. Aucune des dispositions des présentes Règles n'est appliquée de façon à exclure, restreindre, ou pénaliser toute autre forme de signature électronique [satisfaisant aux exigences de l'article 7 de la Loi type sur le commerce électronique] [apposée à un message de données et suffisamment fiable au regard de l'objet pour lequel ledit message a été créé ou communiqué, compte tenu de toutes les circonstances, y compris toute convention en la matière.]."

56. Les membres du Groupe de travail se sont généralement déclarés favorables à un article allant dans le sens de la proposition susmentionnée. S'agissant de la forme, il a été proposé d'aligner la référence aux consommateurs, au paragraphe 1 du projet d'article, sur le libellé de la note** relative à l'article premier de la Loi type, qui était ainsi rédigée: "La présente loi ne se substitue à aucune règle de droit visant à protéger le consommateur" (voir ci-dessus par. 20 et ci-dessous par. 70). Il a aussi été proposé de supprimer le second libellé entre crochets dans le

paragraphe 3, puisque la référence à l'article 7 de la Loi type était la variante la plus appropriée. En outre, pour aligner le libellé sur l'article 7, il faudrait aussi remplacer les mots "signature électronique" par le mot "méthode". Il a été proposé par ailleurs de remplacer le titre du projet d'article E par "autonomie des parties". Ces propositions ont bénéficié d'un appui général.

57. On a fait valoir que la référence à une convention entre les parties ne traitait pas de façon suffisamment claire la question d'un préjudice éventuel pour les tiers non parties à la convention. Pour veiller à ce que toute convention entre les parties ne puisse pas avoir d'effets sur les tiers, il a été proposé d'adopter, en s'inspirant du projet d'article E, des termes indiquant que les parties étaient libres de s'accorder "entre elles" sur certains effets. Cette proposition a été largement appuyée.

58. On a exprimé quelques inquiétudes quant au sens du paragraphe 3 et à sa relation avec les paragraphes 1 et 2. On a fait observer que si les paragraphes 1 et 2 portaient clairement sur la question de l'autonomie des parties, le paragraphe 3, par contre, introduisait un nouveau principe, à savoir celui de la non-discrimination. Sans examiner plus avant la teneur de cette disposition au stade actuel, il a été proposé de faire du paragraphe 3 un article séparé. Cette proposition a été largement appuyée. Quant au sens de ce paragraphe, on a fait valoir qu'une telle disposition n'était pas nécessaire puisque le projet de Règles n'avait pas pour objet de privilégier une technique ou une autre, même s'il était axé sur l'infrastructure à clef publique. Il a été largement estimé, cependant, qu'en attendant une décision finale du Groupe de travail sur la question de savoir si les Règles uniformes traiteraient de conséquences juridiques particulières de l'utilisation des signatures numériques et autres signatures électroniques, il était utile d'avoir une disposition allant dans le sens du paragraphe 3.

59. Une autre crainte a été exprimée concernant l'article proposé sur l'autonomie des parties, à savoir que dans le contexte du projet d'article F, qui visait les obligations à la fois contractuelles et extracontractuelles, il pouvait permettre aux parties de convenir de modifier la responsabilité délictuelle. On a fait valoir, en réponse à cet argument, que dans les relations commerciales les parties devaient être libres de modifier ces obligations et, par exemple, d'accepter un niveau de responsabilité délictuelle supérieur ou inférieur à celui qui était normalement prévu par la loi.

60. Pour tenir compte des diverses opinions et préoccupations exprimées au cours du débat, la proposition initiale a été modifiée comme suit:

> "1. Les présentes Règles régissent uniquement les relations commerciales et ne sont pas appliquées de manière à se substituer à toute loi visant à protéger les consommateurs.
>
> 2. Les parties commerciales sont libres, par convention expresse ou tacite, entre elles, de modifier tout aspect des présentes Règles ou de s'en écarter.
>
> (Le Commentaire indiquerait qu'«Aucune des dispositions des présentes Règles n'est impérative».)
> (Le Commentaire indiquerait que cette disposition sur l'autonomie se rapporte uniquement aux présentes Règles et n'a pas d'incidences sur les dispositions d'ordre public ou sur les dispositions impératives applicables aux contrats [, telles que les dispositions relatives aux contrats léonins].)
> (Le Commentaire pourrait traiter de la signification des termes «entre elles».)
>
> 3. Aucune des dispositions des présentes Règles n'est appliquée de manière à exclure, restreindre, ou pénaliser toute autre méthode [de signature] satisfaisant aux exigences de l'article 7 de la Loi type sur le commerce électronique."

61. La proposition révisée a bénéficié d'un large appui quant au fond. Toutefois, on a estimé que le principe de l'autonomie des parties pourrait être exprimé de façon plus succincte. Quelques doutes ont également été émis sur

la question de savoir si les règles devraient être limitées aux relations commerciales, comme indiqué au paragraphe 1 de la proposition, ou si les projets d'articles F à H pourraient également être utiles en ce qui concernait les consommateurs. Il a été suggéré d'appliquer les règles de la même manière aux consommateurs et aux parties commerciales, à condition qu'elles n'aient pas d'incidences sur les dispositions impératives concernant la protection des consommateurs. Selon un avis, la référence aux dispositions impératives ou aux dispositions d'ordre public devrait être transférée du commentaire pour être explicitement énoncée dans le texte de la règle proposée.

62. Pour tenir compte de certaines des préoccupations exprimées à propos des paragraphes 1 et 2, le libellé suivant a été proposé:

> "Les présentes Règles s'appliquent uniquement dans la mesure où les parties n'en ont pas convenu autrement et ne se substituent à aucune disposition impérative ou disposition d'ordre public."

Cette proposition a bénéficié d'un certain appui.

63. On a fait observer que, pour bien comprendre qu'elle était la portée d'un article sur l'autonomie des parties, il pourrait être important d'examiner la nature des projets d'articles F à H. Selon un avis, ces projets d'articles devaient combler des lacunes ou servir de règles par défaut s'appliquant lorsque les parties n'avaient conclu aucune convention sur les questions visées. Selon un autre avis, ils s'appliqueraient sauf si les parties en convenaient autrement. L'opinion selon laquelle les projets d'articles F à H devraient servir à combler des lacunes a bénéficié d'un large appui.

64. Après un débat, le Groupe de travail a conclu que tant les propositions détaillées que la proposition concise concernant un nouvel article sur l'autonomie des parties visaient le même principe. Il a été convenu que, pour continuer le débat à une prochaine session, il faudrait que l'article révisé sur l'autonomie des parties traite de la législation relative à la protection des consommateurs, soit centré sur les relations commerciales, telles que définies dans la note **** relative à l'article premier de la Loi type, garantisse la liberté contractuelle des parties, et préserve les lois impératives. Il a donc été décidé que ces principes sur l'autonomie des parties formeraient une base satisfaisante pour l'examen des projets d'articles F à H et que le débat sur la question pourrait être repris à un stade ultérieur, à la lumière de l'examen de ces projets d'articles. S'agissant de la nécessité d'une disposition sur la non-discrimination, question soulevée lorsqu'il avait été proposé d'inclure un article plus détaillé sur l'autonomie des parties, aucune décision n'a été prise. Il a été convenu d'en reporter l'examen après celui des projets d'articles F à H.

Article F. Obligations du détenteur de la signature

65. Le texte de l'article F examiné par le Groupe de travail était le suivant:

> "1. Le détenteur d'une signature a l'obligation:
>
> a) de faire preuve de la diligence voulue pour éviter l'utilisation non autorisée de sa signature;
>
> b) d'avertir [les personnes voulues] [aussitôt que possible] si sa signature est compromise et pourrait être utilisée pour créer des signatures électroniques renforcées non autorisées;
>
> c) de veiller, de bonne foi, à ce que toutes les déclarations faites par lui aux certificateurs d'informations et aux parties se fiant à la signature soient exactes et complètes.
>
> 2. Le détenteur d'une signature est responsable des conséquences de l'inexécution des obligations énoncées au paragraphe 1."

