NATIONS
UNIES

A

Assemblée générale

Distr. GÉNÉRALE

A/CN.9/437
12 mars 1997

FRANÇAIS
Original : ANGLAIS

COMMISSION DES NATIONS UNIES
POUR LE DROIT COMMERCIAL INTERNATIONAL
Trentième session
Vienne, 12-30 mai 1997

RAPPORT DU GROUPE DE TRAVAIL SUR LE COMMERCE ÉLECTRONIQUE SUR LES TRAVAUX DE SA TRENTE ET UNIÈME SESSION (New York, 18-28 février 1997)

TABLE DES MATIÈRES

TABLE DES MATIÈRES (suite)

INTRODUCTION

1. Après avoir adopté la Loi type de la CNUDCI sur le commerce électronique, ci-après dénommée la Loi type, la Commission a procédé, à sa vingt-neuvième session (1996), à un débat sur les travaux futurs dans ce domaine, à partir des discussions préliminaires qu'avait eues le Groupe de travail sur les échanges de données informatisées à sa trentième session (A/CN.9/421, par. 109 à 119). D'une manière générale, il a été convenu que la CNUDCI devait continuer à élaborer des normes juridiques susceptibles de rendre l'échange de données électroniques plus prévisibles, ce qui favoriserait les échanges dans toutes les régions.

2. De nouvelles propositions ont été faites quant aux sujets et priorités envisageables aux fins de travaux futurs. Selon l'une d'elles, la Commission devrait commencer à élaborer des règles sur les signatures numériques. Il a été fait observer que dans nombre de pays l'adoption de textes de loi sur les signatures numériques ainsi que de textes reconnaissant les actes d'autorités de certification (ci-après dénommées "tiers authentificateurs") ou d'autres personnes autorisées à émettre des certificats électroniques ou d'autres formes de garantie quant à l'origine et à l'attribution de messages portant une "signature" numérique était considérée comme essentielle au développement du commerce électronique. Il a été souligné que la possibilité d'utiliser des signatures numériques conditionnerait le développement de la pratique contractuelle et la négociabilité des titres représentatifs de marchandises ou autres titres grâce à des moyens électroniques. De nouvelles lois appelées à régir les signatures numériques étaient en cours d'élaboration dans un certain nombre de systèmes de droit. L'entreprise était cependant loin d'être uniforme. Si la Commission décidait d'entreprendre des travaux dans ce domaine, elle serait en mesure d'harmoniser les lois nouvelles ou, du moins, d'arrêter des principes communs dans le domaine de la signature électronique et de fournir ainsi une infrastructure internationale à cette activité commerciale.

3. Cette proposition a recueilli une large adhésion. Toutefois, on s'est accordé à dire que, si elle décidait d'entreprendre des travaux dans le domaine des signatures numériques par l'intermédiaire de son Groupe de travail sur les échanges de données informatisées, la Commission devait donner à celui-ci un mandat précis. On a également estimé que dans la mesure où la CNUDCI ne pouvait pas entreprendre de définir des normes techniques, elle devait prendre soin de ne pas aborder de questions techniques touchant les signatures numériques. Il a été rappelé qu'à sa trentième session, le Groupe de travail avait estimé qu'il faudrait peut-être se pencher sur la question des tiers authentificateurs et ce, probablement, dans le contexte des registres et des prestataires de services. Il avait toutefois considéré qu'il ne devait pas se lancer dans des considérations techniques concernant le caractère approprié de l'utilisation de telle ou telle norme (A/CN.9/421, par. 111). Certains se sont demandés si les travaux sur les signatures numériques ne risquaient pas de déborder le champ du droit commercial et de mettre en jeu également des questions générales relevant du droit civil ou du droit administratif. D'autres ont rétorqué qu'il en était de même des dispositions de la Loi type et que la Commission ne devait pas répugner à élaborer des règles utiles au motif que celles-ci pourraient également se révéler utiles en dehors de la sphère des relations commerciales.

4. Il a également été proposé, sur la base du débat préliminaire tenu par le Groupe de travail, d'axer les travaux futurs sur les prestataires de services, par exemple sur les questions ci-après : normes minima d'exécution en l'absence d'accord entre les parties; étendue des risques supportés par les destinataires; effet de ces règles ou accords sur les tiers; répartition des risques d'intrusion ou d'actes non autorisés; et étendue des garanties obligatoires, le cas échéant, ou d'autres obligations dans le cas de la fourniture de services à valeur ajoutée (voir A/CN.9/421, par. 116).

5. De l'avis d'un grand nombre de participants, il convenait que la CNUDCI examine la relation entre les prestataires de services, les utilisateurs et les tiers. Il importait d'orienter les travaux sur ce sujet vers la définition de normes internationales de conduite commerciale visant à favoriser le commerce électronique et non de s'assigner pour objectif l'institution d'un régime réglementaire applicable aux prestataires de services ou d'autres règles qui pourraient engendrer des coûts inacceptables pour les applications commerciales de l'échange de données informatisées (EDI) (voir A/CN.9/421, par. 117). On a toutefois jugé que la matière des prestataires de services pourrait se révéler trop vaste et englober un trop grand nombre de cas de figure différents pour être traitée comme un tout. On s'est accordé à penser que les questions concernant les prestataires pouvaient être convenablement traitées dans le contexte de chacun des nouveaux sujets sur lesquels travaillerait le Groupe.

6. Il a en outre été proposé que la Commission entreprenne de définir de nouvelles règles générales qui permettent de préciser la manière dont les prestations conventionnelles classiques pourraient être exécutées grâce au commerce électronique. Le sens d'expressions comme "exécution", "livraison" et d'autres termes dans le contexte du commerce électronique où l'offre et l'acceptation ainsi que la livraison du produit pourraient s'effectuer sur des réseaux d'ordinateurs situés n'importe où de par le monde était entouré de beaucoup d'incertitude. L'expansion rapide du commerce électronique, ainsi que des transactions sur l'Internet et d'autres systèmes conféraient un caractère prioritaire à ce sujet. Il a été proposé que le Secrétariat réalise une étude pour délimiter le champ de ces travaux. Si, après avoir examiné l'étude en question, la Commission décidait d'entreprendre cette tâche, elle pouvait décider, entre autres possibilités, d'insérer ces règles dans la section de la Loi type intitulée "Dispositions spéciales".

7. Il a par ailleurs été proposé que la Commission concentre son attention sur la question de l'incorporation par référence. On a rappelé que le Groupe de travail avait été d'avis qu'il conviendrait de traiter le sujet dans le cadre de travaux plus généraux sur les questions des registres et des prestataires de services (A/CN.9/421, par. 114). Les membres de la Commission se sont accordés à dire que la question pourrait être étudiée à l'occasion des travaux sur les tiers authentificateurs.

8. Après l'avoir débattue, la Commission a jugé qu'il convenait d'inscrire à son ordre du jour la question des signatures numériques et des tiers authentificateurs, à condition d'y voir l'occasion pour elle de traiter d'autres sujets d'études proposés, pour l'avenir, par le Groupe de travail. Il a été également convenu, s'agissant de donner un mandat plus précis au Groupe, que les règles uniformes devaient 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, prestataires 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.

9. La Commission a prié le Secrétariat d'établir un document d'information sur les questions relatives aux signatures numériques et aux prestataires de services en partant de l'analyse des textes de lois en cours d'élaboration dans divers pays. En se fondant sur ce document, le Groupe de travail devrait réfléchir à l'opportunité de définir des règles uniformes concernant les questions susmentionnées. Il a été convenu qu'à l'occasion des travaux de sa trente et unième session, le Groupe de travail pourrait entreprendre d'élaborer des projets de règles touchant certains aspects des questions susmentionnées. La Commission a prié le Groupe de travail de lui fournir des éléments d'information qui lui permettent de se prononcer en toute connaissance de cause sur le champ d'application des règles uniformes devant être élaborées. Étant donné le vaste champ d'activité visé par la Loi type et les travaux qu'il faudrait mener en matière de commerce électronique, il a été décidé de rebaptiser le Groupe de travail sur les échanges de données informatisées "Groupe de travail sur le commerce électronique"[1].

10. Le Groupe de travail sur le commerce électronique, qui était composé de tous les États Membres de la Commission, a tenu sa trente et unième session à New York du 18 au 28 février 1997. Ont assisté à cette session les représentants des États membres du Groupe de travail ci-après : Allemagne, Argentine, Australie, Autriche, Bulgarie, Chine, Égypte, Espagne, États-Unis d'Amérique, Fédération de Russie, Finlande, France, Hongrie, Inde, Iran (République islamique d'), Italie, Japon, Kenya, Mexique, Ouganda, Pologne, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, Singapour, Slovaquie et Thaïlande.

11. Y ont également assisté les observateurs des pays dont les noms suivent : Canada, Colombie, Danemark, Gabon, Indonésie, Irlande, Koweït, Mauritanie, Mongolie, République de Corée, République tchèque, Suède, Suisse et Turquie.

---

[1] Documents officiels de l'Assemblée générale, cinquante et unième session, Supplément n° 17 (A/51/17), par. 216 à 224.

12. Y ont en outre été représentées les organisations internationales ci-après : Conférence des Nations Unies sur le commerce et le développement (CNUCED), Commission européenne, Association internationale du barreau, Chambre de commerce internationale (CCI) et Union internationale des avocats (UIA).

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

Président : M. Mads Bryde ANDERSEN (Danemark);

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

Rapporteur : M. Piotr AUSTEN (Pologne).

14. Le Groupe de travail était saisi de deux documents : l'ordre du jour provisoire (A/CN.9/WG.IV/WP.70) et une note du Secrétariat (A/CN.9/WG.IV/WP.71).

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

1. Élection du bureau.

2. Adoption de l'ordre du jour.

3. Planification des travaux futurs sur les aspects juridiques du commerce électronique : signatures numériques, tiers authentificateurs et questions juridiques connexes.

4. Questions diverses.

5. Adoption du rapport.

I. DÉBATS ET DÉCISIONS

16. Le Groupe de travail a examiné, en se fondant sur la note établie par le Secrétariat (A/CN.9/WG.IV/WP.71), les questions relatives aux signatures numériques et aux tiers authentificateurs et les questions juridiques connexes. Il est rendu compte de ses débats et conclusions sur ces aspects dans la section II ci-dessous. Le Groupe de travail a également tenu des discussions préliminaires sur les questions de l'incorporation par référence et des travaux futurs. Ces discussions sont reflétées ci-dessous dans les sections III et IV.

II. QUESTIONS JURIDIQUES ET DISPOSITIONS ÉVENTUELLES À INSÉRER DANS LES RÈGLES UNIFORMES SUR LES SIGNATURES NUMÉRIQUES

A. Observations générales

17. Avant d'aborder la question des dispositions éventuelles à insérer dans les règles uniformes sur les signatures numériques et autres questions juridiques connexes, le Groupe de travail a procédé à un échange de vues sur la portée de ses travaux et examiné les mesures actuellement prises par les pays pour régler les questions juridiques relatives aux signatures numériques et aux tiers authentificateurs.

18. Ces mesures ont été portées à la connaissance du Groupe de travail. Plusieurs pays examinaient la question du régime juridique à appliquer aux techniques capables de remplir, dans un milieu électronique, des fonctions analogues à celles de la signature manuscrite dans les documents sur papier. Dans certains pays, l'examen de la question n'en était encore qu'au stade préliminaire, mais dans d'autres, des lois sur les signatures numériques avaient déjà été adoptées ou étaient en cours d'élaboration, sur la base de la Loi type. Ces lois prévoyaient souvent l'emploi

de signatures numériques s'appuyant sur la cryptographie à clef publique et les tiers authentificateurs. Il s'agissait soit de lois de caractère général adoptées pour permettre l'emploi de signatures numériques en vue d'authentifier les messages électroniques, soit de lois plus détaillées, qui mettaient en place le cadre juridique requis pour le fonctionnement du système des tiers authentificateurs et portaient parfois aussi sur un certain nombre de questions liées à des considérations d'ordre public, telles que la création du cadre administratif requis par l'infrastructure à clef publique, l'utilisation de la cryptographie pour les signatures numériques ou aux fins de confidentialité, la protection du consommateur et la possibilité que l'État conserve l'accès à l'information chiffrée, par exemple au moyen d'un dispositif de séquestre des clefs. Les travaux d'harmonisation actuellement entrepris au niveau régional par plusieurs organisations internationales ont également été portés à la connaissance du Groupe de travail.

19. Le Groupe de travail a estimé que l'une des questions les plus importantes qu'il y avait lieu d'examiner pour renforcer l'infrastructure juridique du commerce électronique était celle du régime juridique des techniques — signatures numériques et autres formes de signatures électroniques — utilisées pour remplir des fonctions équivalentes à celles des signatures manuscrites. L'on s'est accordé à penser que l'absence de règles juridiques applicables aux signatures numériques et autres signatures électroniques risquait de constituer un obstacle aux transactions économiques effectuées par voie électronique. L'on a également jugé que, dans la mesure où les pays n'abordaient pas tous la question sous le même angle et envisageaient des solutions différentes, il était justifié que la CNUDCI intervienne aux fins d'harmonisation. Non seulement elle pourrait prêter conseil quant au cadre juridique à mettre en place par les pays concernant les signatures numériques et autres formes de signature électronique, mais il serait utile qu'elle fasse porter ses travaux sur la question des critères régissant la reconnaissance des certificats délivrés par des tiers authentificateurs étrangers. L'on a fait valoir que la CNUDCI serait peut-être en mesure de faciliter ce processus en fixant des règles minima internationalement acceptables pour l'octroi de licence aux tiers authentificateurs.

20. Le Groupe a examiné la question de savoir si ses travaux devaient porter uniquement sur les "signatures numériques" (c'est à dire les techniques faisant appel à la "cryptographie à clef publique", appelée aussi "cryptographie à double clef"), ou aussi sur d'autres formes de signatures électroniques. Il a été fait observer que des techniques ne faisant pas appel à la cryptographie à clef publique, généralement appelées "signatures électroniques", étaient aussi mises au point en vue de remplir les fonctions qui étaient habituellement celles des signatures manuscrites. Ces techniques consistaient à utiliser des codes ou "mots de passe", ou des dispositifs d'identification biométrique, et pourraient coexister avec un système de signatures numériques fondé sur la cryptographie à clef publique. Il a été fait observer que, pour des actes sur support papier, certaines transactions n'avaient pas à être certifiées ni authentifiées. Les signatures numériques dans une infrastructure à clef publique offraient, certes, une très grande sécurité juridique, mais, a-t-il été fait observer, d'autres techniques pourraient se révéler être utiles aux fins d'identification et d'authentification dans toutes sortes de situations où un tel degré de sécurité juridique n'était pas nécessaire. C'est pourquoi certains ont été d'avis que le Groupe de travail ne devait pas donner l'impression, en faisant porter ses travaux uniquement sur les signatures numériques, qu'il n'encourageait pas le recours à ces techniques. Dans le cadre de ce débat, il a été dit que ce n'était pas nécessairement pour s'assurer la plus grande sécurité juridique possible que l'on avait recours aux signatures numériques utilisant la cryptographie à clef publique. Les techniques y relatives étaient suffisamment maniables pour offrir aussi des degrés de sécurité moindre, ce qui les rendaient moins coûteuses.

21. L'on s'est accordé à penser que les règles uniformes applicables aux signatures électroniques devraient avoir pour objet de donner aux législateurs des indications sur les techniques de nature à remplir une multitude de fonctions d'authentification dans un milieu électronique. Ces techniques se classaient le long d'une "échelle mobile" allant du degré de sécurité le plus élevé (comme les signatures légalisées ou certifiées conformes dans les documents sur support papier) au degré de sécurité relative offert par les marques manuscrites ou les tampons. Toutefois, une difficulté surgirait lors des travaux relatifs aux signatures électroniques : si les règles uniformes devaient donner toutes les indications nécessaires pour appliquer les principes énoncés dans l'article 7 de la Loi type, elles risquaient de devoir s'écarter d'une approche purement fonctionnelle et prévoir plus ou moins en détail de quelle manière les techniques particulières pouvaient remplir les fonctions susmentionnées.

22. Il a été généralement reconnu que, conformément au principe de la neutralité qui était celui de la Loi type, les règles uniformes ne devaient pas contrarier le recours à une méthode donnée qui soit suffisamment fiable pour remplacer les signatures manuscrites et autres signatures utilisées dans les documents sur papier, comme stipulé à l'article 7 de la Loi type. Toutefois, en vue de faciliter les délibérations, le Groupe de travail a décidé de faire porter d'abord ses travaux sur les questions relatives aux signatures numériques, mieux connues que les autres techniques, sur le plan de la législation et des ouvrages juridiques. Il a été convenu que le débat pourrait prendre un tour plus général, selon qu'il conviendrait, et que les questions concernant d'autres techniques de signature électronique pourraient aussi être examinées.