Remarques générales

66. Avant de conclure, provisoirement, ses délibérations sur la définition des termes “détenteur de la signature” au projet d’article A (voir ci-dessus par. 40 à 47), le Groupe de travail s’était demandé si ledit détenteur devrait satisfaire aux obligations énoncées au projet d’article F. Il a été rappelé que, puisque le terme “signature” renvoyait à un dispositif technique et non à la notion juridique de signature, le terme “détenteur de la signature” pourrait donner lieu à des interprétations erronées. Selon un avis, les termes “détenteur du dispositif” seraient préférables. On a aussi rappelé que, compte tenu de la décision du Groupe de travail d’examiner tout d’abord les questions relatives à l’infrastructure à clef publique avant d’étendre éventuellement le champ d’application des Règles uniformes à d’autres techniques de signature électronique, il serait peut-être plus approprié d’employer la terminologie établie dans ce domaine. En conséquence, des termes tels que “abonné” ou “détenteur de la clef” seraient peut-être préférables. Si tous les membres du Groupe de travail ont convenu qu’il fallait remplacer le terme “détenteur de la signature” par une formulation plus appropriée, aucune décision définitive n’a été prise à cet égard. Il a été décidé qu’il faudrait peut-être réexaminer et définir à un stade ultérieur les termes “détenteur du dispositif”, “détenteur du dispositif de signature”, “détenteur de la clef” et “abonné”, qui avaient tous été employés comme synonymes pendant le débat.

67. On a fait observer, au cours de ce débat, que les notions de “détenteur de clef” et d’“abonné” pourraient correspondre à des stades différents du cycle de vie d’une paire de clefs. En effet, si la paire de clefs était normalement créée avant la demande de certificat, les Règles uniformes, par contre, devraient s’appliquer uniquement aux clefs et aux détenteurs de clefs, à compter de l’émission (ou de la demande) d’un certificat d’identification pour permettre l’utilisation pratique des clefs. Cet argument a bénéficié d’un certain appui mais, selon l’avis qui a prévalu, si le détenteur de la clef ne devrait avoir d’obligations que pour les paires de clefs effectivement protégées par un certificat (c’est-à-dire au moment où le certificat était émis), en revanche son devoir de protéger ces clefs certifiées contre toute utilisation abusive devrait être rétroactif jusqu’au moment de la création de la paire de clefs.

68. S’agissant de la référence générale à l’infrastructure à clef publique et à la terminologie qui s’y rapporte, on a estimé que le jeu des relations entre trois types distincts de parties (c’est-à-dire les détenteurs des clefs, les autorités de certification et les parties se fiant à la signature) correspondait à un modèle possible d’infrastructure à clef publique mais que d’autres modèles étaient concevables, où il n’y avait pas, par exemple, d’autorité de certification indépendante. Les membres du Groupe de travail ont généralement accepté cet avis. Ils ont cependant estimé dans l’ensemble que le fait de se concentrer sur les questions relatives à l’infrastructure à clef publique avait notamment pour grand avantage de permettre de structurer plus facilement les Règles uniformes autour de trois fonctions (ou rôles) relatives aux paires de clefs, à savoir la fonction d’émetteur de la clef (ou d’abonné), la fonction de certification et la fonction de confiance. De l’avis général, ces trois fonctions étaient communes à tous les types d’infrastructure à clef publique, et devaient être traitées, qu’elles soient remplies par trois entités séparées ou que deux d’entre elles soient remplies par la même entité (par exemple, lorsque l’autorité de certification était également la partie se fiant à la signature). En outre, on a largement estimé qu’il serait plus facile d’établir, à un stade ultérieur, une règle entièrement neutre quant aux techniques utilisées, si l’on se concentrait sur les fonctions caractéristiques de l’infrastructure à clef publique et non sur tel ou tel modèle particulier (pour la poursuite du débat, voir ci-dessous par. 109).

69. Le Groupe de travail s’est ensuite penché sur la question de savoir qui pourrait être tenu de satisfaire aux obligations énoncées au projet d’article F. Il a été largement estimé qu’il faudrait prendre uniquement en considération le détenteur “légitime” de la clef. En outre, il a été convenu que seul un détenteur sachant qu’il était en possession d’une paire de clefs et ayant exprimé l’intention d’utiliser la clef devrait être tenue de satisfaire à ces obligations. On a établi, à cet égard, un parallèle entre la détention d’une paire de clefs et la détention d’une carte de crédit. On s’est rendu compte, toutefois, qu’il faudrait aussi tenir compte d’autres types de situations. Par

exemple, un acheteur potentiel pourrait recevoir d'un vendeur une paire de clefs devant servir à sécuriser les opérations possibles avec ce vendeur. Une telle paire de clefs pourrait être envoyée par une messagerie électronique, sans que le destinataire du message soit au courant de l'émission et de l'attribution de cette paire de clefs. Les membres du Groupe de travail se sont accordés à penser que, dans un tel cas, le bénéficiaire de la paire de clefs ne devrait pas correspondre à la définition du "détenteur de la clef" et qu'il ne devrait avoir aucune obligation au titre des Règles uniformes. On a fait observer que la notion de "soin raisonnable" pourrait être suffisante dans une telle situation puisqu'on ne pouvait attendre aucun "soin raisonnable" concernant la paire de clefs d'un détenteur n'était pas au courant.

70. Lors du débat sur la question de savoir qui serait tenu de satisfaire aux obligations énoncées dans le projet d'article F, le Groupe de travail a examiné les conséquences de sa décision précédente de traiter les questions concernant la législation relative à la protection des consommateurs par une disposition analogue à la note** relative à l'article premier de la Loi type. On a estimé que (tout au moins dans la législation d'un petit nombre de pays), même lorsque le détenteur d'une clef avait exprimé l'intention d'utiliser une paire de clefs, les obligations énoncées au projet d'article F pourraient être jugées trop dures si ledit détenteur était considéré comme un consommateur. S'il a été généralement estimé que, dans un grand nombre de pays, l'obligation générale de diligence figurant dans le projet d'article F s'appliquerait également aux consommateurs, le Groupe de travail a toutefois réaffirmé sa décision de ne pas se lancer dans l'établissement de règles particulières visant les consommateurs pour le commerce électronique. Il a été rappelé qu'en vertu de cette décision, cependant, les consommateurs ne devaient pas être exclus du champ d'application des Règles uniformes et qu'il incomberait à chacun des États adoptant ces dernières de décider de la nécessité d'exclure certaines catégories d'utilisateurs de clefs de ce champ d'application (voir ci-dessus par. 20 et 56).

71. Le Groupe de travail a ensuite examiné la question de savoir envers quelle(s) personne(s) le détenteur de la clef avait les diverses obligations énoncées au projet d'article F. Selon un avis, il avait des obligations soit envers l'autorité de certification, soit envers toute autre partie pouvant se fier à une signature numérique dans le cadre de relations contractuelles avec lui. Toutefois, selon l'avis qui a prévalu, le détenteur de la clef avait des obligations envers toute partie qui pourrait raisonnablement se fier à une signature numérique, que cette partie soit ou non liée au détenteur par une relation contractuelle. Les relations entre le détenteur de la clef et une autorité de certification ou un émetteur de clefs indépendant seraient normalement de nature contractuelle, mais la relation entre le détenteur de la clef et les parties se fiant à la signature pourrait soit être de nature contractuelle dans le cadre d'une opération commerciale, soit fondée sur la responsabilité délictuelle. Étant donné la nature générale des obligations, on a estimé qu'il serait plus exact de parler au projet d'article F des "devoirs" du détenteur de la clef plutôt que de ses "obligations". Le Groupe de travail a pris note de cette proposition. De l'avis général, le texte des Règles uniformes devrait clairement établir que le détenteur de la clef avait des obligations envers toute partie qui se fiait raisonnablement à l'utilisation d'une clef et subissait un préjudice du fait de l'inexécution par le détenteur de cette clef de ses obligations. Il a aussi été convenu qu'aux fins du projet d'article F, les "parties se fiant raisonnablement" à l'utilisation d'une clef devraient inclure les autorités de certification.

72. Dans le cadre du débat général sur le projet d'article F, on a déclaré qu'il était trop ambitieux de s'employer, comme on le faisait actuellement, à établir dans les Règles uniformes une série de dispositions normatives de caractère législatif (voir ci-cessus par. 19 et 51) et qu'il pourrait donc être plus facile de régler les questions traitées dans ces Règles si l'on reconsidérait l'objet et la nature de l'ensemble du projet. Deux autres possibilités ont été proposées. La première consistait à limiter la teneur des Règles à une disposition législative type de caractère général, qui aurait pour effet d'offrir la reconnaissance la plus large possible à l'autonomie des parties. Le reste des questions actuellement traitées dans les Règles uniformes pourrait l'être dans un guide juridique visant à aider les parties à structurer leurs contrats concernant les questions relatives aux signatures électroniques. La seconde possibilité consistait à traiter l'ensemble des questions faisant l'objet des Règles uniformes dans un guide législatif, éventuellement accompagné de dispositions données à titre d'exemples. On a fait remarquer que l'hypothèse de travail actuelle qui était d'élaborer des dispositions législatives types accompagnées d'un guide législatif pourrait,

dans la pratique, ne pas être très différente de la dernière possibilité proposée, mais selon l'avis de la très grande majorité, le Groupe de travail devrait poursuivre sa tâche (dont l'importance a été réaffirmée, bien que certaines délégations aient mis en doute sa faisabilité) sur la base de l'hypothèse de travail actuelle (voir ci-dessus par. 51). On a fait observer que, le cas échéant, il pourrait envisager de laisser le choix dans le texte des Règles uniformes, entre plusieurs formulations.

Paragraphe 1

Alinéa a)

73. Il a été largement admis que des éléments supplémentaires devraient être insérés parallèlement à la notion exprimée par le membre de phrase "éviter l'utilisation non autorisée de la clef". On a estimé que le détenteur de la clef devrait être dans l'obligation d'éviter de faire un emploi abusif de la clef et de faire preuve de la diligence voulue en assurant le contrôle de la clef et le contrôle des informations contenues dans le dispositif de signature ou utilisées en liaison avec le dispositif de signature pour créer une signature numérique. Il a été généralement convenu que la notion de "contrôle" de la clef et des informations qu'elle contenait était essentielle, en particulier pour déterminer le moment à compter duquel le détenteur de la clef devait se conformer aux obligations énoncées dans le projet d'article F. En particulier, dans les cas où le contrôle de la clef était transféré à plusieurs détenteurs successifs, le projet d'article F devrait préciser que seule la personne qui exerçait le contrôle de la clef était dans l'obligation de la protéger.

74. S'agissant du débat sur le point de savoir qui contrôlait la clef, il a été demandé si, à un moment donné, il pouvait y avoir plus d'un détenteur d'une même clef. Il a été proposé d'ajouter au paragraphe 1 un libellé tel que: "dans le cas [de codétenteurs] [où plus d'une personne a le contrôle de la clef], les obligations prévues au paragraphe 1 sont conjointes". Le Groupe de travail a pris note de cette proposition et décidé qu'elle devrait apparaître dans le projet révisé des Règles uniformes à élaborer pour poursuivre le débat lors d'une session ultérieure.

75. S'agissant des mots "faire preuve de la diligence voulue", on a fait observer que le projet d'article F se fondait sur l'hypothèse que la responsabilité du détenteur de la clef reposait sur la notion de diligence (ou, en d'autres termes "de responsabilité pour négligence") plutôt que sur la notion de stricte responsabilité.

Alinéa b)

76. Une règle allant dans le sens de l'alinéa b) a suscité l'adhésion générale. On a fait observer que les mots placés entre crochets renvoyaient à deux questions importantes qu'il fallait préciser: les personnes à avertir et le moment auquel il fallait les avertir.

77. S'agissant de la première question, selon un avis, il ne fallait pas faire référence aux parties à notifier ou du moins ces parties ne devraient pas être précisées dans la mesure où différents organismes pouvaient être compétents lorsqu'il y avait répartition des fonctions des autorités de certification. Il a été proposé que cette question soit étudiée plus à fond ultérieurement, lorsque la portée des obligations visées dans ces règles aurait été précisée et que la question des personnes auxquelles elles s'appliquaient aurait été réglée. À ce moment, on pourrait expressément mentionner dans cet article les personnes concernées. Pour les mêmes raisons, il a été proposé de conserver les mots "les personnes voulues".

78. S'agissant du moment auquel il faudrait donner notification, il a été proposé de retenir les mots "sans retard excessif" car cette formule était bien comprise et largement utilisée dans un certain nombre de juridictions et offrait un degré de souplesse approprié.

79. À ce sujet, il a été demandé également à quel moment l'obligation d'avertir s'imposait. Selon une possibilité qui a été exposée, cette obligation devrait s'imposer au moins dès qu'il y a eu connaissance du fait que la clef était compromise, mais on a estimé que l'obligation pourrait intervenir avant ce moment s'il pouvait être établi que le détenteur de la clef aurait dû savoir que la clef était compromise. Selon un autre avis, l'obligation d'avertir s'imposait lorsque le détenteur de la clef avait "des raisons suffisantes de soupçonner" ou "avait des raisons plausibles de soupçonner" que la clef était compromise ou qu'elle était ou aurait pu être compromise. On s'est demandé s'il y avait une différence entre le critère de connaissance dans la première proposition et le fait que la clef soit compromise dans la deuxième. Différents avis ont été exprimés quant à la question de savoir si ces normes étaient les mêmes ou si elles parvenaient au même résultat, ou si le résultat dans chaque cas était souhaitable. S'agissant du dernier point, selon un avis, le fait d'attribuer la responsabilité au motif que la clef "aurait pu être compromise" imposait une trop lourde charge au détenteur de la clef et risquait de décourager l'utilisation de cette technologie. Après un échange de vues, le Groupe de travail a convenu d'une manière générale que ces deux normes devraient être incluses dans un projet révisé de l'alinéa b) qui serait examiné ultérieurement.

80. Il a été proposé que la règle énoncée à l'alinéa b), si elle traitait essentiellement de la question de la négligence, soit complétée par une règle portant sur la répartition des risques. Si la question des risques devait être envisagée, il serait alors nécessaire de décider à quel moment le risque était transféré du détenteur de la clef: lorsque la notification était donnée, lorsque la notification était reçue ou lorsqu'il était donné suite à la notification. En réponse à cette observation, il a été indiqué que les questions relatives au transfert du risque étaient différentes des règles concernant une conduite appropriée et raisonnable, qui reposaient sur la notion de faute. La notion de risque était importante lorsqu'il n'était pas question de faute. Ces deux types de règles devraient être considérés séparément, car la responsabilité ne pouvait pas être mise sur le même plan que le risque. On a fait observer que l'alinéa a) établissait l'obligation de prendre soin de la clef ce qui, en vertu du paragraphe 2, pouvait entraîner la responsabilité du détenteur au cas où il n'aurait pas fait preuve de la diligence voulue. L'alinéa b) était important à cet égard, car il offrait un moyen permettant au détenteur de la clef d'atténuer les effets d'un manque de diligence en notifiant que la clef était compromise. S'agissant de la responsabilité, on a également fait observer qu'il pourrait être important d'examiner le fondement de toute relation entre les parties, de nature contractuelle ou non, et le contenu du contrat. De l'avis général, il fallait formuler une règle fondée sur la faute.