23. S'agissant de la portée des travaux, l'on s'est accordé à penser qu'elle ne devait pas s'étendre aux questions relatives à l'utilisation de la cryptographie à des fins de confidentialité. Ces questions, qui étaient déjà examinées dans d'autres instances internationales — l'Organisation de coopération et de développement économiques (OCDE), par exemple — ne se rapportaient pas directement à l'application d'un système de signatures numériques et pourraient compromettre l'avancement des travaux du Groupe, dont le but principal était de faciliter le commerce électronique. D'une façon plus générale, l'on a estimé qu'il ne fallait pas chercher à aborder, dans les règles uniformes, les questions de sécurité nationale, d'ordre public, de droit pénal ou administratif que pourrait soulever l'application de systèmes de signature numérique.

24. Des opinions diverses ont été exprimées sur le point de savoir si le Groupe de travail devait aussi examiner les questions concernant le droit relatif aux consommateurs. Un membre du Groupe a estimé que ces questions devaient être exclues du champ des travaux actuels, qui devaient porter exclusivement sur les transactions commerciales. De l'avis d'un autre, si les principales questions à considérer ne concernaient pas directement les consommateurs, il pouvait être approprié d'examiner, à l'occasion de l'élaboration de règles uniformes sur les signatures numériques, la question de savoir si des règles différentes étaient requises pour les transactions relatives aux consommateurs. L'on a cependant fait valoir qu'il pourrait être particulièrement difficile d'élaborer des dispositions propres au droit relatif aux consommateurs, en raison de la nature même du commerce électronique, qui rendait quasiment impossible l'identification d'une partie en tant que consommateur. À l'issue du débat, il a été décidé que le Groupe ferait porter l'essentiel de ses travaux sur les transactions commerciales, mais qu'il prendrait note des incidences que les questions qu'il examinait pouvaient avoir sur les transactions relatives aux consommateurs.

B. Questions juridiques spécifiques et projets de dispositions sur les signatures numériques

25. Quant à la forme que devaient prendre les travaux du Groupe, les avis étaient partagés. Selon certains, il était prématuré d'envisager une Loi type sur les questions relatives aux signatures numériques et questions connexes. Pour d'autres, il fallait partir du principe que ces travaux devaient compléter la Loi type. Il a été rappelé qu'à sa vingt-neuvième session, la Commission avait demandé au Groupe de travail de réfléchir à l'opportunité et à la possibilité de rédiger des règles uniformes sur les questions relatives aux signatures numériques et aux tiers authentificateurs. La Commission était convenue qu'à l'occasion des travaux de sa trente et unième session, le Groupe de travail pourrait entreprendre d'élaborer des projets de règles touchant certains aspects des questions susmentionnées (voir ci-dessus, par. 9).

26. Le Groupe de travail a jugé préférable de ne décider de la forme que prendraient ses travaux que lorsqu'il aurait achevé l'examen des questions juridiques de fond. Il a également décidé de surseoir à l'examen des rapports précis existant entre ses travaux futurs et la Loi type. Il a été convenu que les éventuelles règles uniformes concernant les signatures numériques devraient s'inspirer de l'article 7 de la Loi type et être considérées comme définissant la manière dont une méthode fiable pourrait servir à identifier une personne et signifier qu'elle approuvait l'information contenue dans un message électronique. De façon plus générale, les travaux sur les signatures numériques devaient être conformes aux principes énoncés et à la terminologie employée dans la Loi type.

27. Pour faciliter les travaux qu'il serait amené à entreprendre, le Groupe de travail a décidé de partir, à titre préliminaire, du principe que ces travaux prendraient la forme de projets de dispositions juridiques. L'on a cependant fait valoir qu'il pourrait peut-être envisager de donner des explications supplémentaires, au moyen,

éventuellement, d'un préambule, d'un guide d'application ou de directives distinctes, touchant en particulier les questions que l'on jugerait mal se prêter à une uniformisation. Il a été indiqué, à titre d'exemple, que des observations de la CNUDCI concernant les diverses questions soulevées par l'établissement de l'infrastructure à clef publique pourraient jouer un rôle didactique utile.

28. Il a été décidé que le Groupe de travail poursuivrait ses délibérations sur la base du projet de dispositions uniformes figurant dans la note du Secrétariat (A/CN.9/WG.IV/WP.71, par. 52 à 76). Il a été constaté que celui-ci revêtait un caractère purement indicatif et, de l'avis général, que le Groupe de travail ferait mieux, à ce stade, de se pencher sur le cadre théorique dans lequel devaient s'inscrire les règles uniformes sur les signatures numériques que de se consacrer à la rédaction de chacun des articles. On s'accordait à penser qu'il faudrait peut-être saisir l'occasion qu'offrirait l'examen de chacune des questions visées dans le projet de dispositions pour déterminer : a) si l'uniformité était nécessaire; b) si la question était traitée de façon suffisamment poussée dans la Loi type ou si des dispositions plus détaillées étaient souhaitables; c) si la question ne se rapportait qu'aux signatures numériques ou si elle pouvait être traitée à un niveau plus général; d) si la question relevait directement du droit commercial international, du mandat de la CNUDCI et de son domaine de compétence; e) si une règle impérative était nécessaire ou si l'autonomie des parties devrait prévaloir.

1. Définitions

29. Il a été indiqué d'emblée qu'il se pourrait que le Groupe de travail doive examiner d'autres définitions que celles des termes "signature numérique", "tiers authentificateurs homologués" et "certificats" proposées dans la note du Secrétariat (A/CN.9/WG.IV/WP.71, par. 52 à 60). Les définitions ci-après ont été suggérées : "on entend par 'clef privée' celle des clefs d'une paire qui est utilisée pour créer une signature numérique"; "on entend par 'clef publique' celle des clefs d'une paire qui est utilisée pour vérifier une signature numérique"; "on entend par 'paire de clefs' dans un système de cryptologie asymétrique une clef privée et la clef publique qui lui est mathématiquement associée, la deuxième de celle-ci permettant de vérifier une signature numérique créée au moyen de la première". Le Groupe de travail a pris note de cette suggestion. Il a été dit que les définitions proposées revêtaient un caractère quelque peu circulaire. On a fait observer, de façon plus générale, qu'il convenait de se garder d'introduire dans des règles uniformes normatives des définitions qui pourraient être contraires à la tradition législative de bien des pays. La question ayant été débattue, on s'est accordé à penser qu'il faudrait peut-être envisager à nouveau la possibilité d'ajouter un nombre limité de définitions à une date ultérieure.

a) Signature numérique

30. Le Groupe de travail a examiné la définition de la notion de signature numérique sur la base du projet de disposition suivant :

> "Projet d'article A
>
> 1) Une signature numérique est une valeur numérique apposée à un message électronique et qui, grâce à une procédure mathématique bien connue associée à la clef cryptographique privée de l'expéditeur, permet de déterminer que cette valeur numérique a été créée à partir de la clef cryptographique privée de l'expéditeur.
>
> 2) Les procédures mathématiques utilisées pour créer les signatures numériques autorisées en vertu de [cette loi] [ces règles] sont basées sur le chiffrement de la clef publique. Appliquées à un message de données, ces procédures mathématiques opèrent une transformation du message de telle sorte qu'une personne disposant du message initial et de la clef publique de l'expéditeur peut déterminer avec exactitude
>
> a) Si la transformation a été opérée à l'aide de la clef privée correspondant à celle de l'expéditeur; et

b) Si le message initial a été altéré une fois la transformation opérée.

3) Une signature numérique apposée à un message de données est considérée comme ayant été autorisée si elle peut être vérifiée conformément aux procédures énoncées par un tiers authentificateur homologué en vertu de [cette loi] [ces règles].

4) [L'autorité compétente dans l'État qui édicte la loi] adoptera des règles spécifiques régissant les prescriptions techniques à respecter s'agissant des signatures numériques et leur vérification."

Paragraphes 1) et 2)

31. Il a été indiqué que la définition de la notion de signature numérique devait être élargie de façon à englober non seulement la cryptographie à clef publique, mais aussi d'autres types de signature électronique. La plupart des membres du Groupe estimaient cependant qu'il était inopportun d'essayer d'établir une définition de la signature numérique qui s'écarterait des usages existants. Il a été convenu que la notion de signature numérique ne devait s'étendre qu'aux systèmes de cryptologie asymétriques, mais qu'il faudrait peut-être établir d'autres définitions englobant des techniques auxquelles renverrait la notion plus large de signature électronique.

32. Touchant le paragraphe 1), il a été indiqué que les mots "a été créée à partir" devraient être remplacés par les mots "n'a pu être créée qu'à partir". Le Groupe de travail a décidé qu'à un stade aussi peu avancé de ses délibérations, il ne devrait pas essayer de remanier le texte dans le détail. On s'est généralement accordé à penser que la notion de signature numérique telle qu'elle était définie aux paragraphes 1) et 2) convenait pour délimiter le champ d'application des travaux futurs. La question ayant été débattue, le Groupe de travail a jugé les paragraphes 1) et 2) généralement acceptables quant au fond, tout en convenant qu'il aurait peut-être à en remanier le libellé ultérieurement.

Paragraphe 3)

33. Diverses questions ont été soulevées concernant l'objet du paragraphe 3). On a émis l'opinion que s'il visait les concepts d'infrastructure à clef publique et de vérification des signatures numériques, son but n'était pas atteint; en revanche, il traitait de questions de fond ne relevant pas de la définition de la signature numérique. L'on a avancé que le paragraphe 3) pourrait être interprété comme introduisant une procédure de vérification comme condition de la validité de la signature numérique. L'on a estimé qu'il était préférable de le supprimer et de le remplacer par une définition descriptive de la vérification des signatures.

34. L'on a fait valoir que le paragraphe 3) pouvait être interprété comme traitant uniquement de la validité des signatures numériques utilisées dans le cadre d'une infrastructure à clef publique exploitée par les autorités publiques. Dans son libellé actuel, cette disposition paraissait excessivement rigide, ce qui pourrait exclure l'acceptation du recours aux signatures numériques dans un autre contexte, comme les infrastructures à clef publique créées par des entités autres que les autorités publiques. D'une manière générale, on a estimé qu'il n'était pas souhaitable d'alourdir les transactions qui pourraient se dérouler dans des cercles fermés entre des parties qui n'éprouvaient pas le besoin de recourir aux services de tiers authentificateurs. Alors que les États examinaient diverses options concernant la mise en place d'infrastructures à clef publique, certains ont estimé qu'il serait prématuré de privilégier, dans le cadre du projet de règles uniformes, un système donné d'infrastructures au détriment de tous les autres.

35. On a exprimé l'avis que, si le paragraphe 3) devait être lu conjointement avec l'article 7 de la Loi type, ces deux dispositions n'étaient peut-être pas totalement compatibles. Par exemple, le paragraphe 3) nuançait la notion de signature numérique en lui ajoutant le qualificatif "autorisée", mot qui n'était utilisé ni dans le contexte de l'article 7 de la Loi type, ni dans aucune des dispositions des projets d'articles A à J tels qu'ils figuraient dans la note du Secrétariat (A/CN.9/WG.IV.WP.71). En outre, l'article 7 mentionnait l'utilisation d'une méthode de signature "aussi fiable qu'il était approprié au vu de l'objet pour lequel le message de donnée avait été créé ou communiqué", reconnaissant ainsi divers niveaux de fiabilité au vu de l'objet pour lequel le message avait été créé ou communiqué,

y compris tout accord des parties. On a fait valoir que, en vertu de l'article 7, les parties à une transaction se faisant réciproquement confiance pourraient convenir d'un niveau de sécurité qui leur suffirait sans avoir obligatoirement recours à des tiers authentificateurs. Du point de vue des parties, la considération primordiale était de savoir si le système qu'elles exploitaient était fiable. On a fait valoir qu'un certain nombre d'éléments assuraient la fiabilité du matériel du logiciel et des procédures utilisés par les parties (par exemple, être raisonnablement certain qu'il n'y aurait ni intrusion ni usage impropre; offrir un degré raisonnable d'accessibilité, de fiabilité et de bon fonctionnement; être raisonnablement adapté à l'exercice des fonctions qui leur étaient assignées; et fonctionner conformément aux principes de sécurité généralement admis). Il incombait donc aux parties de décider si le degré de fiabilité qu'elles exigeaient devait comprendre une procédure de vérification appliquée par des tiers authentificateurs. Le libellé du paragraphe 3), pour sa part, supposait que les signatures numériques ne seraient fiables que si elles pouvaient être certifiées avec l'assistance de tiers authentificateurs. Il apparaissait donc plus restrictif que l'article 7 de la Loi type. L'on a avancé qu'il faudrait procéder à une révision de fond de l'article 3 si l'on voulait l'harmoniser avec l'article 7.

36. Des questions ont également été soulevées concernant la mention, au paragraphe 3), de la vérification de la signature numérique conformément aux procédures fixées par les tiers authentificateurs. On a émis l'opinion qu'une référence à ces procédures soulevait la question des instructions techniques applicables à la vérification de la signature numérique et autres critères de fonctionnement appliqués par des tiers authentificateurs, ou celle des effets juridiques découlant des cas où ces procédures n'auraient pas été suivies. Or, il s'agissait là de questions de fond qui ne pouvaient pas être convenablement traitées dans le champ d'application limité du projet d'article A. Il a donc été proposé de supprimer la mention concernant les procédures de vérification.

37. Ayant examiné les différentes vues exprimées, le Groupe de travail a décidé de supprimer le paragraphe 3). Il a été convenu d'ouvrir le débat sur les options possibles concernant les infrastructures à clef publique après l'examen de la question des effets juridiques des signatures numériques.

Paragraphe 4)

38. On a émis l'opinion que le paragraphe 4), dans la mesure où il confiait à l'État la responsabilité de fixer les règles techniques régissant les signatures numériques, excluait les infrastructures à clef publique mises en place par des entités autres que les autorités publiques. Ayant décidé de supprimer le paragraphe 3), et compte tenu du lien logique existant entre les deux dispositions, le Groupe de travail a décidé que le paragraphe 4) serait, lui aussi, supprimé.

b) Tiers authentificateurs homologués

39. Pour l'examen des questions ayant trait à la définition du tiers authentificateur homologué, le Groupe de travail s'est fondé sur le projet de disposition ci-après :

"Projet d'article B

1) ... [c'est l'État qui édicte la loi qui choisit l'organe ou l'autorité compétente chargé d'homologuer les tiers authentificateurs] peut homologuer les tiers authentificateurs permettant à ceux-ci d'agir en vertu de [la présente loi] [ces règlements]. Cette homologation peut être annulée.

2) ... [c'est l'État qui édicte la loi qui précise l'organe ou l'autorité compétente chargé de promulguer des règlements s'agissant des tiers authentificateurs homologués] peut établir des règles régissant les modalités en vertu desquelles les homologations peuvent être accordées, et promulguer des règlements précisant le fonctionnement des tiers authentificateurs.

3) Les tiers authentificateurs homologués peuvent délivrer des certificats concernant les clefs cryptographiques de personnes physiques ou morales.

4) Les tiers authentificateurs homologués peuvent proposer ou faciliter l'enregistrement et le datage de la transmission et de la réception de messages de données, et remplir d'autres fonctions ayant trait aux communications protégées au moyen de signatures numériques.

5) ... [c'est l'État qui édicte la loi qui nomme l'organe ou l'autorité compétente chargé d'établir des règles spécifiques s'agissant des fonctions à remplir par les tiers authentificateurs homologués] peut promulguer des lois spécifiques en ce qui concerne les fonctions à remplir par les tiers authentificateurs homologués s'agissant de la délivrance de certificats aux personnes physiques ou morales."

40. Le Groupe de travail a procédé à un échange de vues sur l'approche à adopter en ce qui concerne les tiers authentificateurs. Selon l'une des opinions exprimées, le projet d'article B, tel qu'il était libellé, semblait prescrire une méthode précise pour utiliser une infrastructure à clef publique; or, il était préférable de laisser chaque État adopter ses propres règles en la matière. L'on a fait valoir que, s'il était vrai que les tiers authentificateurs pouvaient jouer un rôle essentiel pour ce qui était de certifier la fiabilité des signatures numériques, des systèmes de signature numérique qui fonctionneraient sans tiers authentificateurs n'étaient pas inconcevables. Il a également été avancé qu'instaurer un système juridique d'homologation publique des tiers authentificateurs ne contribuerait pas nécessairement à promouvoir la confiance dans la fiabilité des signatures numériques; il vaudrait mieux pour cela faire appel à des tiers authentificateurs homologués par des entités privées, ou à d'autres dispositifs issus du marché. Selon un autre point de vue, le projet d'article B était acceptable, dans l'ensemble, aux fins de définir les tiers authentificateurs homologués, car il était formulé en termes non impératifs, en particulier pour ce qui était du paragraphe 2, qui n'empêchait pas l'État d'utiliser différemment sa propre infrastructure à clef publique.