81. On s'est demandé si le Groupe de travail voudrait peut-être envisager d'aborder les effets juridiques du manque de diligence. Selon un avis, dans la mesure où il s'était avéré très difficile dans le passé de parvenir à un consensus sur cette question, celle-ci ne devrait pas être examinée dans le présent contexte. Selon un autre avis, le document WP.79 traitait des effets de façon plus détaillée et pourrait fournir un point de départ utile pour examiner ces questions plus à fond. Selon un autre avis encore, la responsabilité ne devrait pas être traitée de façon approfondie en dehors du cadre du paragraphe 2 qui n'avait pas encore été examiné.

82. S'agissant de la forme, on a estimé que les mots "et pourrait être utilisée pour créer des signatures électroniques renforcées non autorisées" n'étaient pas nécessaires, car il apparaissait clairement à quelles fins le dispositif de signature pouvait être utilisé, et il n'était pas besoin de le préciser.

83. Le Groupe de travail a convenu qu'un nouveau projet d'alinéa b) devrait tenir compte des modifications examinées: il faudrait avertir "sans retard excessif"; les deux notions "savait ou aurait dû savoir" et "est ou pourrait avoir été compromise" devraient figurer entre crochets comme variantes; et les mots "et pourrait être utilisée pour créer des signatures électroniques renforcées non autorisées" devraient être supprimés.

Alinéa c)

84. Il a été proposé de supprimer les mots "aux certificateurs d'informations et aux parties se fiant à la signature", car si les déclarations faites à ces parties étaient probablement celles qui devaient être visées, il était concevable que des déclarations puissent être faites à d'autres parties compétentes. Cet article devrait être centré sur l'obligation

de donner des informations exactes et complètes, indépendamment de leur destinataire. En réponse à cette observation, on a indiqué que le fait de supprimer les mots renvoyant aux certificateurs d'informations et aux parties se fiant à la signature pourrait donner à entendre que l'obligation était illimitée, alors qu'il faudrait en fait mettre l'accent sur les déclarations se rapportant au processus d'identification. Il a été proposé d'ajouter après le mot "déclarations" les mots "qui sont pertinentes pour la délivrance du certificat".

85. S'agissant du critère d'objectivité, il fallait, selon une autre proposition, ajouter après le mot "déclarations" les mots "qui sont pertinentes dans le processus de délivrance d'un certificat ou qui figurent dans le certificat". On a fait observer qu'un tel critère limitait l'alinéa c) aux déclarations faites par le détenteur de la clef ou par la personne qui demandait un certificat et qu'il ne serait pas pertinent dans les cas où le détenteur d'une clef ne ferait pas une demande de certificat. Toutefois, l'objectif n'était pas que ces mots soient interprétés dans un sens qui ferait que la personne qui demande un certificat serait tenue responsable de déclarations qui pourraient avoir été formulées de façon incorrecte dans le certificat ou qui, d'une autre manière, ne reposeraient pas sur les informations fournies par ladite personne. Dans ce cas, le certificateur d'informations aurait une obligation correspondante en vertu du projet d'article H en ce qui concerne la teneur du certificat. Si l'on retenait une interprétation étroite de cette obligation, le détenteur d'une clef serait toutefois responsable envers une partie se fiant à la signature lorsque celle-ci aurait subi des pertes ou un préjudice du fait d'informations fallacieuses ou fausses fournies par le détenteur de la clef et figurant dans le certificat. À l'encontre de la proposition tendant à limiter cet alinéa au processus de certification, on a fait valoir que l'obligation énoncée à l'alinéa c) devrait avoir un caractère général et inclure la fourniture d'informations en vertu de l'alinéa b).

86. Selon une autre proposition concernant la portée de l'alinéa c), il fallait diviser cet alinéa en deux parties. Les déclarations faites à une partie se fiant à la signature pourraient relever de l'obligation générale de faire des déclarations exactes et complètes, tandis que les déclarations faites à un certificateur d'informations pour obtenir un certificat pourraient faire l'objet d'un alinéa distinct. Dans le cas des informations fournies au certificateur d'informations, on a mis en lumière la relation existant entre l'obligation énoncée dans ce projet d'article et celle énoncée dans le projet d'article H 1) b) (qui imposait une obligation concernant les informations à certifier).

87. Quelques craintes ont été exprimées au sujet des personnes auxquelles les obligations énoncées au paragraphe 1 devraient s'appliquer. On a fait observer qu'il ne serait peut-être pas judicieux de considérer qu e l'ensemble de l'article F établissait des obligations pour la même personne, alors que les alinéas du présent projet renvoyaient à différents concepts. Par exemple, l'alinéa a) renvoyait à la fois aux informations et au dispositif sur lequel ces informations étaient stockées et à la manière dont il en était fait usage. Il se pourrait que l'obligation s'applique à une catégorie plus large de personnes que le seul détenteur de la clef. En revanche, l'alinéa c) renvoyait aux informations sous forme de déclarations faites à certaines personnes en vue d'obtenir un certificat. Il serait peut-être nécessaire de traiter ces différences séparément dans une version révisée des obligations énoncées au paragraphe l du projet d'article F.

88. S'agissant de la bonne foi du détenteur de la clef au moment où il fait les déclarations, on a indiqué qu'un tel critère était inutilement subjectif et faible et pourrait entraîner, par exemple, un moindre niveau de responsabilité lorsque le détenteur était imprudent ou stupide. Ce qu'il fallait, c'était un libellé objectif précisant bien qu'il ne s'agissait pas d'une conséquence voulue de cet alinéa. D'après une proposition, il fallait remplacer les mots "de bonne foi" par une référence à la diligence; ainsi, l'alinéa pourrait commencer comme suit: "De faire preuve de la diligence voulue en veillant à ce que...". En ce qui concernait les mots "exactes et complètes", il était superflu, selon un avis, de parler de déclarations "complètes" car, dans certaines juridictions, la notion de "complétude" était déjà incluse dans la notion d'"exactitude". Le Groupe de travail a pris note de cette observation.

89. S'agissant de la terminologie, le Groupe de travail a de nouveau examiné le sens d'un certain nombre d'expressions, notamment: détenteur de la signature, détenteur du dispositif, détenteur de la clef et dispositif de signature, dispositif de création de signature, dispositif de vérification de signature (voir par. 40 à 47 ci-dessus). Il

a été proposé que l'expression "détenteur de la clef" désigne la personne par qui, ou au nom de qui, la signature était apposée au message de données, en adoptant le libellé de l'alinéa c) de l'article A du document WP.80, définition qui reconnaissait le concept de représentation. S'agissant du dispositif ou de la signature utilisé, le Groupe de travail a généralement convenu que ce n'était pas le dispositif qui était utilisé pour créer la clef qui était examiné, mais plutôt le dispositif qui était utilisé pour créer la signature.

90. Le Groupe de travail a envisagé s'il était souhaitable de prendre en compte la représentation dans le concept du détenteur de la clef (voir ci-dessus par. 43). De l'avis général, la représentation ne devrait pas être abordée dans les Règles uniformes car il serait difficile de parvenir à un accord sur les principes de la représentation et la prise en compte de ce concept rendrait trop large le champ d'application du projet d'article F. Au cas où la question de la représentation interviendrait, par exemple lorsqu'un employé utiliserait un dispositif de signature pour une société, cet article aurait pour effet, sans préjudice du droit des sociétés, que la signature de l'employé serait considérée comme celle de la société, qui était effectivement le "détenteur de la clef". Le Groupe de travail a réaffirmé la décision qu'il avait prise précédemment et selon laquelle les questions de représentation devraient être réglées en vertu de la loi applicable.

91. Sur le plan de la forme, on a estimé que le mot "*material*" (dans la version anglaise) n'était pas approprié dans certaines juridictions et qu'il ne faudrait donc pas l'utiliser. Toujours sur le plan rédactionnel, on a estimé que, dans la mesure où l'obligation énoncée à l'alinéa c) précédait l'obligation énoncée à l'alinéa a) dans le temps, l'ordre de ces deux alinéas devrait être inversé.

92. Après un échange de vues, le Groupe de travail a convenu que le champ d'application de l'alinéa c) devrait être limité aux obligations du détenteur de la clef dans le cadre du processus de certification; que le détenteur de la clef devrait veiller à ce que les déclarations soient exactes et complètes; que la mention "de bonne foi" devrait être remplacée au début de l'alinéa par les mots "de faire preuve de la diligence voulue en veillant"; que les mots "qui sont pertinentes dans le processus de délivrance d'un certificat ou qui figurent dans le certificat" devraient être ajoutés pour qualifier les "déclarations", étant entendu qu'il devrait être bien clair que le détenteur de la clef serait uniquement responsable de ces déclarations lorsqu'elles ont été convenablement consignées dans le certificat et non des fautes ou inexactitudes introduites par le certificateur d'informations; que la référence "aux certificateurs d'informations et aux parties se fiant à la signature" devrait être supprimée; que l'ordre des alinéa a) et c) devrait être inversé; que la notion de représentation ne devrait pas être abordée dans cet article.

Paragraphe 2

93. La proposition visant à conserver le projet de paragraphe 2 dans sa version actuelle, sans amendement, a reçu un certain appui. L'avis a été exprimé, cependant, que les Règles uniformes devraient se référer aux conséquences juridiques de l'inexécution des obligations énoncées dans le projet de paragraphe 1. L'un des moyens d'aborder ces conséquences consistait à inclure une référence spécifique à la loi nationale ou applicable, une seconde solution étant de promouvoir une harmonisation en examinant les conséquences possibles et en rédigeant une règle uniforme qui aborderait la question des dommages-intérêts, mais ne lierait pas le détenteur de la clef aux conséquences de l'utilisation du dispositif de signature, des questions d'autorisation et d'intention, en particulier, pouvant alors se poser. Selon un autre avis, toutefois, le message de données devrait être attribué au détenteur de la clef (voir ci-dessous par. 97 et 104). Afin d'axer le paragraphe 2 sur les dommages-intérêts plutôt que sur les conséquences, il a été proposé d'adopter les mots "Le détenteur de la clef est responsable du préjudice et des blessures résultant de l'inexécution des obligations énoncées au paragraphe 1". Comme autre moyen d'aborder les conséquences juridiques de l'inexécution des obligations énoncées dans le projet de paragraphe 1, il a été proposé d'envisager le projet d'article 7 du document WP.79 ou, peut-être, un article s'inspirant de l'article 74 de la Convention des Nations Unies sur les contrats de vente internationale de marchandises. Afin d'examiner cette proposition plus avant, il a été proposé le libellé suivant, qui s'inspire de l'article 74:

"La responsabilité du détenteur de la clef ne peut être supérieure à la perte que le détenteur de la clef prévoyait ou aurait dû prévoir au moment de son inexécution à la lumière des faits ou problèmes dont le détenteur de la clef avait connaissance ou aurait dû avoir connaissance, comme étant des conséquences possibles de l'inexécution par le détenteur de la clef des obligations énoncées au paragraphe 1".

94. En réponse à cette proposition inspirée de l'article 74 de la Convention des Nations Unies sur les contrats de vente, il a été exprimé la crainte que la responsabilité qui pourrait naître dans le contexte d'un contrat de vente de marchandises ne soit pas la même que la responsabilité qui pourrait découler de l'utilisation d'une signature et ne pourrait pas être quantifiée de la même façon. Alors qu'il pourrait être possible de prévoir le préjudice découlant de la contravention à un contrat de vente de marchandises, le même critère ne pourrait pas s'appliquer en cas d'utilisation d'une technique particulière de signature. Dans ce contexte, on a indiqué que, conformément aux Règles uniformes, l'utilisation d'une certaine technique de signature ne devrait pas conduire à une limitation de responsabilité particulière (ou à tout autre avantage compétitif par rapport aux utilisateurs de signatures manuscrites traditionnelles), établie au profit des utilisateurs des techniques électroniques. Selon un autre avis, le critère de prévisibilité du préjudice était une norme internationalement reconnue qui pourrait se révéler utile dans le contexte des signatures et faciliter la rédaction d'une règle uniforme. Selon un autre avis, dans l'éventualité où l'on envisagerait un article sur les dommages-intérêts, il pourrait être nécessaire d'opérer une distinction entre un préjudice découlant d'une action du détenteur de la clef qui n'aurait pas respecté la norme énoncée au projet de paragraphe 1 et un préjudice découlant du fait que le détenteur de la clef n'aurait pas agi, c'est-à-dire entre un préjudice direct et un préjudice indirect.

95. Il a été proposé d'analyser les obligations du détenteur de la clef énoncées à l'article F se référant aux parties ou classes de parties envers lesquelles l'obligation était contractée, au certificateur d'informations, d'une part, et à un groupe de parties potentielles se fiant à la signature, d'autre part. Il était évident que la relation entre le détenteur de la clef et le certificateur d'informations serait une relation contractuelle qui serait régie par la loi applicable. Des doutes ont été exprimés quant au fait de savoir si l'on pouvait appliquer une règle sur le caractère prévisible ou indirect du préjudice à une telle relation contractuelle. S'agissant du groupe de parties se fiant à la signature, il a été estimé qu'il pourrait être approprié d'établir une règle qui déterminerait quelles parties se fiant à la signature pourraient, de façon prévisible, subir un préjudice et le type de préjudice pour lequel le détenteur de la clef serait responsable. Des doutes ont été exprimés quant à savoir si l'article 74 de la Convention des Nations Unies sur les contrats de vente englobait ces deux concepts et si, de toute façon, il serait souhaitable d'avoir une règle unique concernant la prévisibilité couvrant les obligations énoncées aux alinéas a) à c) du projet de paragraphe 1. Il a également été souligné que le projet d'article G traitait de questions liées à la partie se fiant à la signature et qu'il devrait être pris en compte dans tout article traitant des conséquences de l'inexécution, par le détenteur de la clef, des obligations énoncées dans le projet d'article F.

96. Pour préciser le champ d'application du projet de paragraphe 2, il a été proposé de supprimer la référence aux "conséquences de l'inexécution des obligations énoncées au paragraphe 1", afin d'éviter toute incertitude quant à ce que l'inclusion de ces mots pourrait signifier et pour éviter d'avoir à examiner si l'obligation non respectée était contractuelle. Il a également été souligné que l'expression "les conséquences" pourrait suggérer que toutes les conséquences possibles étaient envisagées et ne tenait aucun compte du caractère indirect de ces conséquences possibles. La proposition visant à supprimer cette expression a bénéficié d'un large appui.

97. On a également craint que si l'on lisait ensemble les projets d'articles F et G, il pourrait s'ensuivre un effet juridique autre que la responsabilité, à savoir l'attribution. Il a été estimé que pour lever toute incertitude, il était nécessaire de disposer au moins d'une règle ou d'une présomption réfutable concernant l'attribution de la signature. Si, selon certains avis, un tel article pourrait être utile et renforcerait la confiance placée dans le commerce électronique, il a été souligné que des difficultés ne manqueraient pas de survenir dans le contexte de l'article 13 de la Loi type, qui traitait de l'attribution d'un message de données. De l'avis général, l'attribution ne devrait pas être examinée dans le contexte du projet d'article F (voir ci-dessous par. 104).