41. S'agissant de l'approche que l'on pourrait adopter quant aux tiers authentificateurs, le Groupe de travail a été invité à envisager deux objectifs éventuels concernant la définition des termes "tiers authentificateur". L'un des objectifs pourrait être de donner à l'État des directives concernant les éléments essentiels à prendre en compte dans l'utilisation des infrastructures à clef publique nationales. L'on a fait valoir que le projet d'article B n'était pas suffisamment détaillé pour donner des directives suffisantes à cet égard. Un autre objectif pourrait être de confier à l'État la responsabilité de l'infrastructure à clef publique au plan national, mais de préciser, dans la définition du terme "tiers authentificateur", les critères que devait appliquer chaque État en matière de reconnaissance des certificats délivrés par des tiers authentificateurs étrangers. Il a été suggéré que, si le Groupe de travail voulait circonscrire la portée du projet de règles uniformes à ce dernier objectif, il faudrait peut-être ajouter au projet d'article B un chapeau, qui pourrait, par exemple, se lire comme suit : "Les dispositions uniformes s'appliquent aux certificats délivrés par un régime juridique doté des attributs suivants :". L'on a toutefois fait observer que, si l'on adoptait une telle proposition, il faudrait remanier considérablement les autres dispositions du projet d'article B. L'on a suggéré par ailleurs de ne pas énoncer de critère spécifique dans ce projet d'article, et de se contenter de la disposition générale qui figurait au paragraphe 2. On pourrait également faire figurer d'autres observations dans des directives concernant l'élaboration du projet de règles uniformes, notamment une liste indicative des critères dont pourraient éventuellement tenir compte chaque État.

42. Le Groupe de travail s'est accordé à penser que l'on devait pouvoir examiner à un stade ultérieur la question de savoir si, dans le projet de règles uniformes, la définition du tiers authentificateur devait servir à d'autres fins que de définir les critères à appliquer par chaque État pour reconnaître les certificats délivrés par des tiers authentificateurs étrangers. La plupart des membres du Groupe ont estimé que, si l'établissement de normes ou de critères pouvait aider les tiers authentificateurs à instaurer le degré de confiance nécessaire à leur fonctionnement, il pourrait par ailleurs se révéler nécessaire de faire la distinction entre la question générale de la fiabilité du tiers authentificateur, qui dépendrait peut-être du régime juridique sous lequel ils avaient été établis, et les questions plus spécifiques liées au degré de confiance inspiré par les certificats délivrés par tel ou tel tiers authentificateur.

43. Il a été avancé que les dispositions concernant les fonctions et attributions du tiers authentificateur, telles qu'énoncées dans le projet d'article B, n'avaient pas seulement pour utilité de constituer les éléments structurels d'un système de tiers authentificateurs (par exemple une infrastructure à clef publique). Elles étaient aussi utiles pour déterminer les effets à donner aux signatures numériques et aux actes liés à des signatures numériques ou impliquant

l'utilisation de ces signatures. Cela étant, l'on a avancé que, dans ses délibérations en la matière, le Groupe de travail pouvait avoir intérêt à garder à l'esprit un ensemble de facteurs utiles pour déterminer les effets juridiques à donner aux signatures numériques. L'on a présenté les facteurs suivants comme instrument d'analyse que pourrait envisager le Groupe de travail : a) les types de signature (c'est-à-dire, du général au particulier, la signature électronique, la signature numérique, la signature numérique avec certificat et la signature numérique avec certificat délivré par un tiers authentificateur homologué); b) les parties concernées (à savoir, les parties contractantes directes, y compris les tiers authentificateurs, les tiers tels que les chargeurs et les banques, les entités gouvernementales, d'autres entités telles que les prestataires de services ou les entreprises de télécommunications); c) les actes ou événements auxquels est conféré un effet juridique (c'est-à-dire l'utilisation d'une signature numérique, la délivrance de certificats, y compris la délivrance sans autorisation, l'expiration du certificat, la révocation du certificat, la révocation de l'homologation accordée à un tiers authentificateur); d) le champ d'application des travaux de la CNUDCI dans ce domaine (application internationale uniquement, application internationale plus propositions pour des législations nationales, propositions pour des législations nationales); e) l'effet juridique (c'est-à-dire la validité, les obligations de l'entité qui délivre les certificats et de la personne faisant fond sur les certificats, les recours, la responsabilité, y compris ses limites, la preuve); f) les techniques de rédaction (c'est-à-dire la prescription de normes, l'effet juridique si les normes sont respectées, l'effet juridique si les normes ne sont pas respectées). Le Groupe de travail a estimé que la liste de facteurs proposée lui serait fort utile pour analyser l'objectif et les incidences des dispositions concernant les tiers authentificateurs.

44. Au cours du débat qui a suivi, le Groupe de travail s'est demandé s'il serait souhaitable d'imposer, dans le cadre du projet de règles uniformes, des critères de fonctionnement aux tiers authentificateurs, qu'ils soient ou non homologués.

45. L'on a suggéré de compléter le projet d'article B en y ajoutant des règles uniformes qui indiqueraient expressément les critères à prendre en considération pour l'homologation des tiers authentificateurs, ou qui définiraient les normes minima auxquelles ces derniers devaient répondre pour que les certificats qu'ils délivraient aient valeur juridique. Cela était indispensable si l'on voulait que les tiers authentificateurs soient visés par les règles uniformes. On a renvoyé à la note du Secrétariat (A/CN.9/WG.IV/WP.71, par. 44) où étaient énumérés un certain nombre d'éléments qui pourraient être considérés pour déterminer la fiabilité d'un tiers authentificateur. De l'avis général, cette liste pouvait utilement servir de point de départ des discussions si l'on décidait d'approfondir la question. Il a été proposé d'étendre le champ des critères de sorte à prendre en compte, par exemple, la compétence du personnel d'encadrement, ou la séparation des tâches d'authentification de toute autre tâche que l'authentificateur pouvait éventuellement assurer par ailleurs.

46. Certains membres du Groupe de travail ont estimé qu'il n'y avait pas lieu de spécifier des critères d'habilitation applicables aux tiers authentificateurs. On a rappelé que le Groupe de travail avait étudié la question du rôle de l'État dans les infrastructures à clef publique et conclu que, dans certains pays, des entités privées rempliraient la fonction d'authentificateur sans avoir besoin d'obtenir au préalable l'autorisation de l'État (voir ci-dessus, par. 40). De plus, les critères de l'administration publique n'étaient pas les seuls acceptables; on pouvait aussi envisager d'autres possibilités, par exemple, s'en remettre aux usages et pratiques du commerce entre États, ou encore à des normes de compétence fixées par des entités non gouvernementales sérieuses, comme c'était le cas dans certains domaines commerciaux. L'on a fait valoir que spécifier des critères d'habilitation n'était ni pertinent, ni judicieux lorsque la fonction d'authentification pouvait être exercée sans l'autorisation de la puissance publique. De plus, il faudrait alors préciser dans tous les cas quelle entité ou autorité avait compétence pour déterminer si tel ou tel authentificateur remplissait bien les critères — ce qui créerait des problèmes lorsqu'il s'agissait d'authentificateurs ne faisant pas partie d'une infrastructure à clef publique régie par l'État.

47. Face à ces objections, on a fait valoir que l'établissement de critères communs d'habilitation des tiers authentificateurs permettrait d'inspirer confiance dans l'authenticité des signatures numériques. De telles normes ne seraient peut-être pas nécessaires tant que les transactions électroniques se faisaient au moyen d'un système fermé que les partenaires jugeaient suffisamment sûr pour, s'ils se faisaient confiance, se dispenser de certificats d'authentification. Mais pour que l'usage des signatures numériques puisse se répandre, il fallait amener le grand public à croire en leur authenticité et à l'efficacité des méthodes employées pour la garantir. Ce but serait atteint

si l'on parvenait à le convaincre que les entités chargées d'authentifier une clef publique devaient remplir certains critères qui assuraient que l'on pouvait se fier à elles. On a fait observer que, s'il ne fallait pas écarter a priori l'éventuel recours aux usages et pratiques du commerce ou les normes d'habilitation acceptables que les entités non gouvernementales pouvaient peut-être fixer dans un domaine commercial particulier, il n'existait pas encore de pratique établie pour déterminer quels critères appliquer aux tiers authentificateurs.

48. On a fait valoir que les deux formules à l'étude — établissement de normes d'habilitation par l'État et acceptation de normes applicables aux entités ne faisant pas partie d'une infrastructure à clef publique régie par l'administration publique — n'étaient pas nécessairement incompatibles. Elles se différenciaient peut-être simplement par les effets juridiques respectifs des signatures numériques dans l'un ou l'autre cas. Lorsque c'était l'État qui habilitait le tiers authentificateur, il ne le faisait qu'après s'être assuré que ce dernier remplissait les critères, cette conformité aux normes étant indispensable pour que les certificats délivrés puissent avoir un effet juridique. Dans le second cas, le tiers authentificateur n'avait pas besoin, pour pouvoir assumer cette fonction, de prouver qu'il remplissait les critères; mais si les certificats qu'il délivrait venaient à être contestés (par exemple devant les tribunaux ou une instance d'arbitrage), l'organe saisi devrait, pour se prononcer sur leur fiabilité, déterminer s'ils émanaient d'une autorité répondant bien aux critères.

49. L'on a avancé que la fiabilité d'un certificat donné pourrait être fonction de la décision prise par l'authentificateur concernant ledit certificat, et non pas de critères d'ordre institutionnel. La fiabilité conjoncturelle ne dépendrait pas nécessairement de l'habilitation éventuelle de l'authentificateur ni des usages et pratiques du commerce acceptés sur le plan international. L'on a estimé que le critère de fiabilité pourrait varier en fonction du motif pour lequel la fiabilité devait être assurée (certification croisée, octroi de licence, détermination de la responsabilité).

50. Les travaux ne faisant que commercer et les vues divergeant, les membres du Groupe se sont dans leur ensemble ralliés à la proposition préconisant de ne rejeter d'emblée aucune des deux possibilités ci-dessus et de les considérer comme des hypothèses de travail, en revenant sur ces points plus tard, après avoir examiné d'autres questions qui s'y rattachaient intrinsèquement, par exemple celle de la responsabilité des tiers authentificateurs et les problèmes que soulevait l'authentification internationale.

2. Responsabilité

51. Pour l'examen des notions ayant trait à la responsabilité du tiers authentificateur, le Groupe de travail s' est fondé sur le projet de dispositions ci-après :

"Projet d'article H

1) Un tiers authentificateur homologué est responsable devant toute personne ayant agi de bonne foi sur la foi d'un certificat délivré par ce tiers authentificateur, en cas de perte due à une faute d'enregistrement imputable au tiers authentificateur, à une défaillance technique ou à d'autres circonstances de même nature [même si la perte n'est pas imputable] [si la perte est imputable] à une négligence du tiers authentificateur.

2) Variante X La responsabilité pour toute perte individuelle ne dépasse pas [montant]. ... [l'État qui édicte la loi désigne l'organe ou l'autorité ayant compétence pour réviser le montant maximum] peut modifier ce montant tous les deux ans de façon à tenir compte de l'évolution des prix.

Variante Y ... [l'État qui édicte la loi désigne l'organe ou l'autorité ayant compétence pour promulguer des règlements relatifs à la responsabilité] peut promulguer des règlements relatifs à la responsabilité des tiers authentificateurs.

3) Dans le cas où la partie ayant subi une perte a contribué à celle-ci soit délibérément, soit par négligence, l'indemnisation peut être réduite, voire totalement refusée.

[4) Lorsqu'un tiers authentificateur homologué a reçu notification de l'annulation d'un certificat, il enregistre immédiatement cette annulation. Si le tiers authentificateur faillit à cette tâche, il est responsable de toute perte encourue par l'utilisateur.]"

Paragraphes 1) et 2)

Observations générales

52. Le Groupe de travail a débattu du champ et des implications du projet de dispositions sur la responsabilité du tiers authentificateur. On a fait observer que dans cette question, deux types de responsabilité étaient en jeu : la responsabilité structurelle, lorsque le tiers authentificateur ne respectait pas les conditions de son habilitation, et la responsabilité conjoncturelle, qui résultait de sa décision de délivrer, suspendre ou annuler un certificat. Dans le premier cas, l'authentificateur trahissait la confiance que l'administration publique avait mise en lui, et l'organe qui l'avait homologué pouvait à bon droit lui imposer une amende ou d'autres sanctions, à la mesure de la faute. Dans le second cas, le tiers authentificateur n'avait pas rempli les obligations professionnelles qu'il avait envers son client. Bien souvent, cependant, c'était le partenaire commercial de ce dernier, qui généralement ne passait pas de contrat avec le tiers authentificateur, qui subirait le préjudice. On a posé la question de savoir si, dans ces conditions, il conviendrait de donner à la partie lésée un recours direct contre le tiers authentificateur, ou seulement le droit de se retourner contre son partenaire, lequel pourrait disposer à son tour d'un recours contre l'authentificateur. On pouvait craindre qu'il ne soit difficile d'établir un régime de responsabilité satisfaisant qui donne à l'utilisateur d'un certificat un recours direct contre le tiers authentificateur.

53. On a avancé qu'il vaudrait peut-être mieux que le Groupe de travail n'aborde pas la question de la responsabilité du tiers authentificateur, qui était délicate et complexe et ne pouvait être traitée comme il le fallait dans le projet de règles uniformes. On a rappelé que, lors de l'élaboration de la Loi type, il avait été décidé de laisser complètement de côté la question de la responsabilité des tiers prestataires de services. On pouvait penser que cette question était étroitement liée à celle du préjudice, qui ne se prêterait peut-être pas facilement à une harmonisation internationale. Le Groupe de travail a été invité à déterminer s'il valait mieux laisser au droit national le soin de régir ces deux questions, sans les aborder dans les règles uniformes. Si tel était effectivement le cas, on pouvait soit s'en remettre aux dispositions internes visant le conflit de lois, qui détermineraient les normes applicables; soit introduire dans les règles uniformes une disposition précise visant le conflit de lois; soit déterminer directement quelle règle il convenait d'appliquer en cas de conflit de lois (par exemple la règle interne du pays où le tiers authentificateur était officiellement établi ou autorisé à exercer sa fonction). On a fait valoir à l'appui de cette suggestion que la question de la responsabilité était essentiellement celle des garanties données par l'authentificateur, et qu'il était préférable qu'elle soit réglée par les partenaires eux-mêmes, ou conformément aux dispositions du droit interne applicables à leur relation contractuelle.

54. Toutefois, l'élaboration de normes régissant la responsabilité du tiers authentificateur a aussi été vigoureusement défendue. La question de la responsabilité, a-t-on fait valoir, était trop importante pour qu'on laisse aux seules parties le soin de la régir, d'autant que les utilisateurs de certificats ne passeraient peut-être pas tous directement contrat avec l'authentificateur. Si l'utilisateur n'était pas pleinement autorisé à demander à son partenaire commercial réparation des fautes du tiers authentificateur, la victime d'un acte frauduleux où le tiers authentificateur aurait, soit en toute connaissance de cause, soit par négligence, laissé utiliser des noms ou des identités fictifs se trouverait sans aucun recours. De plus, en l'absence de dispositions régissant la responsabilité, l'on risquait de voir certains pays n'imposer, pour encourager ou faciliter l'implantation de tiers authentificateurs sur leur territoire, qu'une responsabilité dérisoirement limitée, ce qui serait pour le moins fâcheux. Devant ces "paradis de l'authentification" qui pourraient se créer, les partenaires commerciaux risquaient de se montrer réticents à user des signatures numériques, ce qui n'irait pas dans le sens du développement du commerce électronique que l'on s'était fixé comme objectif. Aussi difficile que soit la question de la responsabilité, qui recouvrait à la fois la responsabilité

contractuelle et la responsabilité délictuelle, il fallait, selon le sentiment général, qu'elle fût visée dans les règles uniformes.

55. À l'issue des débats, le Groupe de travail a décidé que les règles uniformes devaient en principe comporter des dispositions régissant la responsabilité du tiers authentificateur pour autant que celui-ci intervienne dans des systèmes de signature numérique.