98. Après un débat, le Groupe de travail a convenu, étant donné l'appui reçu par la proposition tendant à conserver le paragraphe 2 sous sa forme actuelle avec les amendements proposés et à envisager une règle sur les conséquences s'inspirant éventuellement de l'article 74 de la Convention des Nations Unies sur les contrats de vente internationale de marchandises, d'inclure un projet révisé de paragraphe 2 traitant des deux possibilités dans les futurs documents de travail en vue de leur examen par le Groupe de travail. Cette disposition devrait se limiter, dans son application, aux obligations à inclure dans une version révisée du paragraphe 1 du projet d'article F.

Article G. Foi accordée à une signature électronique renforcée

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

> "Une personne est fondée à se fier à une signature électronique renforcée à condition de prendre des mesures raisonnables pour déterminer si ladite signature est valable et n'a pas été compromise ou annulée".

100. On a exprimé la crainte que la forme de l'article ne soit inappropriée. En effet, il ne s'agissait pas de savoir si la partie se fiant à la signature était fondée à le faire mais de savoir ce que toute personne cherchant à se fier à la signature devrait faire pour que la foi qu'elle y accordait soit jugée raisonnable. À cet égard, il serait important d'indiquer les cas dans lesquels il ne serait pas raisonnable de se fier à la signature. Pour tenir compte de ce déplacement d'accent, le libellé suivant a été proposé:

> "1. Une personne n'est pas fondée à se fier à un certificat ou à une signature étayée par un certificat s'il n'est pas raisonnable de le faire.
>
> 2. Pour déterminer s'il est raisonnable de se fier à un certificat ou à une signature, il est tenu compte des facteurs suivants:
>
> a) toutes restrictions dont le certificat peut faire l'objet;
>
> b) nature de l'opération sous-jacente que le certificat ou la signature est censé étayer;
>
> c) adoption ou non par la partie se fiant au certificat ou à la signature de mesures appropriées pour déterminer la fiabilité de la signature ou du certificat;
>
> d) toute convention ou tout usage commercial ou toute pratique existant entre la partie se fiant au certificat ou à la signature et le certificateur d'informations ou l'abonné".

101. Cette proposition a bénéficié d'un appui. Pour préciser ce que l'on entendait par "opération sous-jacente" à l'alinéa b), on a indiqué qu'il pourrait ne pas être suffisant de se fier uniquement à l'utilisation d'une technique d'identification et qu'une quelconque autre forme d'identification ou de vérification pourrait être nécessaire. Ainsi, une banque pourrait souhaiter obtenir confirmation du fait qu'une opération d'un de ses clients, pouvant être jugée inhabituelle, était bien attribuable audit client, même après utilisation d'une technique d'identification appropriée. On a exprimé la crainte que les facteurs énoncés aux alinéas a) à d) soient trop généraux et, compte tenu du fait que le Groupe de travail partait du principe que les Règles uniformes traitaient des questions relatives à l'infrastructure à clef publique, il pourrait être utile de préciser qu'il était nécessaire de vérifier la validité ou la fiabilité du certificat. À cette fin, il a été proposé d'ajouter à l'alinéa c) les mots "y compris la consultation d'une liste d'annulations de certificats, le cas échéant".

102. Il a été proposé d'ajouter aux facteurs énoncés aux alinéas a) à d) de la proposition un point sur la question de savoir si la partie se fiant à la signature savait ou aurait dû savoir que la clef avait été compromise ou annulée ou, selon une autre formulation, qu'il n'était pas raisonnable de se fier à la signature ou au certificat. Pour donner plus

de souplesse au texte proposé, il a été suggéré par ailleurs d'ajouter au paragraphe 2 les mots "s'il y a lieu" après les mots "il est tenu compte". Ces deux propositions ont bénéficié d'un certain appui.

103. La proposition tendant à conserver le projet d'article G sous sa forme actuelle ou à le supprimer complètement a aussi été appuyée. On a fait observer que si l'on suivait dans un article la structure du texte proposé on donnerait l'impression de soumettre la foi accordée aux signatures renforcées à certaines exigences ou conditions. Replacées dans le contexte de l'article 13 de la Loi type, ces exigences pourraient engendrer une situation dans laquelle il serait plus facile de se fier à une signature électronique relativement peu sûre qu'à une signature renforcée plus sûre. La forme de signature la plus sûre risquerait alors d'être aussi plus difficile à utiliser. Selon un autre avis, il faudrait établir un lien quelconque entre la foi accordée à la signature et l'article 13 de la Loi type, en particulier ses paragraphes 3 et 4. Selon un autre avis encore, la formulation actuelle du projet d'article G reflétait une attitude plus positive pour ce qui était de savoir si les parties se fiant à ce type de signature étaient fondés à le faire. Néanmoins, on a estimé qu'une partie se fiant à la signature devrait peut-être prendre certaines précautions et une autre proposition a été formulée, à savoir:

> "Une personne est fondée à se fier à une signature électronique renforcée à condition de prendre des mesures raisonnables pour vérifier la validité de la signature conformément aux normes convenues avec le détenteur de la clef ou pour vérifier l'information fournie par le certificateur d'informations."

Cette proposition n'a pas été appuyée.

104. On a exprimé la crainte que le Groupe de travail soit en train d'essayer d'intégrer dans le projet d'article G des effets juridiques inclus dans les projets d'articles B et C, mais qui, avait-il été décidé, ne devaient pas être examinés au stade actuel. En indiquant dans le projet d'article G qu'une personne était fondée à se fier à une signature, on risquait de présumer de certains effets juridiques, alors qu'en définissant ce qu'il fallait faire pour pouvoir se fier à une signature, on évitait de traiter des effets juridiques que pourrait avoir la signature. Puisque les projets d'articles F, G et H étaient axés sur les règles de conduite à suivre par les parties dans une infrastructure à clef publique, il ne convenait pas d'y inclure des effets juridiques. Quant à la question de l'attribution soulevée par l'article 13 de la Loi type (voir ci-dessus par. 97), on a fait observer que si le champ d'application de cet article était limité de manière générale aux cas où existait une relation contractuelle entre l'expéditeur et le destinataire du message de données, les Règles uniformes, par contre, étaient censées avoir un champ d'application plus large. On a aussi fait observer que le fait d'énoncer dans le projet d'article G une série de mesures à prendre en considération pour déterminer s'il était raisonnable de se fier à un certificat ou à une signature n'était pas incompatible avec l'exigence de "dispositions raisonnables"énoncée à l'article 13 et n'établissait pas d'effet juridique quant à la validité de la signature. Sur ce dernier point, il a été noté que le projet d'article F, tel que révisé par le Groupe de travail, ne traitait pas non plus des effets juridiques ou de la validité de la signature et la forme de ces deux projets d'articles était donc cohérente.

105. Selon un avis contraire, le fait d'indiquer dans le projet d'article G qu'une personne était fondée à se fier à une signature ajoutait un avantage qui n'existait pas en vertu de la Loi type, que l'effet juridique spécifique soit énoncé ou non dans d'autres articles. Il a été proposé de combiner l'approche susmentionnée avec l'énonciation des mesures à envisager pour déterminer s'il était raisonnable de se fier à une signature, de la façon suivante: "1. Une personne est fondée à se fier à un certificat ou à une signature étayée par un certificat dans la mesure où il est raisonnable de le faire". Un deuxième paragraphe énoncerait ensuite les points à prendre en considération, comme proposé précédemment, en ajoutant une catégorie supplémentaire comprenant "tous les autres facteurs pertinents".

106. S'agissant de la forme, il a été noté que les mots "foi" et "renforcée" n'étaient pas courants dans certaines langues ou dans certains systèmes juridiques et qu'il serait peut-être nécessaire de chercher des termes plus appropriés.