Nature de la responsabilité

56. S'agissant de la nature de la responsabilité du tiers authentificateur, on s'est en particulier demandé si la responsabilité devait reposer sur la notion de faute ou s'il s'agirait de "responsabilité de plein droit", notion également appelée "responsabilité objective" ou "responsabilité sans faute". On a soulevé des objections à l'insertion de dispositions posant la responsabilité objective du tiers authentificateur. On a fait observer que la responsabilité objective s'écartait du principe général du droit de la responsabilité civile en vertu duquel chacun était responsable de sa propre faute, de sorte qu'elle était acceptée en droit interne pour des motifs exceptionnels d'ordre public, la responsabilité sans faute s'appliquant à des personnes se livrant à des activités par trop dangereuses. Il n'y avait aucun motif impérieux de soumettre les tiers authentificateurs à un régime de responsabilité objective. En outre, un tel régime aurait pour effet fâcheux d'entraver le développement de la certification homologuée et de limiter ainsi les possibilités d'emploi de signatures numériques. Au surplus, il a été fait observer que le tiers authentificateur pourrait fournir à ses clients et au public toute une gamme de services pouvant aller de l'établissement de la liste des détenteurs de la clef publique et de leurs clefs respectives à des services plus individualisés consistant à garantir l'authenticité des clefs publiques et l'identité de leurs détenteurs. Le degré de l'obligation assumée par les tiers authentificateurs, ainsi que leurs tarifs variaient selon le type de service fourni. Si l'on considérait cette gamme de services, il n'était pas raisonnable d'imposer le même degré de responsabilité à tous les tiers authentificateurs quelles que soient les circonstances. Il a donc été proposé de fonder le régime de responsabilité applicable aux tiers authentificateurs sur la négligence, suivant en cela la solution envisagée au paragraphe 1 du projet d'article H.

57. L'on a fait observer toutefois qu'il ne serait pas équitable d'imposer à la partie lésée la charge de faire la preuve de la négligence du tiers certificateur. Vu le degré de spécialisation technique que l'on était en droit d'attendre de lui et le niveau de confiance élevé qu'il était censé inspirer, ce dernier devait normalement voir sa responsabilité engagée chaque fois que l'émission de certificats défectueux entraînait des dommages. On a relevé que dans certains systèmes de droit, les membres de certaines catégories professionnelles (par exemple, les notaires dans certains pays de droit civil) étaient tenus de souscrire une assurance au tiers et de participer à une caisse commune d'indemnisation destinée à indemniser les parties lésées du fait de leurs actes. On a estimé que les tiers authentificateurs faciliteraient sans doute la création d'une telle caisse en se regroupant au sein d'un cadre institutionnel, par exemple, un dispositif de délivrance de licences.

58. L'on a jugé que les divergences d'opinions qui s'étaient fait jour au sein du Groupe de travail pourraient être aplanies si, en lieu et place d'une règle positive spécifiant les circonstances où les tiers authentificateurs verraient leur responsabilité engagée, le projet de règles uniformes contenait une disposition énonçant une présomption simple de responsabilité. En vertu de cette proposition, par exemple, en cas d'identification erronée d'une personne ou d'attribution par erreur d'une clef publique à une personne, le tiers authentificateur verrait sa responsabilité retenue à raison de la perte subie par toute partie lésée, à moins qu'il ne puisse démontrer qu'il s'était efforcé de son mieux d'éviter l'erreur. Il pourrait réfuter la présomption, par exemple, en démontrant qu'il s'était conformé à une norme de conduite qui aurait été établie par les règles uniformes. On a fait observer qu'un tel régime de responsabilité, qui rappelait ceux institués dans certains droits internes en matière de responsabilité du fait des produits, conférerait un surcroît de protection aux utilisateurs de services sans pour autant imposer une responsabilité objective au tiers authentificateur. Le Groupe de travail a accueilli favorablement cette proposition dans laquelle on s'est accordé à voir un moyen viable, pour le Groupe, de traiter dans l'avenir de la difficile question de la responsabilité des tiers authentificateurs.

59. Le Groupe de travail a ensuite examiné les cas où la responsabilité du tiers authentificateur ne serait pas retenue à raison d'une prestation défaillante. On a estimé qu'en vertu du régime de responsabilité envisagé, le tiers

authentificateur devait être déchargé de toute responsabilité pour autant qu'il puisse démontrer qu'il avait fait preuve de sérieux pour identifier le détenteur de la clef publique ou s'acquitter de ses fonctions d'authentification, que l'erreur était le fait de l'utilisateur même, ainsi qu'il était stipulé au paragraphe 3 du projet d'article H, ou qu'elle était imputable à des circonstances indépendantes de sa volonté. On s'est accordé à estimer que des causes d'exemption analogues seraient acceptables.

Déclarations des pratiques d'authentification (Certification practice statements) et autonomie des parties

60. L'on a fait valoir que, s'agissant de la responsabilité, il importait de ne pas perdre de vue les attentes et intérêts mutuels de l'utilisateur et du tiers authentificateur. Ce dernier devait rendre publiques, par une déclaration, ses pratiques d'authentification et informer ainsi les utilisateurs des méthodes et procédures notamment qu'il employait pour identifier le détenteur de la clef publique. L'utilisateur, pour sa part, devait déterminer raisonnablement la véracité de ce document. En outre, il devait être tenu de s'assurer qu'un certificat demeurait valide (par exemple, qu'il n'avait pas été révoqué) avant de s'en prévaloir. Enfin, il était censé agir avec prudence, en se fondant sur les informations mises à sa disposition. À la question de savoir comment l'utilisateur pourrait procéder pour vérifier la validité d'un certificat, il a été répondu que les tiers authentificateurs pourraient être tenus d'établir des bases de données, comme certains le faisaient déjà, auxquelles les parties intéressées pourraient accéder pour vérifier la validité du certificat. En réponse à cette proposition, on a fait observer que, s'il était sans doute bon d'encourager l'utilisateur à faire preuve de prudence dans le maniement du certificat, c'était au tiers authentificateur qu'il incombait au premier chef de veiller à son authenticité et à sa validité et qu'il fallait s'entourer de toutes les précautions avant d'imposer à l'utilisateur des devoirs qui risquaient de lui faire endosser une partie de cette responsabilité. Dans la plupart des cas, l'utilisateur ne serait normalement pas en mesure de déterminer un certain nombre de facteurs ayant trait à la validité du certificat, comme les procédures d'identification utilisées par le tiers authentificateur ou la question de savoir si le détenteur de la clef publique détenait également la clef privée correspondante. Il serait déraisonnable de reporter l'une quelconque de ces responsabilités sur l'utilisateur.

61. Le Groupe de travail a discuté du rôle de la déclaration des pratiques d'authentification et de la mesure dans laquelle elle pourrait contribuer à limiter ou à définir autrement le champ de la responsabilité incombant au tiers authentificateur. Afin de protéger les intérêts des utilisateurs, le tiers authentificateur pourrait être tenu de révéler la portée de sa responsabilité par des dispositions contenues dans sa déclaration. D'un point de vue technique, il serait possible, pour les utilisateurs, de prendre connaissance de la déclaration par voie électronique. On a exprimé l'opinion qu'une partie qui solliciterait les services d'un tiers authentificateur devait accepter d'être liée par les termes de la déclaration lorsqu'elle utilisait les services dudit tiers authentificateur. Les arrangements contractuels conclus entre les parties devaient l'emporter sur les règles découlant d'autres sources et, à cet égard, il importait de garantir l'opposabilité de ces termes et conditions. Certains ont toutefois estimé qu'une disposition aussi importante, pour les parties, que celle limitant la responsabilité du tiers authentificateur devait figurer dans le certificat et non pas dans un document - même d'accès facile - simplement mentionné dans ledit certificat.

62. Les membres du Groupe de travail se sont accordés à penser qu'en concevant un régime de responsabilité à l'intention des tiers authentificateurs, il fallait tenir dûment compte de la nécessité de sauvegarder l'autonomie des parties. Toutefois, on a exprimé la crainte qu'un tiers authentificateur puisse se soustraire à la responsabilité encourue du fait de sa propre négligence à la faveur de clauses d'exemption ou de déni de responsabilité contenues dans la déclaration des pratiques d'authentification ou dans tout autre document qu'il aurait publié. On a fait valoir que le récepteur d'un message qui aurait utilisé un certificat pour vérifier l'authenticité d'une signature numérique n'aurait souvent aucun lien juridique direct avec le tiers authentificateur et qu'en conséquence il ne serait pas en mesure de négocier avec celui-ci les clauses de cette responsabilité. Même l'initiateur du message qui entretiendrait une relation de droit avec le tiers authentificateur pourrait parfois ne pas être en mesure de négocier ces clauses qui, dans nombre de cas, prendraient la forme de conditions commerciales préétablies non sujettes à modification. Dans certains systèmes de droit, l'exclusion unilatérale de toute clause de limitation de responsabilité serait contraire à l'ordre public. Toutes limitations et exemptions de responsabilité retenues devaient être conformes à la loi et approuvées par les autorités publiques.

Limites de la responsabilité

63. Le Groupe de travail s'est penché sur la question de savoir si la responsabilité du tiers authentificateur devait être assortie de limites et comment ces limites pouvaient être fixées. En objection à l'introduction de limites en la matière, on a fait remarquer que de telles limites existaient généralement dans les domaines d'activité soumis à une certaine forme de monopole, ce qui était le cas des services postaux ou téléphoniques dans un certain nombre de pays. Mais dans d'autres domaines d'activité, ouverts à la concurrence, il n'y avait aucune raison de fixer des limites en matière de responsabilité.

64. Divers points de vue ont néanmoins été exprimés, qui approuvaient la mise en place d'une forme ou d'une autre de la limitation de responsabilité des tiers authentificateurs. Les arguments suivants ont été avancés : a) l'authentification était un secteur en plein essor, dont le développement pourrait être entravé par le risque d'encourir une responsabilité illimitée; b) il importait de donner au tiers authentificateur la possibilité de déterminer le montant à concurrence duquel il était disposé à assumer une responsabilité, et cette possibilité pouvait bien être une condition préalable sans laquelle il ne pouvait pas contracter une assurance couvrant convenablement ses activités; et c) il se pouvait que, en ce qui concernait les signatures numériques, le rôle du tiers authentificateur se limite à la délivrance d'un certificat qui pouvait, en soi, n'avoir qu'une valeur quantifiable réduite, voire nulle. On a également fait valoir que lorsqu'un certificat était délivré pour établir un lien entre une clef publique et une personne donnée, ledit certificat pouvait être apposé à un certain nombre de messages dans toute une série d'opérations différentes dont le tiers authentificateur ne pouvait dans la plupart des cas pas prévoir le montant total. On a fait remarquer que dans le cas des opérations sur carte de crédit, il existait des moyens d'autoriser chaque opération séparément, afin que la société ayant délivré la carte de crédit puisse, chaque fois que la carte était utilisée pour effectuer une opération dont le montant excédait un plafond déterminé à l'avance, estimer le risque qu'elle courait en cas d'utilisation non autorisée. Or, le tiers authentificateur n'avait pas cette possibilité et n'était en principe pas au courant des termes des opérations effectuées par ses clients. Il aurait été dès lors difficile d'établir un seuil ou plafond de responsabilité en se fondant sur le montant de l'opération aux fins de laquelle une signature numérique avait été utilisée. Étant donné qu'une seule signature pouvait être apposée à un nombre infini d'opérations, il était peu probable que les tiers authentificateurs soient en mesure d'acquérir une assurance responsabilité civile d'un coût raisonnable.

65. S'agissant des méthodes qui pouvaient être utilisées pour limiter la responsabilité incombant au tiers authentificateur, un certain nombre de suggestions ont été examinées par le Groupe de travail. L'une des façons de procéder consistait à déterminer un montant fixe, à l'instar de la variante X du paragraphe 2 du projet d'article H. Selon d'autres formules, la limitation de la responsabilité devait se fonder sur un multiple du droit payé par le détenteur, sur un pourcentage de la valeur de l'opération ou sur un pourcentage de la perte effectivement subie par la partie lésée. L'on a toutefois fait remarquer que le dommage qui pouvait résulter des actes d'un tiers authentificateur n'était pas suffisamment facile à quantifier pour qu'il puisse servir de critère objectif permettant d'assigner un montant fixe. Par ailleurs, le service rendu par un tiers authentificateur et les droits qu'il prélevait n'avaient souvent aucun rapport avec la valeur des opérations auxquelles ils se rapportaient, ni avec le dommage qui pouvait être subi par les parties. D'autres formules de limitation, par exemple celles figurant dans la Convention des Nations Unies sur le transport de marchandises par mer (Règles de Hambourg) ou dans la Loi type de la CNUDCI sur les virements internationaux, avaient trait à des opérations portant sur des éléments quantifiables (valeur des marchandises, montant du virement, etc.) qui n'existaient pas nécessairement dans le cas à l'étude.

66. Un autre moyen de limiter la responsabilité consistait à exclure celle-ci pour certains types de dommages, les dommages "indirects" par exemple. Concernant cette dernière possibilité, on a fait remarquer que la notion de "dommages indirects" pouvait ne pas être interprétée de la même manière dans différents systèmes juridiques. On a donc fait valoir qu'il serait préférable de préciser les types de pertes qui seraient couverts par cette notion et pour lesquels le tiers authentificateur ne serait pas responsable. La mise au point d'une formule qui aboutirait à exclure la responsabilité pour dommages indirects, conformément à la méthode adoptée dans la Loi type de la CNUDCI sur les virements internationaux, a recueilli une certaine approbation, mais l'on a aussi fait remarquer qu'elle pouvait ne pas convenir dans le cas des signatures numériques et des tiers authentificateurs. On a fait valoir que le dommage serait rarement le produit direct d'un acte tel que la délivrance d'un faux certificat, mais qu'il résulterait plutôt du fait

qu'un tiers se fierait à une signature numérique non fiable utilisant un tel certificat. Dans ces conditions, la plupart des dommages susceptibles de résulter des activités du tiers authentificateur pouvaient être considérés comme "indirects". Il a aussi été proposé d'utiliser l'élément "d'imprévisibilité" comme critère pour limiter la responsabilité du tiers authentificateur. On a estimé que le régime de responsabilité applicable aux vendeurs en vertu de la Convention des Nations Unies sur les contrats de vente internationale de marchandises pouvait être étudié plus avant en tant qu'élément de référence possible.

67. Considérant la diversité des formules proposées, le Groupe de travail a prié le Secrétariat d'établir un rapport succinct sur les régimes juridiques en vigueur et les méthodes utilisées pour limiter la responsabilité, en particulier dans le cadre des conventions internationales applicables au transport de marchandises et au transport de passagers. Ce rapport pourrait aussi traiter du régime de responsabilité établi par certaines législations nationales pour des catégories professionnelles assurant, pour les documents sur support papier, des fonctions analogues à celles envisagées pour les tiers authentificateurs.

Règles minima en matière de responsabilité

68. Il a été noté qu'à ce stade de ses délibérations, le Groupe de travail ne s'était pas prononcé sur la question de savoir si les tiers authentificateurs devaient demander l'homologation préalable d'une entité publique. Il a été proposé que, lorsqu'il reviendrait sur cette question en reprenant l'examen du projet d'article B, le Groupe de travail examine aussi la question de savoir si ladite entité serait subsidiairement responsable des actes du tiers authentificateur.

69. En ce qui concerne les paragraphes 1) et 2), le Groupe de travail a provisoirement conclu que le régime de responsabilité applicable au tiers authentificateur devait être fondé sur le principe de la dualité, c'est-à-dire prévoir que la responsabilité pourrait varier selon que le tiers authentificateur était tenu d'appliquer des normes imposées par une entité publique ou fonctionnait simplement sur la base de règles convenues entre particuliers.

70. Il a été suggéré que tout tiers authentificateur soit, lorsqu'il délivre un certificat, soumis à une obligation, qui pourrait être formulée comme suit :

> "Lorsqu'il délivre un certificat, tout tiers authentificateur signifie qu'il confirme :
>
> 1) Que le tiers authentificateur s'est conformé à toutes les conditions applicables prévues dans les présentes règles pour la délivrance des certificats et, si le tiers authentificateur a délivré ou autrement remis le certificat à toute personne qui se fie raisonnablement au certificat ou à une signature numérique vérifiable par la clef publique indiquée dans le certificat, que le détenteur désigné dans le certificat l'a accepté;
>
> 2) Que le détenteur désigné dans le certificat détient la clef privée correspondant à la clef publique indiquée dans le certificat;
>
> 3) Que la clef publique et la clef privée du détenteur sont appariées;
>
> 4) Que toutes les informations données dans le certificat sont exactes, sauf si le tiers authentificateur a déclaré dans le certificat [ou fait savoir par incorporation par référence dans le certificat] que l'exactitude de certaines informations n'est pas confirmée;
>
> et
>
> 5) Que, à la connaissance du tiers authentificateur, n'a été omis du certificat aucun fait matériel connu qui, s'il était connu, compromettrait la fiabilité des déclarations ci-dessus."

Il a été généralement reconnu que le libellé proposé était, dans une large mesure, acceptable quant au fond en tant que point de départ de futures discussions, en ce qu'il fixait des règles minima auxquelles les parties n'auraient pas le droit de déroger par voie d'accord privé. En particulier, aucune clause limitant la responsabilité du tiers authentificateur ne serait considérée comme couverte par la protection ou les avantages visés au titre des règles uniformes si elle était incompatible avec les conditions susmentionnées. S'agissant de la responsabilité d'un tiers authentificateur, le tiers authentificateur serait présumé responsable des conséquences de la délivrance d'un certificat, sauf s'il pouvait prouver qu'il avait satisfait aux conditions susmentionnées. Toutefois, si un tiers authentificateur voulait s'imposer des obligations plus strictes que celles qui étaient mentionnées plus haut, il devait être autorisé à le faire, soit en introduisant des clauses à cet effet dans sa déclaration des pratiques d'authentification, soit de toute autre manière.

71. Le Groupe de travail a convenu que les règles minima mentionnées plus haut devaient être applicables à la délivrance de certificats aux fins de l'authentification des signatures numériques, telles qu'elles étaient définies dans le projet d'article A. L'on s'est accordé à penser que le projet de règles uniformes ne devait pas porter sur d'autres activités ou services dont pourraient s'acquitter le tiers authentificateur. Ces activités et services pourraient être régis par des accords contractuels entre le tiers authentificateur et son client et par toute autre loi applicable (par exemple les règles impératives du droit relatives à l'acceptabilité des clauses d'exemption de responsabilité).

Paragraphes 3 et 4

72. Le Groupe de travail a estimé que les paragraphes 3 et 4 étaient généralement acceptables, quant au fond, en tant que point de départ de futures discussions. En ce qui concernait le paragraphe 3, l'on s'est accordé à penser qu'il fallait peut-être tenir compte du principe de la négligence concurrente lors de l'élaboration de la version révisée du projet d'article H, mais que la disposition énoncée au paragraphe 3 pourrait ne plus être nécessaire, puisque le Groupe de travail avait décidé que le régime de la responsabilité applicable aux tiers authentificateurs ne devait pas être fondé seulement sur la négligence. En ce qui concernait le paragraphe 4, il a été décidé de supprimer les mots "encourue par l'utilisateur" pour étendre la portée de la disposition aux pertes encourues par toute partie intéressée.

73. À l'issue du débat, le Groupe de travail a demandé au Secrétariat de préparer une version révisée du projet d'article H au vu des délibérations et décisions ci-dessus.

3. Questions ayant trait à la certification transfrontière

74. Pour l'examen des questions ayant trait à la certification transfrontière, le Groupe de travail s'est fondé sur le projet de disposition ci-après :

> "Projet d'article I
>
> 1) Les certificats émis par les tiers authentificateurs d'un autre pays peuvent être utilisés pour une signature numérique selon les mêmes modalités que les signatures numériques soumises [à la présente loi][aux présentes règles] s'ils sont reconnus par un tiers authentificateur homologué et que celui-ci garantit, à l'instar de ce qu'il fait pour ses propres certificats, que les détails figurant dans le certificat sont corrects et, en outre, que le certificat est valable et en vigueur.
>
> 2) ... [l'État qui édicte la loi choisit l'organe ou le tiers authentificateur chargé d'établir les règles relatives à l'approbation des certificats étrangers] est autorisé à approuver les certificats étrangers et à adopter des règles spécifiques régissant cette approbation."

75 Avant l'ouverture des débats sur les questions ayant trait à la certification transfrontière, il a été rappelé au Groupe de travail que, conformément au mandat que la Commission lui avait confié, il devait conseiller celle-ci quant au bien fondé et à la possibilité d'établir des règles uniformes relatives aux signatures numériques, aux tiers authentificateurs et aux questions connexes (voir par. 9 ci-dessus). Il n'était pas demandé au Groupe de travail, au

stade actuel, d'arrêter la version définitive d'un projet de texte qui serait soumis pour examen à la Commission à sa trentième session.

76. Les débats antérieurs du Groupe de travail concernant le rôle du tiers authentificateur dans le cadre du projet d'article B, en particulier les différentes vues exprimées sur la question de savoir si le tiers authentificateur devait obtenir l'agrément de l'État (voir par. 40 à 50 ci-dessus) ont également été évoqués. D'une manière générale le Groupe de travail a estimé qu'il serait en mesure de faire progresser les débats sur cette question après avoir examiné la question de la responsabilité du tiers authentificateur et celle ayant trait à la certification transfrontière. On a noté dans le même temps qu'une décision sur les questions soulevées par le projet d'article B aurait également des incidences sur le régime de certification transfrontière envisagé dans le projet de règles uniformes.

77. Sur le plan général, on a relevé que les paragraphes 1) et 2) abordaient la relation entre les certificats émis par les tiers authentificateurs locaux et ceux émis à l'étranger dans une optique légèrement différente. Le paragraphe 1) permettait à un tiers authentificateur local de garantir, à l'instar de ce qu'il faisait pour ses propres certificats, que les données figurant dans le certificat étranger étaient correctes et que ce dernier était valable et valide. Aux termes du paragraphe 2), l'organe ou l'autorité chargé d'homologuer les tiers authentificateurs dans l'État qui édicte la loi avait la possibilité de reconnaître les certificats étrangers émis par des tiers authentificateurs étrangers dans les conditions qu'il avait stipulées. Il a été indiqué que les questions traitées dans le paragraphe 1) pouvaient correspondre à une certification croisée tandis que le paragraphe 2) traitait de ce qui pourrait être plus précisément désigné comme une "reconnaissance transfrontière". Il serait préférable d'étudier ces différentes questions séparément.

78. On a émis l'opinion que les paragraphes 1) et 2) contenaient deux options différentes pour un éventuel régime de reconnaissance des certificats étrangers dans le cadre du projet de règles uniformes. Chacune des deux options a recueilli un certain appui. Mais, d'une manière générale, on a estimé qu'elles ne devaient pas nécessairement être considérées comme s'excluant mutuellement. Si certains participants souhaitaient que les paragraphes 1) et 2) fassent, quant au fond, l'objet de deux articles distincts, on a également préconisé que leurs champs d'application respectifs fassent l'objet d'un examen plus approfondi. Le paragraphe 1) contenait essentiellement une disposition relative à l'attribution des responsabilités du tiers authentificateur local au cas où le certificat étranger se révélerait défectueux, responsabilités qui découleraient du projet d'article H. Le paragraphe 2) en revanche ne traitait pas des questions de responsabilité, mais des effets juridiques qui pourraient découler directement d'un certificat étranger, par exemple la question de savoir si l'on pouvait se prévaloir d'un certificat étranger dans le cadre d'un différend porté devant les tribunaux de l'État qui édicte la loi. Ces effets juridiques n'étaient pas nécessairement fondés sur l'existence de la garantie envisagée au paragraphe 1), ni modifiés par elle.

79. Compte tenu de la décision prise par le Groupe de travail d'aborder dans l'élaboration du projet de règles uniformes non seulement la question des tiers authentificateurs homologués par des entités publiques mais également de tiers authentificateurs relevant du secteur privé (voir par. 48 à 50 ci-dessus), on s'est accordé à reconnaître que le projet d'article premier devrait traiter de la reconnaissance des certificats étrangers émis par les deux types de tiers authentificateurs.

80. Il a été proposé que le Groupe de travail examine également la question des conditions de reconnaissance des certificats étrangers. Celles-ci pourraient prendre la forme de prescriptions fixées par l'État, ou être prévues dans le cadre d'arrangements entre les tiers authentificateurs locaux et étrangers. Des précisions ont été apportées sur les modalités de structuration de ces arrangements qui pourraient être envisagées. On a rappelé que l'infrastructure à clef publique était souvent fondée sur divers niveaux d'autorité hiérarchique. Dans le cadre de ces structures hiérarchiques, il semblait probable que la certification croisée s'opérerait en deux stades. Le stade initial serait réservé exclusivement à une "autorité centrale" (qui homologuerait la technologie et les pratiques de toutes les parties autorisées à utiliser les paires de clefs et qui homologuerait les tiers authentificateurs subordonnés. Dans un deuxième stade, avec l'expansion de ce secteur, les tiers authentificateurs subordonnés placés sous l'autorité centrale pourraient être directement habilités à garantir que les certificats émis par les tiers authentificateurs étrangers étaient corrects. En élaborant les règles relatives aux questions de certification croisée, le Groupe de travail devait tenir compte de la nécessité éventuelle, en particulier en ce qui concerne les signatures numériques n'exigeant qu'un faible

degré de sécurité, d'assurer l'application des certificats étrangers en l'absence d'un accord entre les tiers authentificateurs. Il a donc été suggéré qu'il pourrait être nécessaire d'élaborer une norme supplétive permettant la reconnaissance des signatures numériques étrangères émises dans ces circonstances.

81. D'aucuns ont affirmé que l'inclusion de dispositions traitant des questions de reconnaissance transfrontière pouvait contribuer dans une large mesure à renforcer la fiabilité des certificats. Toutefois, le Groupe de travail devait examiner soigneusement les méthodes et procédures à appliquer concernant cette certification ou reconnaissance. De l'avis de certains, s'agissant de l'évaluation de la fiabilité d'un certificat étranger, le destinataire d'un message à signature numérique accompagné de ce certificat devait se poser un certain nombre de questions, notamment celles de savoir si le tiers authentificateur ayant délivré le certificat était autorisé à agir à l'étranger, si sa signature numérique était authentique, s'il existait des voies de recours contre lui, si la signature numérique avait été reconnue comme produisant des effets juridiques, et si elle pouvait être opposée à son auteur.

82. De ce point de vue, certains membres ont ajouté que la certification croisée pouvait globalement assurer quatre niveaux différents de fiabilité. Au niveau le plus élevé, le tiers authentificateur local, à la demande de la partie se fiant à un certificat étranger, garantirait la teneur dudit certificat sur la base de sa connaissance déclarée des procédures ayant abouti à la délivrance du certificat, assumant ainsi l'entière responsabilité de toute erreur ou de toute autre irrégularité dans le certificat. Au niveau immédiatement inférieur, le tiers authentificateur local garantirait la teneur d'un certificat étranger sur la base des informations reçues quant à la confiance à accorder au tiers authentificateur de l'autre pays. Un degré moindre de confiance serait atteint lorsque le tiers authentificateur local ne s'engagerait qu'à garantir que le tiers authentificateur de l'autre pays est digne de foi, sans assumer la responsabilité de la teneur du certificat étranger. Au niveau le plus bas, le tiers authentificateur local se bornerait à garantir l'identité du tiers authentificateur de l'autre pays, en vérifiant sa clef publique et sa signature numérique. Il a été recommandé que le Groupe de travail tienne compte du degré de sécurité recherché par le destinataire du message, lors de la formulation des dispositions relatives à la certification ou à la reconnaissance croisée des certificats étrangers.

83. À ce sujet, une comparaison a été faite entre la situation d'un tiers authentificateur garantissant qu'un certificat étranger est correct et valide et celle d'une institution financière garantissant une lettre de crédit émise par une banque étrangère. L'acceptabilité de la lettre de crédit par son destinataire dépendait de facteurs tels que la fiabilité de la banque étrangère émettant la lettre de crédit et son applicabilité dans le pays du destinataire. Dans certains cas, ce dernier pourrait insister pour obtenir une contre-garantie d'une banque locale. Le niveau adéquat de sécurité pour les transactions serait établi par le destinataire de la lettre de crédit, compte tenu du niveau de risque qu'il serait prêt à assumer. De même, une partie à une transaction impliquant l'utilisation d'un certificat étranger pourrait par exemple juger suffisant le fait de savoir que le certificat a été émis par un tiers authentificateur de l'autre pays dont la valeur est connue, sans juger nécessaire d'obtenir une garantie d'un tiers authentificateur local. Certains membres ont déclaré craindre que le projet d'article I ne soit perçu comme décourageant ou entravant l'utilisation de certificats non garantis par un tiers authentificateur local, même dans le cas de transactions où les parties se satisferaient d'un degré de sécurité ou de certitude juridique moindre. Il était important de faire en sorte que le projet d'article I traite les questions de certification croisée ou de reconnaissance transfrontière sans rigorisme.

84. En ce qui concernait la comparaison mentionnée plus haut entre le rôle des tiers authentificateurs et celui des banques dans le contexte de transactions relatives à l'émission de lettres de crédit, les membres du Groupe ont généralement estimé que, s'agissant de l'élaboration de règles uniformes pour la reconnaissance des certificats, il convenait de garder à l'esprit le fait que les signatures numériques pouvaient être utilisées non seulement pour le transfert de droits mais également pour le transfert d'obligations, notamment dans le cas où une signature numérique était apposée à une notice relative à une cession de créance. C'est pourquoi le risque résultant de l'acceptation d'une signature numérique devait peut-être être assumé par le bénéficiaire ou par son auteur, suivant le type de transaction en question.

85. En ce qui concernait le champ éventuel de la certification et de la reconnaissance croisées, d'aucuns ont affirmé que, dans une certaine mesure, les fonctions remplies par le tiers authentificateur étaient analogues à celles d'un notaire dans certains régimes juridiques. En fait, dans divers systèmes juridiques, certains types de transactions

exigeaient qu'un notaire ou toute autre personne assumant des fonctions analogues certifie certains faits (par exemple, l'identité de l'une des parties) ou éléments de la transaction (par exemple, la signature des parties ou l'authentificité d'un document). Toutefois, les transactions pour lesquelles il était exigé une certification par notaire variaient suivant les régimes juridiques et il serait impossible de tenter d'harmoniser les solutions nationales concernant les formalités à accomplir pour les principales transactions.

86. On a estimé que la reconnaissance des certificats étrangers serait souvent réciproque et que le pouvoir d'accorder cette reconnaissance découlerait donc d'accords bilatéraux ou multilatéraux internationaux. On a d'autre part émis des réserves quant à l'idée de faire référence à cette réciprocité dans des projets de règles uniformes, étant donné la diversité des acceptions du terme "réciprocité" dans les différents droits nationaux. La proposition tendant à faire référence à des accords bilatéraux ou multilatéraux internationaux, d'autre part, a suscité des réactions diverses. À l'appui de cette suggestion, on a fait observer qu'une telle mention permettrait d'indiquer clairement que les projets de règles uniformes n'affecteraient pas les obligations internationales que les États pourraient avoir à assumer, par exemple, dans le cadre d'accords régionaux d'intégration ou de coopération économique. Cependant, on a indiqué aussi qu'aucune référence précise à de tels accords n'était nécessaire, étant donné que rien, dans le paragraphe 1 du projet d'articles, n'empêchait l'État qui édicte la loi d'organiser une authentification mutuelle ou une reconnaissance mutuelle de certificats étrangers par le biais de tels accords. On a suggéré en outre qu'au lieu de mentionner des accords internationaux dans le projet d'article premier, le Groupe de travail devait envisager de formuler des règles de fond en vue de la reconnaissance des certificats étrangers. On a déclaré qu'une référence à des accords bilatéraux ou multilatéraux internationaux dans le contexte de l'article premier devrait être évitée à moins que : a) le Groupe de travail ne parvienne à la conclusion qu'il n'était pas possible d'établir des règles harmonisées de reconnaissance, ou, b) qu'une telle indication ne renvoie à des accords prévoyant un niveau plus satisfaisant de reconnaissance des certificats étrangers que ceux découlant des projets de règles uniformes.

87. On a fait observer que les paragraphes 1) et 2) de l'article premier comportaient deux options différentes, pour l'État qui édicte la loi, selon que le tiers authentificateur était ou non assujetti à une approbation gouvernementale préalable. Cependant, on a estimé que, lu conjointement avec le projet d'article B, rendant nécessaire l'approbation préalable de l'État qui édicte la loi, le paragraphe 1 pourrait être conçu comme permettant la reconnaissance des certificats émis par les tiers authentificateurs étrangers qui n'auraient pas été autorisés à opérer selon les règles nationales, tout en déniant tout effet juridique aux certificats émis par les tiers authentificateurs nationaux qui n'auraient pas reçu l'autorisation nécessaire de l'État qui édicte la loi. À cet égard, on s'est demandé si l'objet du projet d'article premier était de rendre possible, pour un tiers authentificateur habilité par les autorités à étendre l'effet juridique aux certificats émis par d'autres autorités, nationales ou étrangères, non soumises à l'obligation d'autorisation gouvernementale préalable. Si c'était bien là l'intention, le projet d'article premier pourrait devoir être révisé en fonction de la décision que prendrait le Groupe de travail s'agissant du projet d'article B.