107. Après un débat, le Groupe de travail est convenu de ce qui suit: les deux formulations du projet d'article G (voir ci-dessus par. 100 et 105) devraient être regroupées dans un article G révisé, en vue d'un examen ultérieur; il faudrait également inclure la référence à "tous les autres facteurs pertinents" et la proposition concernant le fait que la partie se fiant à la signature savait ou aurait dû savoir que la clef avait été compromise ou annulée ou, selon une autre formulation, qu'il n'était pas raisonnable de se fier à la signature ou au certificat; enfin les mots "s'il y a lieu" devraient être ajoutés au paragraphe 2.

Article H. Obligations d'un certificateur d'informations

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

"1. Un certificateur d'informations a l'obligation:

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

b) de prendre des mesures raisonnables pour déterminer avec exactitude l'identité du détenteur de la signature et tous autres faits ou informations qu'il certifie;

c) de fournir des moyens raisonnablement accessibles qui permettent à une partie se fiant à la signature de s'assurer:

i) de l'identité du certificateur d'informations;

ii) de la méthode employée pour identifier le détenteur de la signature;

iii) de toutes restrictions quant aux fins pour lesquelles la signature peut être utilisée; et

iv) du fait que la signature est valable et n'a pas été compromise;

d) de fournir un moyen permettant au détenteur de la signature d'avertir qu'une signature électronique renforcée a été compromise;

e) de veiller, de bonne foi, à ce que toutes les déclarations qu'il fait sont exactes et complètes;

f) d'utiliser des systèmes et des procédures fiables pour la fourniture de ses services.

2. Un certificateur d'informations est responsable des conséquences de l'inexécution des obligations énoncées au paragraphe 1."

Remarques générales

109. Selon un avis, l'expression d'opinions concernant les obligations et la responsabilité d'une autorité de certification était largement conditionnée par la définition d'une autorité de certification. Une décision devrait être prise, en particulier, quant au fait de savoir si les fonctions d'une autorité de certification pouvaient être assurées par une personne ou par une entité qui était déjà partie à la transaction sous-jacente aux fins de laquelle un certificat pourrait être utilisé (hypothèse de travail adoptée actuellement par le Groupe de travail), ou si l'autorité de certification devrait, dans tous les cas, être indépendante des parties (situation apparentée à celle d'un notaire public dans plusieurs pays de droit civil). Après un débat, le Groupe de travail a décidé de poursuivre son examen de la question sur la base de l'hypothèse de travail adoptée lors de la présente session (voir ci-dessus par. 68). Si le Groupe de travail n'a pas examiné la définition de "l'autorité de certification" à proprement parler, il a été

généralement convenu que les mots “dans le cours de ses affaires” figurant dans la définition du terme “certificateur d’information” au projet d’article A ne devraient pas être interprétés comme signifiant que les activités liées à la certification devraient être les activités professionnelles exclusives d’une autorité de certification. Selon un avis, il pourrait être nécessaire d’établir une différence entre une entité qui ne délivrait des certificats qu’accessoirement dans le cadre de ses activités et une entité qui faisait profession de délivrer des certificats (soit exclusivement, soit en association avec d’autres activités qu’elle pouvait exercer). Selon un autre avis, étant donné le rôle important dévolu aux autorités de certification et les responsabilités qui pourraient en découler pour elles-mêmes et pour les parties se fiant à la signature, les Règles uniformes devraient préciser le statut des autorités de certification. Après un échange de vues, il a été convenu que les questions de la définition, du rôle et du statut des autorités de certification devraient être examinées de façon plus approfondie lors d’une future session.

Paragraphe 1

110. La discussion a porté sur le fait de savoir si la liste des obligations énoncées au paragraphe 1, indépendamment de ce que pouvaient être ces obligations, devrait être exhaustive ou non. L’avis selon lequel le paragraphe 1 devrait être libellé sous la forme d’une liste ouverte et illustrative d’obligations a reçu un appui marqué. Il a été proposé d’utiliser, en guise d’introduction au paragraphe 1, une formule du type: “Sans que cela limite le caractère général du devoir de diligence qui incombe à l’autorité de certification, une autorité de certification a, notamment, l’obligation...”. Il a été déclaré que, bien que cette formulation puisse sembler contraignante pour l’autorité de certification, elle serait en fait cohérente avec la règle générale qui s’appliquerait actuellement aux autorités de certification dans de nombreux systèmes juridiques. Il a également été déclaré qu’une déclaration générale concernant les obligations de l’autorité de certification, au paragraphe 1, pourrait être compensée par des exonérations de responsabilité qui seraient précisées au paragraphe 2 ou dans le projet d’article E. À cet égard, il a été proposé que le Groupe de travail concentre son attention sur la façon dont des clauses contractuelles exonérant la responsabilité de l’autorité de certification pourraient être étendues au-delà de la sphère contractuelle. En réponse, il a été déclaré que, même dans le cadre de la sphère contractuelle, des restrictions devraient être apportées à l’aptitude des autorités de certification à limiter leur responsabilité, par exemple dans le cas où une telle limitation serait manifestement injuste. Le Groupe de travail a convenu que la question des limites contractuelles et autres fixées pour la responsabilité de l’autorité de certification devrait être examinée de façon plus approfondie lors d’une future session.

111. Selon un autre avis, le paragraphe 1 devrait être libellé sous la forme d’une liste exhaustive d’obligations. Il a été déclaré qu’en vertu de la législation de certains pays, l’autorité de certification n’était pas nécessairement tenue d’agir avec diligence. Les diverses obligations de l’autorité de certification devraient donc être énoncées de façon détaillée afin de déterminer la portée exacte de sa responsabilité. Une autre justification à l’appui de cette opinion était que les Règles uniformes devraient traiter uniquement de l’exécution des fonctions des autorités de certification et ne devraient pas exposer de nouveau les principes généraux de la législation sur les délits civils qui pourrait être applicable à toute personne s’engageant dans n’importe quel type d’activité. Selon cet avis, dans la mesure où la “fonction de l’autorité de certification” était un concept vérifiable, les Règles uniformes devraient seulement porter sur les activités relevant de cette fonction et ne devraient pas avoir un caractère général. Il a été convenu que les deux avis devraient être pris en compte dans le texte révisé qui serait établi en vue de la poursuite du débat à une future session.

112. S’agissant de la substance des obligations précises énoncées aux alinéas a) à f), elle a bénéficié d’un appui général. Diverses propositions ont été faites quant à la façon dont l’expression de ces obligations pourrait être améliorée. Selon un avis, l’obligation faite à l’alinéa b) de déterminer l’identité du détenteur de la signature était peut-être superflue, car elle ne faisait qu’illustrer l’obligation plus générale de veiller, aux termes de l’alinéa e), à ce que les déclarations soient exactes. De l’avis général, cependant, il a été estimé que l’alinéa b) était utile, car il clarifiait la situation. Il a par ailleurs été proposé que l’alinéa b) contienne une obligation supplémentaire tendant à préciser, dans le certificat, l’identité du détenteur de la clef.

113. Il a par ailleurs été proposé que, dans le cadre de ses obligations de base, l'autorité de certification soit dans l'obligation de tenir une liste d'annulation de certificats. Il a été proposé d'ajouter à l'alinéa d) les mots suivants: "et d'assurer un service prompt et immédiat d'annulation". Cette proposition a bénéficié d'un certain appui. Il a cependant été souligné que l'obligation de tenir une liste d'annulation de certificats pourrait se justifier pour des transactions et des certificats de valeur élevée (c'est-à-dire pour les "signatures électroniques renforcées" destinées à produire un effet juridique), mais serait très contraignante (et contraire à la pratique existante) si elle devait être imposée à tous les certificats (y compris les "certificats bon marché" utilisés dans le contexte d'un grand nombre de signatures numériques). À cet égard, il a été rappelé que l'une des principales difficultés rencontrées par le projet actuel consistait à établir un critère viable permettant d'opérer une distinction entre les transactions de niveau supérieur (pour lesquelles on recherchait un haut niveau de sécurité en appliquant des critères rigoureux aux certificats et aux autorités de certification, éventuellement en vue de produire certains effets juridiques prédéterminés) et le grand nombre d'utilisations ordinaires de signatures numériques et de certificats (pour lesquels la production d'effets juridiques quant à la "signature" se justifiait rarement, et pour lesquels la politique généralement appliquée consistait à ne pas interférer avec l'autonomie des parties). Il a été exprimé l'avis que, s'il était possible que l'on ne trouve pas de critère viable de ce type, une limitation de la portée des Règles uniformes à la sphère commerciale (c'est-à-dire excluant les transactions des consommateurs) pourrait offrir une solution acceptable.

114. D'autres propositions ont été faites pour tenir compte d'éléments supplémentaires dans la liste des obligations figurant au paragraphe 1: l'obligation de fournir des informations sur l'annulation et la suspension des certificats; à l'alinéa e), un texte reflétant une disposition analogue figurant dans le projet d'article F; et, à l'alinéa f), un texte exprimant l'obligation, pour l'autorité de certification, d'utiliser, pour assurer ses services, des ressources humaines fiables. Il a été proposé d'insérer, à l'alinéa c) du paragraphe 1, le texte suivant: "du fait que la personne qui est nommée dans le certificat détient [détenait au moment pertinent] la clef privée correspondant à la clef publique"; et "que les clefs soient une paire de clefs qui fonctionne".

Paragraphe 2

115. S'agissant de la disposition générale concernant la responsabilité de l'autorité de certification en cas d'inexécution des obligations énoncées au paragraphe 1, il a été largement admis qu'il conviendrait de créer une règle uniforme et ne pas se contenter de renvoyer à la loi applicable. En ce qui concerne la teneur d'une telle règle, on a estimé qu'elle devrait établir une responsabilité générale pour négligence, sous réserve d'exonération contractuelle, le cas échéant, et sous réserve également que l'autorité de certification s'exonère elle-même de la responsabilité en démontrant qu'elle s'est acquittée des obligations prévues en vertu du paragraphe 1. Le texte ci-après a été proposé pour remplacer le paragraphe 2:

"2. Sous réserve du paragraphe 3, une autorité de certification est tenue responsable d'un préjudice subi:

a) soit par une partie qui a passé un contrat avec l'autorité de certification pour la délivrance d'un certificat;

b) soit par une personne qui se fie à un certificat délivré par l'autorité de certification, si le préjudice a été causé parce que le certificat était incorrect ou défectueux.

3. Une autorité de certification n'est pas tenue responsable en vertu du paragraphe 2:

a) si, et dans la mesure où elle a inclus dans les informations consignées dans le certificat une déclaration limitant la portée ou l'étendue de sa responsabilité envers toute personne; ou

b) si elle prouve qu'elle [n'a pas été négligente] [a pris toutes les mesures raisonnables pour prévenir ce préjudice]".

116. Si un certain soutien a été exprimé en faveur de cette proposition, de vives objections ont été formulées au motif que le fait d'adopter le libellé proposé correspondrait à établir une norme stricte de responsabilité pour "tout préjudice" et qu'en imposant une stricte norme de responsabilité aux autorités de certification, on risquerait d'entraver sérieusement le développement de l'utilisation du commerce électronique. S'agissant du texte proposé pour l'alinéa a) du paragraphe 3, des doutes ont été émis quant au point de savoir si les informations figurant dans le certificat en vue de limiter la responsabilité de l'autorité de certification à l'égard de ce certificat pourraient s'appliquer également à la responsabilité contractuelle et extracontractuelle. Dans ce contexte, le Groupe de travail a été instamment prié de ne pas chercher à établir de distinction pertinente dans les Règles uniformes en se fondant sur les notions de responsabilité contractuelle et extracontractuelle, ces notions pouvant être très différentes selon les pays. En outre, selon un avis, la clause limitant la responsabilité de l'autorité de certification ne devrait pas être invoquée au cas et dans la mesure où l'exclusion ou la limitation de responsabilité serait manifestement injuste. Cet avis a été appuyé par certaines délégations.

117. Un appui a également été exprimé en faveur du maintien de la présente structure du paragraphe 2, compte tenu d'une liste exhaustive d'obligations au paragraphe 1.

118. S'agissant du débat auquel ont donné lieu les obligations de l'autorité de certification, il a été demandé qui assumerait le risque d'une perte découlant de la confiance accordée à un certificat sujet à caution (par exemple compromis ou annulé) lorsque toutes les parties ont fait preuve de diligence conformément aux articles F, G et H des Règles uniformes. Selon un avis, compte tenu de la formulation négative proposée pour le projet d'article G, la partie se fiant au certificat supporterait ce risque subsidiaire. On a fait observer que, dans la pratique, la confiance accordée aux moyens de communication tels que le téléphone ou la télécopie imposait déjà ce risque subsidiaire à la partie se fiant à ces moyens de communication. Selon une autre proposition, des dispositions devraient être adoptées dans le projet d'article H pour faire en sorte que le risque subsidiaire soit supporté par l'autorité de certification. Selon une autre proposition encore, les Règles uniformes ne devraient pas se prononcer sur ce point mais laisser aux tribunaux le soin de déterminer quelle partie devrait supporter le risque, au vu de toutes les circonstances pertinentes.

119. Après un échange de vues, le Groupe de travail n'a pas pris de décision finale sur la teneur du projet d'article H. Le Secrétariat a été prié de préparer des variantes tenant compte des diverses opinions exprimées, afin que le débat puisse se poursuivre lors d'une session ultérieure.

C. AUTRES QUESTIONS À EXAMINER

120. Le Groupe de travail a dressé la liste des questions qui, en raison du manque de temps, n'avaient pu être examinées à cette session mais qui devraient l'être ultérieurement à l'occasion d'ajouts éventuels aux Règles uniformes. On a fait valoir que, dans le cadre de ses futurs débats sur les Règles uniformes, le Groupe de travail voudrait peut-être envisager de prévoir un article pour faire en sorte que les certificats ne fassent pas l'objet d'un préjudice en fonction du lieu où ils étaient émis. Le texte ci-après a été proposé: "En déterminant si, ou dans quelle mesure, un certificat produit légalement ses effets, il n'est pas tenu compte du lieu où le certificat a été émis, ni de l'État dans lequel l'émetteur a son adresse professionnelle". Le Groupe de travail a pris note de cette proposition.

121. Les autres questions devant faire l'objet d'un examen ultérieur étaient notamment les suivantes: reconnaissance internationale des certificats; effet juridique des signatures électroniques; attribution des signatures électroniques; relation entre les Règles uniformes et la Loi type; définition et qualités minimales des autorités de

certification; incompatibilité éventuelle entre les fonctions des autorités de certification et l'exécution de toute autre fonction dans le cadre de la même transaction; et annulation et suspension des certificats.

122. Il a été noté que la prochaine session du Groupe de travail devrait se tenir à Vienne du 6 au 17 septembre 1999, ces dates devant être confirmées par la Commission à sa trente-deuxième session, prévue à Vienne du 17 mai au 4 juin 1999. Il a été proposé, au nom d'un certain nombre de délégations, que la durée des futures sessions du Groupe de travail soit limitée à une semaine et que cette question soit dûment examinée par la Commission à sa trente-deuxième session. Le Groupe de travail a pris note de cette proposition en faisant observer qu'une telle question ne pourrait être tranchée que par la Commission.

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 207 à 211.