88. En ce qui concernait la garantie prévue au paragraphe 1, on a fait observer que, dans certaines législations nationales, il était difficile de résoudre ce problème par une disposition de portée générale, sans avoir à ajouter des dispositions plus détaillées étant donné que les garanties fournies par le tiers authentificateur pouvaient varier considérablement d'un pays à l'autre. Les tiers authentificateurs nationaux auraient alors quelque difficulté à assumer la responsabilité des certificats émis à l'étranger, faute d'une entente concernant le type de garantie offert.

89. Après avoir examiné les différentes opinions exprimées, le Groupe de travail s'est accordé à penser qu'il était indiqué de traiter des problèmes de l'authentification internationale dans les projets de règles uniformes. Si les principes consignés au projet d'article premier étaient généralement considérés comme acceptables, il demeurerait prématuré de tenter de formuler des dispositions détaillées sur ces problèmes, à ce stade encore très précoce de ses délibérations. Le Secrétariat a été invité à réviser le projet d'article premier, en tenant compte de ces considérations et de la nécessité de distinguer entre les tiers authentificateurs soumis à autorisation gouvernementale et les autres. Le Secrétariat a été invité à distinguer entre les conditions et les effets de la reconnaissance d'une signature numérique et d'un certificat, d'une part, et la reconnaissance d'un tiers authentificateur de l'autre, et de formuler les propositions appropriées, comportant éventuellement des variantes, pour résoudre ces différents problèmes.

1. Définitions (suite)

b) Tiers authentificateurs homologués (suite)

90. Ayant achevé l'examen préliminaire des questions ayant trait à la responsabilité et à la certification croisée dans le cadre des projets d'articles H et I, le Groupe de travail a repris ses délibérations sur les questions posées par la définition du tiers authentificateur dans le cadre du projet d'article B (voir par. 40 à 49 ci-dessus). On a rappelé que, pour que soient prises en compte et la situation où les tiers authentificateurs opéraient dans un cadre strictement privé et celle où ces entités devaient être autorisées ou homologuées par les autorités publiques avant de pouvoir opérer, le Groupe de travail avait décidé d'adopter, à titre préliminaire, une démarche double (voir par. 48 à 50 ci-dessus), qui semblait impliquer la nécessité d'une définition large du tiers authentificateur, couvrant les deux types de situation. L'on a fait valoir à cet égard que le Groupe de travail pouvait envisager la possibilité de remplacer, dans le texte anglais, l'expression de "certification authority" par "certification entity", afin d'éviter que l'on puisse en déduire que les fonctions d'authentification incombaient nécessairement à des autorités publiques. Cette suggestion a recueilli un certain appui mais il a été rappelé que la première expression était déjà largement utilisée par des entités tant publiques que privées. Il a été instamment demandé au Groupe de travail de faire preuve de prudence à l'égard de toute terminologie qui pouvait aller à l'encontre de la pratique qui était en train de se constituer en matière d'authentification.

91. On a fait remarquer que les dispositions qui figuraient dans le projet d'article B couvraient divers aspects de la question des tiers authentificateurs. Si certains paragraphes, comme le paragraphe 3), relevaient exclusivement de la définition, d'autres dispositions, celles du paragraphe 4), par exemple, étaient plus opérationnelles et décrivaient les fonctions accomplies par les tiers authentificateurs. D'aucuns ont donc estimé qu'il fallait peut-être subdiviser le projet d'article B en deux articles différents traitant, respectivement, de la définition et des fonctions des tiers authentificateurs. L'on a généralement estimé qu'en cas de remaniement du projet d'article B, il convenait peut-être de mentionner d'autres tâches que le datage, telles que la délivrance de paires de clefs, la tenue de répertoires et la conservation des archives, qui ont été qualifiées d'"auxiliaires" par rapport aux fonctions principales exercées par les tiers authentificateurs en matière de signatures numériques. Toutefois, de l'avis général, la prise en compte de ces services auxiliaires ne devait pas élargir la portée des règles uniformes telle qu'elle était définie par référence aux signatures numériques dans le projet d'article A.

92. L'on a avancé que, pour établir la distinction entre les régimes juridiques applicables aux tiers authentificateurs autorisés ou de quelque autre manière homologués par l'État et ceux applicables aux tiers authentificateurs non homologués, l'on pourrait notamment préciser dans le projet de règles uniformes les effets juridiques susceptibles de découler de la délivrance des certificats par les tiers authentificateurs homologués. En réponse à une question portant sur ceux susceptibles de découler de la délivrance de certificats par des tiers authentificateurs non homologués, il a été dit qu'il suffisait de renvoyer à l'article 7 de la Loi type. Cette proposition a recueilli un certain soutien mais on a estimé qu'il convenait peut-être que les règles uniformes explicitent les effets juridiques réalisés par les certificats émanant de tiers authentificateurs purement privés. Selon une autre proposition, la distinction entre les tiers authentificateurs homologués et ceux qui ne l'étaient pas pourrait se fonder sur les différentes fonctions qui pouvaient être accomplies par les uns et les autres. L'on a de manière générale estimé que ces questions méritaient peut-être d'être examinées plus avant, lors d'une session ultérieure du Groupe de travail.

93. Dans le cadre de l'examen du paragraphe 3), la question a été posée de savoir si le membre de phrase "clefs cryptographiques de personnes physiques ou morales" était suffisamment éclairante dans les situations où les clefs cryptographiques étaient délivrées directement à des dispositifs électroniques, ou utilisées par de tels dispositifs, sans intervention humaine directe. Le Groupe de travail a rappelé que la question avait été examinée lors de l'élaboration de la Loi type et, de l'avis général, nécessitait peut-être d'être examinée plus avant à un stade ultérieur, en même temps que les questions relatives aux signatures numériques.

94. S'agissant de la forme que pouvait prendre la révision du projet d'article B, l'attention du Groupe de travail a été appelée sur la méthode suivie dans le cas de la Loi type, qui associait aux dispositions légales un guide pour l'incorporation de ces dispositions au droit interne. Cette méthode permettait d'entrer dans le détail et d'illustrer les

dispositions adoptées, facilitant ainsi leur examen ultérieur par les législateurs. Il a été proposé de faire de même à propos des règles uniformes. S'agissant en particulier des diverses fonctions accomplies par les tiers authentificateurs, il y avait lieu d'inclure des éléments d'explication dans le cadre d'un guide du type susmentionné. Tout en remettant à plus tard sa décision quant à la forme finale des règles uniformes, le Groupe a jugé cette proposition généralement acceptable comme hypothèse de travail.

95. À l'issue des discussions, le Groupe de travail a décidé que les dispositions du projet d'article B devaient faire l'objet de deux articles distincts, dont l'un contiendrait une définition étoffée du tiers authentificateur et l'autre traiterait des fonctions accomplies par le tiers authentificateur. Il a été décidé que la définition générale du tiers authentificateur devait reposer sur le texte du paragraphe 3) du projet d'article B. Il a été aussi convenu qu'à l'expression "personnes physiques ou morales" devaient s'ajouter les mots "dispositifs électroniques", qui seraient placés entre crochets en attendant que le Groupe de travail se penche sur ce point. Outre une définition générale du tiers authentificateur, l'article définitoire révisé devait aussi définir le tiers authentificateur "autorisé", "homologué" ou "accrédité", en se fondant sur le paragraphe 1) du projet d'article B. Quant aux éléments figurant dans les paragraphes 2) et 5) du même projet d'article, ils devaient apparaître dans le chapitre du guide qui correspondrait à la définition des tiers authentificateurs "homologués".

96. De l'avis général, l'article distinct qui traiterait des diverses fonctions accomplies par les tiers authentificateurs pouvait se fonder sur le paragraphe 4) du projet d'article B. Il a été également convenu qu'il faudrait sans doute élargir la portée de ce futur article afin d'y inclure d'autres fonctions. Des éléments à cet effet pouvaient être tirés de textes de loi existants, de directives et de contrats types en vigueur ou envisagés concernant cette profession. Sur le plan de la formulation, on a généralement estimé qu'il fallait sans doute modifier le membre de phrase "communications protégées au moyen de signatures numériques" du paragraphe 4) afin d'éviter que l'on puisse en tirer des conséquences particulières quant à l'acceptabilité des méthodes de protection utilisées par les tiers authentificateurs.

97. Le Secrétariat a été prié de réviser le projet d'article B au vu des délibérations et décisions ci-dessus.

c) Certificats

98. Pour l'examen des questions ayant trait à la définition des certificats, le Groupe de travail s'est fondé sur le projet de dispositions ci-après :

"Projet d'article C

Le certificat délivré par le tiers authentificateur homologué, sous forme de message de données ou autrement, indiquera au minimum les éléments suivants :

a) Nom de l'utilisateur [et adresse ou adresse professionnelle];

b) [Date de naissance de] [suffisamment d'éléments permettant d'identifier] l'utilisateur si celui-ci est une personne physique;

c) si l'utilisateur est une personne morale, nom de la société et tout renseignement pertinent permettant d'identifier cette société;

d) Nom, adresse et siège du tiers authentificateur;

e) Clef cryptographique publique de l'utilisateur;

f) Toute information nécessaire indiquant la manière dont la clef cryptographique publique de l'utilisateur peut être vérifiée par le destinataire de la signature numérique donnée conformément au certificat;

g) Numéro de série du certificat; et

h) [Date de délivrance et date d'expiration] [période de validité] du certificat."

99. Il a été rappelé d'emblée au Groupe de travail que, lorsqu'il avait examiné la définition du tiers authentificateur, il avait décidé de faire preuve de souplesse et de prendre en considération, comme hypothèse de travail, les certificats délivrés aussi bien par les tiers authentificateurs homologués par les pouvoirs publics que par les tiers authentificateurs opérant en dehors de l'infrastructure à clef publique régie par les pouvoirs publics, en n'écartant pour le moment aucune de ces deux possibilités. En conséquence, le mot "homologué" figurant dans le texte introductif du projet d'article C devait être supprimé.

100. Des observations d'ordre général ont été formulées au sujet de la terminologie employée dans le projet d'article C, en particulier au sujet de l'emploi du mot "utilisateur" pour désigner le détenteur de la clef privée d'une paire de clefs cryptographiques. "L'utilisateur", a-t-on estimé, risquait d'être confondu avec le destinataire d'un message, qui pouvait être considéré comme étant "l'utilisateur" du certificat ou de la clef publique utilisée pour vérifier la signature numérique. Plusieurs formules de remplacement ont été suggérées, notamment les expressions "possesseur de la paire de clefs", "détenteur du certificat", "détenteur de la clef privée". Il a été décidé que le Secrétariat devait examiner la terminologie utilisée dans le projet d'article C et dans les autres dispositions du projet de règles uniformes, de sorte à proposer des formules écartant toute ambiguïté.

101. L'on s'est accordé à penser qu'il fallait que le projet d'article C donne une définition du "certificat" avant d'indiquer les éléments qui devaient y figurer. Il a été proposé de le définir à peu près comme suit : "Un certificat est un message de données, qui se présente comme étant un certificat, désigne le tiers authentificateur, contient la clef publique de l'utilisateur, donne le nom de l'utilisateur et porte la signature numérique du tiers authentificateur". Il a été proposé aussi que la définition reprenne les éléments donnés dans une note du Secrétariat, à savoir qu'un certificat est un enregistrement électronique qui précise la clef publique ainsi que le nom du détenteur du certificat comme "sujet" du certificat et qui peut confirmer que le signataire éventuel identifié dans le certificat détient la clef privée correspondante (A/CN.9/WG.IV/WP.71, par. 36). Il a été jugé qu'une définition de cette nature serait généralement acceptable. Il fallait toutefois y spécifier que, si le certificat était transmis par voie électronique, le tiers authentificateur devait le signer numériquement pour assurer l'authenticité tant de son contenu que de sa source.

102. Il a été demandé si les mots "au minimum" concernant les éléments devant figurer dans le certificat signifiaient qu'un certificat qui ne contenait pas toutes les informations énumérées dans le projet d'article C ne serait pas considéré comme tel au sens du projet de règles uniformes. Il a été répondu que, tel qu'il était actuellement rédigé, le projet d'article C indiquait un certain nombre d'éléments obligatoires que le certificat devait contenir pour être considéré comme tel au sens du projet de règles uniformes. Il a été suggéré que, par souci de clarté, la définition du certificat fasse l'objet d'une disposition indépendante et que les informations à fournir dans un certificat soient indiquées dans une disposition distincte.

103. Le Groupe de travail s'est penché sur les éléments d'information devant figurer dans les certificats. À titre d'observation générale, on a fait valoir qu'il fallait réduire autant que faire se pouvait les éléments obligatoires et les limiter à l'information essentielle pour que l'utilisateur du certificat soit en mesure de vérifier la signature numérique utilisée dans un message de données. On a invoqué à cet égard le risque que l'inclusion d'éléments superflus parmi ceux devant figurer dans le certificat n'exclue sans qu'on le veuille du champ d'application du projet de règles uniformes un certain nombre de certificats qui, sinon, auraient suffi aux fins pour lesquelles ils avaient été délivrés. Selon un point de vue, il importait de garder à l'esprit la différence entre l'information figurant dans le certificat et les mesures que le tiers authentificateur devait prendre pour vérifier l'exactitude de cette information. Plus le certificat contenait d'informations, plus la responsabilité du tiers authentificateur risquait d'être engagée. Il a donc été proposé que le projet de règles uniformes n'établisse aucune condition minimale quant au contenu du certificat.

104. Une autre démarche a été proposée, renvoyant à l'examen de la question de la responsabilité du tiers authentificateur, dans le cadre duquel il avait été entendu qu'en cas d'identification erronée d'une personne ou d'attribution erronée d'une clef publique à une personne, le tiers authentificateur assumerait la responsabilité de la

perte subie par toute partie lésée, à moins qu'il ne prouve qu'il avait fait tout ce qui était en son pouvoir pour éviter l'erreur (voir par. 58 ci-dessus). De l'avis général, il était vain d'essayer de protéger l'utilisateur final en exigeant du tiers authentificateur qu'il prenne des dispositions suffisantes pour établir l'exactitude de l'information, ou pour identifier convenablement les détenteurs de clefs privées si, dans le même temps, on permettait au tiers authentificateur de contourner cette responsabilité en délivrant des certificats qui contenaient moins que l'information minimale requise.

105. On a fait valoir que, si le certificat devait remplir un certain nombre de conditions obligatoires quant à son contenu, le tiers authentificateur n'aurait plus la possibilité de contourner sa responsabilité de la manière qui vient d'être décrite. On a rappelé à cet égard que lors de l'examen des questions ayant trait à la responsabilité du tiers authentificateur, une proposition avait été avancée tendant à ce que tout tiers authentificateur soit tenu, lorsqu'il délivre un certificat, de signaler qu'il a vérifié un certain nombre d'éléments (voir par. 70 ci-dessus). Cette proposition a été fortement approuvée. Après examen, le Groupe de travail est convenu que la question ne pouvait pas être étudiée à fond à la session en cours. Il a été décidé que les délibérations à ce sujet devaient reprendre à la première occasion, le Secrétariat devant établir à cet effet des variantes reflétant le débat ci-dessus.

106. S'agissant, en particulier, des données qui pouvaient être requises pour identifier le détenteur de la clef privée, il a été proposé de regrouper en une disposition unique les alinéas a), b), et c). On a relevé à cet égard que dans bien des pays, les renseignements concernant, par exemple, la date de naissance d'une personne étaient protégés au titre de l'inviolabilité de la vie privée et que des règles spécifiques pouvaient régir leur divulgation par voie électronique. Il a donc été proposé de ne pas exiger que le certificat contienne des renseignements personnels de cet ordre. Mais il a été déclaré aussi que, dans certaines circonstances, une personne qui demandait la délivrance d'un certificat pouvait être disposée, voire avoir intérêt, à communiquer certains types de renseignements personnels ou de sources d'information supplémentaires. Le projet de règles uniformes ne devait pas exclure ce cas de figure lorsque la divulgation librement consentie de données personnelles ne contrevenait ni aux règles applicables à la protection des données ni à la politique des autorités de l'État où la demande de délivrance du certificat avait été faite ou bien où le certificat avait été délivré. On a, de manière générale, estimé que les questions relatives à l'inviolabilité de l'information ne relevaient pas du champ d'application du projet de règles uniformes et que la seule chose que le projet d'article C pouvait exiger était que les éléments jugés suffisants aux fins de l'identification soient conformes aux lois régissant le caractère secret des données.

107. Il a été proposé que les éléments visés à l'alinéa a) soient "le nom ou l'identificateur" de l'utilisateur, afin de couvrir aussi les situations où l'utilisateur était identifié non par un nom mais par d'autres éléments, par exemple un numéro de compte, ce qui pouvait être le cas des certificats relatifs à des opérations par carte de crédit. En objection à cette proposition, on a fait valoir qu'elle pouvait encourager l'utilisation de messages et de certificats anonymes, ce qui ne serait pas conforme au souci de promouvoir une plus grande sécurité juridique dans le commerce électronique. Le Groupe de travail a été instamment prié de maintenir la mention du nom du détenteur de la clef privée au nombre des éléments essentiels du certificat.

108. Pour faire en sorte que le détenteur de la clef privée soit convenablement identifié, il a été proposé de retenir dans le projet d'article C la mention d'éléments supplémentaires d'identification tels que l'adresse, dans le cas d'une personne physique, ou le numéro d'enregistrement, dans le cas des personnes morales, le nom d'une personne ou d'une société ne pouvant seul suffire à identifier ladite personne ou société.

109. Selon un point de vue, l'utilisation d'une signature numérique pouvait dans certains cas être limitée à certains types d'opérations, par exemple lorsque le pouvoir qu'avait le signataire d'engager la société au nom de laquelle l'opération était effectuée était limité. Il a donc été proposé que le certificat donne des renseignements sur les restrictions ou limitations de cet ordre, ou mentionne leur source. En réponse à cette suggestion, on a relevé que la question des limites dans lesquelles on pouvait se fier à une signature numérique posait un certain nombre de problèmes juridiques complexes, qui n'étaient pas l'apanage du commerce électronique. S'agissant de documents sur support papier, il n'était pas toujours obligatoire qu'une signature manuscrite soit accompagnée d'une déclaration sur les limites éventuelles des pouvoirs du signataire. Le Groupe de travail a été engagé à ne pas introduire, dans

le cadre des signatures numériques, des exigences plus contraignantes que celles appliquées aux signatures manuscrites.

110. On a rappelé que le Groupe de travail avait déjà examiné les questions ayant trait aux consommateurs et à la responsabilité du tiers authentificateur ainsi qu'aux éventuelles limites ou exclusions de responsabilités en application du droit interne ou de la déclaration sur la pratique en matière d'authentification du tiers authentificateur. Il a été proposé que celui-ci soit tenu de déclarer ces limites ou de mentionner un document accessible à l'utilisateur, lorsque de telles limites pouvaient exister. Il a aussi été proposé que le projet de règles uniformes précise les conséquences pouvant découler de l'absence de cette indication dans le certificat. Dans le même ordre d'idées, il a été proposé que, lorsque la période de validité d'un certificat était limitée, cette limite soit indiquée sur le certificat, sous la forme d'une date d'expiration ou d'une durée de validité. On a jugé important, pour la protection des utilisateurs, que ceux-ci soient informés de la validité des certificats qu'ils utilisaient et qu'ils n'aient pas à courir le risque qu'un certificat soit délivré sans cette indication. Le projet de règles uniformes devait donc prévoir une règle supplétive définissant la durée de validité applicable en l'absence d'indications expresses. L'on a toutefois fait remarquer que l'existence d'une telle clause devait être interprétée comme signifiant que le tiers authentificateur avait la faculté d'omettre de mentionner la durée de validité du certificat.

111. Des questions ont été posées à propos du type d'information que le tiers authentificateur était en mesure de fournir sous une forme accessible à ceux qui utilisaient ses services compte tenu des technologies actuelles. Il a été répondu, qu'à l'heure actuelle, le tiers authentificateur pouvait apposer ou adjoindre des renseignements supplémentaires aux certificats qu'il délivrait, par exemple une déclaration de ses pratiques d'authentification ou les renseignements facultatifs communiqués à cet effet par les détenteurs de clefs privées. Toutefois, de nombreux systèmes informatiques actuellement utilisés par les clients n'étaient pas suffisamment sophistiqués pour leur permettre d'accéder à toute cette information. Abstraction faite des difficultés techniques de cet ordre, il importait de garder à l'esprit que certains des renseignements qui pouvaient être adjoints aux certificats pouvaient émaner des détenteurs de clefs privées et être communiqués sur leur demande. Il était important dans ce cas de distinguer les éléments du certificat qui étaient authentifiés par le tiers authentificateur (identité du détenteur de la clef privée, par exemple) et d'autres éléments émanant des clients du tiers authentificateur et n'étaient pas vérifiés par ce dernier (limites à l'utilisation des clefs privées dans une société, par exemple). Le tiers authentificateur ne devait pas être tenu responsable de l'exactitude de ces derniers renseignements.

112. Dans diverses interventions, on a fait valoir que, sans préjudice des autres éléments d'information qu'il pouvait fournir à ses clients, le tiers authentificateur devait signaler et garantir qu'il avait vérifié l'exactitude et l'exhaustivité des éléments d'information dont la présence sur le certificat était obligatoire.

113. Après avoir examiné les points de vue exprimés à propos du projet d'article C, le Groupe de travail est convenu qu'il fallait ajouter audit article une définition du certificat. Le contenu obligatoire du certificat devait faire l'objet d'une disposition distincte, qui devait traiter aussi des conséquences de l'absence de ces éléments obligatoires. Cette disposition devait reprendre les éléments visés aux alinéas a), b) et c), regroupés en une seule disposition révisée, et comprendre aussi les éléments d'information visés aux alinéas d), e) et h) du projet d'article C. On a par contre estimé que les renseignements visés à l'alinéa f) ne se prêtaient pas à une authentification par des tiers et, en conséquence, il a été convenu de supprimer ledit alinéa. Il a été également convenu que l'alinéa g) devait être placé entre crochets et examiné à un stade ultérieur en tant qu'élément facultatif, l'identification par un numéro de série n'étant peut-être pas possible pour tous les certificats. Le texte révisé du projet d'article C devait mentionner expressément l'applicabilité aux éléments d'information contenus dans le certificat de la loi interne relative à l'inviolabilité des données. Le Secrétariat a été prié de réviser le projet d'article C de sorte à indiquer, sous forme de variantes, les différents points de vue exprimés au sein du Groupe de travail et les conclusions auxquelles celui-ci était parvenu.

4. Signature par des personnes morales ou physiques

114. Pour l'examen des questions ayant trait à la signature par des personnes morales et physiques, le Groupe de travail s'est fondé sur le projet de dispositions ci-après :

"Projet d'article D

1) Les personnes physiques comme les personnes morales peuvent obtenir la certification de clefs publiques utilisées exclusivement aux fins d'identification.

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

115. Un certain nombre de participants se sont accordés à penser qu'il conviendrait de supprimer le projet d'article D. On a déclaré qu'il était inopportun d'établir une distinction entre personne morale et personne physique aux fins des signatures numériques étant donné qu'aucune distinction de ce genre n'était faite dans la Loi type, où la notion de "personne" recouvrait aussi bien les personnes physiques que les personnes morales. De plus, il a été souligné que le paragraphe 2) pourrait fâcheusement porter atteinte à d'autres éléments du droit, par exemple au droit sur la représentation, ainsi qu'aux dispositions du droit des sociétés concernant la représentation de ces dernières par des personnes physiques. Par ailleurs, la règle énoncée au paragraphe 2) paraissait imposer aux utilisateurs de signatures numériques une contrainte qui allait au-delà des prescriptions actuellement applicables aux signatures manuelles.

116. On a toutefois exprimé l'opinion que le projet d'article D — et tout spécialement le paragraphe 2) — avait son utilité. En particulier, lorsqu'aucune autre règle de droit applicable ne précisait la forme sous laquelle une signature obligatoire pouvait être donnée au nom d'une personne morale, une règle supplétive s'inspirant du paragraphe 2) pourrait fournir des indications utiles quant aux circonstances dans lesquelles il serait possible d'accorder foi à une signature numérique censée être celle d'une personne morale. Un appui a été exprimé en faveur du maintien du paragraphe 2) à condition que la disposition soit remaniée de façon à indiquer clairement que, bien qu'il soit fait référence à une "personne physique autorisée à agir au nom" d'une personne morale, il n'était nullement prévu de remplacer le droit interne sur la représentation. La question de savoir si la personne physique avait en fait et en droit l'autorité d'agir au nom de la personne morale continuerait ainsi à relever des règles juridiques appropriées indépendamment des règles uniformes.

117. Après délibération, le Groupe de travail a décidé de mettre entre crochets le projet d'article D afin d'en poursuivre l'examen lors d'une session ultérieure.

5. Affectation des messages de données à signature numérique

118. Pour l'examen de cette question, le Groupe de travail s'est fondé sur le projet de dispositions ci-après :

"Projet d'article E

1) L'expéditeur d'un message de données sur lequel est apposée la signature numérique de l'expéditeur est lié par le contenu du message de la même manière que si celui-ci était signé [à la main] conformément au droit applicable au contenu du message.

2) Le destinataire d'un message de données sur lequel est apposée une signature numérique est en droit de considérer que le message de données provient bien de l'expéditeur, et d'agir sur la foi de cette présomption si :

a) Afin de s'assurer que le message de données est bien celui de l'expéditeur, le destinataire a appliqué correctement la clef publique de l'expéditeur au message de données tel que reçu et que l'application de la clef publique de l'expéditeur a permis de conclure : que le message de données reçu

avait été chiffré à l'aide de la clef privée de l'expéditeur; et que le message initial n'a pas été altéré après avoir été chiffré à l'aide de la clef publique de l'expéditeur;

ou

b) Le message de données tel que reçu par le destinataire résulte des actes d'une personne dont les relations avec l'expéditeur ou un agent de celui-ci ont permis à cette personne d'avoir accès à la clef cryptographique privée de l'expéditeur.

3) Le paragraphe 2) n'est pas applicable :

a) Dès lors que le destinataire savait, ou aurait dû savoir s'il s'était renseigné auprès du tiers authentificateur ou s'il avait pris des précautions raisonnables, que la validité de la clef cryptographique publique de l'expéditeur avait expiré ou que le certificat émis par le tiers authentificateur avait été annulé ou suspendu;

ou

b) Dans un cas relevant de l'alinéa b) du paragraphe 2), lorsque le destinataire savait ou aurait dû savoir, s'il avait pris des précautions raisonnables ou utilisé une procédure convenue, que le message de données n'émanait pas de l'expéditeur."

119. L'on a avancé que l'article E ne s'imposait pas, car ce n'était qu'une réplique, adaptée à l'espèce considérée, de l'article 13 de la Loi type et il pourrait y avoir une certaine confusion quant aux articulations éventuelles entre ces deux ensembles de dispositions. En outre, il risquait de paraître se substituer aux dispositions de loi applicables à l'opération à laquelle se rapportait la signature numérique — par exemple, on risquait de considérer que la disposition du premier paragraphe, qui établissait que l'expéditeur d'un message de données était "lié par le contenu du message", empiétait à tort sur le droit général des obligations.

120. Le plus grand nombre s'est accordé à penser que ce projet d'article, s'il devait sans doute être remanié dans sa formulation, énonçait en son premier paragraphe un principe utile qui établissait l'effet juridique de la signature numérique. On a proposé de libeller ce paragraphe de façon à poser comme présomption absolue que le détenteur d'une signature numérique serait réputé être le signataire du message de données auquel la signature était apposée.

121. S'agissant de l'éventuel recours à la présomption, absolue ou non, pour l'attribution des messages, on a proposé de distinguer entre les types d'opérations où intervenait la signature numérique. Par exemple, il ne fallait pas soumettre à la même règle les opérations purement commerciales entre partenaires qui traitaient depuis longtemps entre eux et les déclarations d'impôts adressées aux administrations publiques.

122. On a ainsi pensé qu'il fallait peut-être, dans une disposition rédigée dans l'esprit du premier paragraphe, distinguer entre différents types de signature numérique (par exemple considérer les degrés respectifs de sécurité assurés par les divers algorithmes et la variation correspondante du coût de la signature) et entre les circonstances dans lesquelles ces signatures étaient employées. On a suggéré, pour remanier le premier paragraphe, de prendre en compte les éléments suivants : la signature numérique se rapportait-elle à un contrat préalable entre les parties ? S'inscrivait-elle dans un cadre contractuel ? Y avait-il établissement d'un certificat d'authentification par un tiers authentificateur non homologué ou par un tiers autorisé ? On a aussi pensé, en évoquant les divers degrés de risque que pouvait entraîner le système de la signature numérique en cas de fraude, qu'il fallait s'occuper tout particulièrement de l'éventualité où la fraude précédait l'établissement de la paire de clefs. En pareil cas, si les parties ne parvenaient pas à s'accorder, l'on a avancé qu'il incombait au destinataire d'établir le lien entre la signature et l'expéditeur. Si un certificat en bonne et due forme avait été délivré, la charge de la preuve pourrait être inversée. Selon d'autres, c'était à la partie qui désignait le tiers authentificateur d'assumer le risque que pouvait comporter l'usage des certificats délivrés par ce tiers.

123. Mais on s'est aussi demandé s'il fallait vraiment considérer tous ces cas, en rappelant en particulier que, lors du débat sur la responsabilité, le Groupe de travail avait décidé de s'en tenir à ceux où un certificat était délivré. De l'avis général, cependant, il ne fallait pas perdre de vue l'ensemble de ces éventualités, ou du moins certaines d'entre elles, lors du remaniement de l'article E, dont le texte révisé serait examiné à une session ultérieure.

124. Le Groupe de travail a décidé, après en avoir débattu, qu'il lui fallait examiner plus avant une disposition révisée concernant l'affectation des messages de données à signature numérique, disposition qui pourrait reprendre l'esprit du premier paragraphe du projet d'article E. On s'est accordé à penser que des commentaires ne seraient sans doute pas superflus pour clarifier les articulations entre ce texte et les articles 7 et 13 de la Loi type. Il a été demandé au Secrétariat de remanier l'article E, en proposant des variantes qui indiqueraient les positions consignées ci-dessus.

6. Annulation de certificats

125. Pour l'examen des questions ayant trait à l'annulation de certificats, le Groupe de travail s'est fondé sur le projet de dispositions ci-après :

> "Projet d'article F
>
> 1) Le détendeur d'un couple certifié de clefs peut annuler le certificat correspondant. L'annulation joue dès l'instant où elle est [enregistrée] [reçue] par le tiers authentificateur.
>
> 2) Le détenteur d'un couple certifié de clefs est tenu d'annuler le certificat correspondant lorsqu'il apprend que la clef cryptographique privée a été perdue, compromise ou risque d'être utilisée à mauvais escient à d'autres égards. Si le détenteur n'annule pas le certificat dans une telle situation, il est responsable de toute perte encourue par des tiers s'étant fiés au contenu des messages du fait que le détenteur a failli à son obligation d'annuler le certificat."

Paragraphe 1

126. Le sens du paragraphe 1 a suscité diverses observations d'ordre général. On a fait valoir que le détenteur de la clef privée devait toujours avoir le droit de demander au tiers authentificateur d'annuler un certificat. Le fait que cette annulation joue dès l'instant où elle aurait été reçue ou enregistrée par le tiers authentificateur ne devait être interprété ni comme limitant ce droit, ni comme signifiant que les tiers étaient tenus de s'assurer de la validité de tout certificat (par exemple, de vérifier que le certificat n'avait pas été annulé) avant de s'en prévaloir, proposition qui suscitait un certain nombre d'objections au sein du Groupe de travail (voir par. 60 ci-dessus).

127. Divers points de vue ont été exprimés touchant le moment où l'annulation prenait effet. L'on a avancé que celle-ci devait jouer dès l'instant où elle aurait été enregistrée par le tiers authentificateur, dans la mesure où il pouvait, dans certains cas, être difficile d'établir le moment de sa réception et, partant, de déterminer le moment précis où un certificat cessait d'être valide. Selon une autre opinion, le tiers authentificateur devait être tenu d'agir en toute diligence dès l'annulation d'un certificat, de manière à éviter au détenteur de la clef privée ou aux tiers toute perte qui pourrait résulter, par exemple, du fait qu'un certificat aurait été accepté par inadvertance après avoir été annulé par son détenteur. Les effets de l'annulation d'un certificat devaient donc être subordonnés aux mesures devant être prises par le tiers authentificateur et sur lesquelles le détenteur de la clef privée n'avait aucune prise.

128. On s'est interrogé sur l'effet éventuel de l'enregistrement de l'annulation d'un certificat. L'on a fait valoir que la notion d'enregistrement de l'annulation de certificat ne convenait peut-être pas tout à fait aux fins envisagées par le projet d'article F, qui avait notamment pour objet de garantir que les tiers étaient dûment informés de l'annulation de tel ou tel certificat. Il a été fait observer qu'en recevant une demande d'annulation, un tiers authentificateur pourrait, dans certains cas, se trouver dans l'obligation de vérifier l'authenticité de ladite demande, procédure qui, suivant les circonstances, pourrait être source de retard. Le moment à partir duquel il conviendrait que l'annulation joue pleinement était donc celui où elle était portée à la connaissance du public par insertion dans une base de données accessible à tous et tenue par le tiers authentificateur, ou par tout autre mode de communication approprié.

129. Cela étant, on a estimé qu'il était tout de même préférable de retenir la date de réception de la demande d'annulation au lieu de celle de son enregistrement en vue d'établir le moment à partir duquel le certificat était réputé annulé. Toutefois, si l'on jugeait que la réception de la demande n'était pas une notion assez précise, on pouvait l'associer à quelque formalité que le tiers authentificateur serait tenu d'accomplir par la suite pour donner effet à l'annulation, par exemple la publication ou la notification de celle-ci.

130. Afin de faire progresser le débat sur la question, le Groupe de travail a été invité à examiner d'une manière générale les incidences du choix du moment à partir duquel l'annulation prendrait effet et à essayer de déterminer les parties susceptibles d'être affectées par cette annulation. Le moment à partir duquel l'annulation jouerait serait décisif pour déterminer les responsabilités respectives du détenteur de la clef privée et du tiers authentificateur l'un envers l'autre et vis-à-vis des tiers. On a exprimé l'avis que le Groupe de travail gagnerait peut-être à envisager chacune de ces situations séparément. À l'appui de cette proposition, on a fait observer que chacune des solutions envisagées au paragraphe 1 avait ses mérites. Touchant le rapport entre le détenteur de la clef privée et le tiers authentificateur, il était peut-être bon de stipuler que l'annulation jouerait dès réception par le tiers authentificateur de la demande d'annulation faite par le détenteur de la clef privée. Toutefois, vis-à-vis des tiers, il était peut-être préférable d'exiger l'enregistrement ou la publication préalable de l'annulation pour que la notification puisse prendre effet.

131. Il a été souligné que la date de prise d'effet de l'annulation avait d'importantes incidences sur la responsabilité du tiers authentificateur et que ces deux questions devraient être traitées de concert. On a fait remarquer que le projet d'article H disposait en son paragraphe 4 que, lorsqu'un tiers authentificateur homologué avait été notifié de l'annulation d'un certificat, l'autorité enregistrerait cette annulation immédiatement. Si l'autorité devait faillir à cette tâche, elle serait responsable de toute perte encourue par l'utilisateur. Par suite, si le projet de règles uniformes stipulait que l'annulation d'un certificat jouait dès l'instant où elle était reçue, le paragraphe 4 du projet d'article H devrait être supprimé, dès lors qu'il n'y aurait aucun fondement à la responsabilité du tiers authentificateur pour faute ou négligence dans l'enregistrement de l'annulation. Toutefois, si l'annulation d'un certificat devait jouer à partir de l'instant où elle était enregistrée, le paragraphe 4 du projet d'article H suffirait à lui seul.

132. En réponse à cette observation, on a fait observer que la règle énoncée au paragraphe 4 du projet d'article H devrait être maintenue quel que soit le choix que le Groupe de travail opérerait entre les deux variantes proposées au paragraphe 1 du projet d'article F. L'enregistrement tardif d'une demande d'annulation pouvait porter préjudice soit au possesseur, soit à la partie qui se prévaudrait du certificat; en conséquence, une disposition sur la responsabilité à raison des conséquences de l'enregistrement tardif resterait nécessaire.

133. À cet égard, il a été fait observer que les normes et directives relatives à la certification et à l'authentification électroniques, telles que le projet de pratiques internationales uniformes en matière d'authentification et de certification en cours d'élaboration par la Chambre de commerce internationale, consacraient le principe selon lequel tout tiers authentificateur était tenu de donner promptement suite à une demande d'annulation d'un certificat. Toutefois, comme on l'avait précédemment fait remarquer, le tiers authentificateur pourrait ne pas être en mesure de donner immédiatement suite à la demande, surtout si, en raison des circonstances, il était amené à procéder à des vérifications, par exemple à confirmer les pouvoirs de la personne qui avait demandé l'annulation au nom du détenteur de la clef privée. Afin de prévenir toute utilisation par inadvertance du certificat pendant la période où le tiers authentificateur procédait à la vérification d'une demande tendant à son annulation, il a été suggéré de prescrire dans le projet de règles uniformes que le tiers authentificateur suspende le certificat dès la réception de la demande faite par le détenteur de la clef privée. On a fait observer qu'à la différence de l'annulation, qui mettait fin à la validité du certificat, la suspension était une mesure temporaire qui avait pour seul effet de priver le certificat de sa validité pour un certain temps.

134. Certains se sont déclarés favorables à l'idée d'introduire la notion de suspension par opposition à l'annulation pure et simple. Toutefois, on a estimé que cette suspension devrait faire l'objet d'une disposition distincte, la notion et les effets de la suspension étant différents de ceux de l'annulation.

135. Ayant examiné les divers points de vue exprimés, le Groupe de travail a convenu que la question de l'annulation de certificats constituait un élément important de tout système juridique régissant convenablement les signatures numériques, et méritait d'être examinée plus avant. On s'est accordé à considérer qu'il fallait étoffer la disposition consacrée à la matière et le Secrétariat a été prié de réviser le projet de disposition au vu des débats du Groupe de travail, de sorte à faire apparaître les variantes touchant la date à partir de laquelle l'annulation prendrait effet. Il a également été convenu d'insérer dans le texte révisé des dispositions sur la suspension de certificats.

Paragraphe 2

136. On a fait observer (l'observation ne concernant que la version anglaise) que le terme "obligation" employé dans la première phrase du paragraphe 2 n'était pas tout à fait propre et qu'il serait préférable dans ce contexte d'utiliser d'autres vocables, par exemple "onus" ou "duty".

137. On a estimé qu'outre le détenteur d'une paire certifiée de clefs, le tiers authentificateur devait être également tenu d'annuler le certificat correspondant lorsqu'il apprenait que la clef cryptographique privée avait été perdue, compromise ou qu'elle risquait d'être utilisée à mauvais escient à d'autres égards. À l'appui de cette thèse, on a fait valoir que certaines normes et directives internationales relatives à la certification et à l'authentification électroniques, telles que le projet de pratiques internationales uniformes en matière d'authentification et de certification en cours d'élaboration par la Chambre de commerce internationale, posaient cette obligation.

138. En réponse aux questions touchant l'aptitude du tiers authentificateur à s'acquitter d'une telle obligation, il a été dit que les techniques disponibles à l'heure actuelle permettaient à tout tiers authentificateur de réagir promptement en pareils cas. Toutefois, le délai était fonction non seulement des techniques disponibles, mais également de la nature du service fourni par le tiers authentificateur à ses clients aux termes de leurs contrats (le tiers authentificateur avait-il chargé des collaborateurs de s'occuper des cas où la clef privée serait perdue, compromise ou utilisée à mauvais escient ? Offrait-il à ses clients des services les week-ends ou seulement pendant les heures ouvrables ? etc.).

139. Le Groupe de travail a pris note des vues exprimées et a décidé d'en tenir compte à l'occasion des discussions qu'il aurait plus tard sur la question de l'annulation de certificats.

7. Registre des certificats

140. Pour l'examen des questions ayant trait au registre des certificats, le Groupe de travail s'est fondé sur le projet de dispositions ci-après :

"Projet d'article G

1) Tout tiers authentificateur homologué conservera un registre électronique auquel pourra accéder le public et qui énumérera les certificats délivrés, indiquant le moment auquel chaque certificat a été délivré, le moment de son expiration, ou encore le moment de sa suspension ou de son annulation.

2) Le registre sera conservé par le tiers authentificateur pendant au moins [10] ans après la date d'annulation ou d'expiration de la période de validité de tout certificat émis par ce tiers authentificateur."

141. Le Groupe de travail a été invité à se demander tout d'abord s'il y avait lieu d'inclure une disposition relative au registre des certificats dans le projet de règles uniformes et, dans l'affirmative, à examiner les éléments que devait comporter un tel registre ainsi que, dans l'hypothèse où une période de conservation était requise, à en déterminer la durée.

142. L'inclusion, dans le projet de règles uniformes, d'une disposition relative au registre des certificats n'a pas soulevé d'objections de principe, mais il a été suggéré que le Groupe de travail reste saisi de la question de savoir

si une telle disposition était en fait nécessaire dans le cadre du projet de règles uniformes ou était utile pour tous les différents types de certificats qui pouvaient être délivrés par des tiers authentificateurs.

143. En ce qui concernait le dispositif à adopter pour le registre, l'on a fait valoir que les tiers authentificateurs appartenant à une même infrastructure de clef publique auraient intérêt à avoir un registre centralisé où ils déposeraient les certificats qu'ils délivraient, au lieu d'établir séparément leur propre registre. Certains pays examinaient actuellement cette solution, dont l'objet était d'éviter la multiplicité des registres. Peut-être était-il utile que le Groupe de travail étudie plus avant cette possibilité.

144. En ce qui concernait le paragraphe 1), il a été estimé qu'il n'était pas nécessaire d'indiquer dans le registre la date à laquelle le certificat avait été délivré et que, par conséquent, les mots "indiquant le moment auquel chaque certificat a été délivré" devraient être supprimés. Il a été dit aussi que le tiers authentificateur devait entrer l'annulation des certificats dans une base de données distincte de façon que les parties intéressées puissent plus facilement vérifier la validité d'un certificat.

145. Au sujet du paragraphe 2), des opinions divergentes ont été exprimées sur la question de savoir si la période de conservation qui y était prévue était nécessaire et si la durée en était adéquate. Il a été dit qu'il était utile de prévoir une période de conservation minimale pour assurer que les données resteraient accessibles aux parties intéressées, mesure qui était particulièrement importante compte tenu des délais impartis par les lois nationales pour exercer des droits, les faire respecter ou demander l'exécution d'obligations. Toutefois, le droit interne fixait des délais différents selon les types de droits et d'obligations. Il prévoyait aussi des périodes de conservation différentes pour les documents publics et privés selon l'objet auquel ils se rapportaient. Dans ces conditions, peut-être était-il préférable de laisser aux lois nationales le soin de déterminer la période de conservation appropriée plutôt que d'en fixer arbitrairement une, qui pourrait ne pas être adaptée dans tous les cas. En outre, le Groupe de travail devait tenir compte du coût que représentait la conservation d'un registre de certificats pendant une période donnée. Dans certains cas, en fonction des services fournis par le tiers authentificateur et de la méthode utilisée pour classer les certificats, il pourrait ne pas être rentable pour lui de conserver certains types de certificats au-delà d'un certain temps. Il n'était pas souhaitable de prévoir une période de conservation générale sans savoir quelles en seraient les conséquences pratiques pour les entreprises.

146. L'on a fait valoir, toutefois, que la question de la période de conservation des documents et informations qui permettaient à une partie intéressée d'établir l'identité de ses partenaires commerciaux et l'authenticité de leurs signatures faisait entrer en jeu un certain nombre de considérations d'intérêt général que le Groupe de travail ne devait pas négliger. Elle méritait d'être traitée dans le projet de règles uniformes. S'agissant de la durée de la période de conservation, il a été estimé que le tiers authentificateur ne devait pas être libre de la fixer unilatéralement en se fondant uniquement sur des considérations de coût. En outre, ce coût ne devait pas être à lui seul un facteur déterminant pour écourter ou supprimer la période de conservation. Les tiers authentificateurs qui s'associeraient pour établir un registre unique dans le cadre d'une infrastructure à clef publique pourraient s'arranger pour en partager les coûts.

147. Il a été suggéré que les parties qui consultaient un registre de certificats devraient être tenues de laisser trace de leur recherche. En effet, l'existence d'une telle preuve pourrait se révéler d'importance au cas où se poserait, entre le tiers authentificateur et la partie intéressée, la question de savoir si cette dernière avait vérifié la validité d'un certificat avant de se fier à un message signé numériquement.

148. Le Groupe de travail a pris note des différentes opinions exprimées et a demandé au Secrétariat de recenser les questions soulevées et de formuler des variantes du projet de dispositions au vu des débats du Groupe de travail.

8. Relations entre utilisateurs et tiers authentificateurs

149. Le Groupe de travail était saisi du projet de dispositions ci-après :

"Projet d'article J

1) Le tiers authentificateur n'a le droit de demander que les renseignements qui lui sont nécessaires pour identifier l'utilisateur.

2) À la demande d'une personne morale ou physique, le tiers authentificateur divulgue les renseignements suivants :

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

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

c) Le coût des services donnés par le tiers authentificateur;

d) La politique ou les pratiques du tiers authentificateur s'agissant de l'utilisation, de la mise en mémoire et de la communication de renseignements d'ordre personnel;

e) Les prescriptions techniques du tiers authentificateur s'agissant du matériel de communication de l'utilisateur;

f) Les conditions dans lesquelles le tiers authentificateur met en garde les usagers en cas d'irrégularité ou de défaut de fonctionnement du matériel de communication;

g) Toute limite à la responsabilité du tiers authentificateur;

h) Toutes restrictions imposées par le tiers authentificateur s'agissant de l'utilisation du certificat;

i) Les conditions dans lesquelles l'utilisateur est en droit de restreindre l'utilisation du certificat.

3) Les renseignements énumérés au paragraphe 1) seront communiqués à l'utilisateur avant la conclusion définitive d'un accord de certification. [Ces renseignements peuvent être communiqués par le tiers authentificateur dans le cadre d'une déclaration de la pratique de certification.]

4) Avec un préavis [d'un mois], l'utilisateur peut mettre fin à l'accord le rattachant à un tiers authentificateur. Ce préavis prend effet une fois qu'il a été reçu par le tiers authentificateur.

5) Avec un préavis [de trois mois], le tiers authentificateur peut mettre fin à l'accord le rattachant à un tiers authentificateur. Ce préavis prend effet dès qu'il a été reçu."

150. Le Groupe de travail a constaté que, dans la mesure où le projet d'article J concernait les relations entre utilisateurs et tiers authentificateurs, il préjugeait des décisions relatives à un certain nombre de questions encore à l'étude. Il a été décidé de mettre entre crochets le projet d'article J dans son ensemble et d'en renvoyer l'examen à une date ultérieure.

III. INCORPORATION PAR RÉFÉRENCE

151. Ayant achevé l'examen préliminaire des questions juridiques et des dispositions éventuelles à insérer dans les règles uniformes sur les signatures numériques, comme indiqué dans la partie II du présent rapport, le Groupe de travail a constaté que le temps lui manquait pour procéder, à la session en cours, à l'examen approfondi des questions touchant l'incorporation par référence.

152. Le Groupe de travail a rappelé que cette question avait été brièvement examinée à diverses étapes de l'élaboration de la Loi type (voir A/CN.9/406, par. 90 et 178, et A/CN.9/407, par. 100 à 105 et 117). À sa précédente session, il s'était accordé à dire qu'il était nécessaire de se pencher sur la question de l'incorporation par référence dans le contexte du commerce électronique. Selon une opinion, il faudrait, si l'on tentait d'établir des normes juridiques pour l'insertion de clauses de référence dans des messages de données, que les trois conditions suivantes soient respectées : a) la clause de référence devait être insérée dans le message de données; b) le document référencé, par exemple des conditions générales, devait être effectivement connu de la partie contre laquelle il pouvait être invoqué; c) le document référencé devait être accepté, en sus d'être connu, par cette partie. De l'avis général, il convenait de traiter le sujet de l'incorporation par référence dans le cadre de travaux plus généraux sur les questions des registres et des fournisseurs de services (A/CN.9/421, par. 114). La Commission, à sa vingt-neuvième session, s'est accordée à dire que la question pourrait être étudiée dans le cadre des travaux sur les tiers authentificateurs[2].

153. À la session en cours, l'on s'est accordé à penser que l'acceptabilité de l'incorporation par référence revêtait une importance considérable pour le développement du commerce électronique en général. Certes, la question devait sans doute être examinée dans le cadre des travaux sur les signatures numériques et les tiers authentificateurs, mais elle méritait aussi de l'être à un niveau plus général. Même si l'on déterminait par la suite qu'il convenait d'élaborer des règles spécifiques pour l'incorporation par référence dans le contexte des signatures numériques, un débat général et, éventuellement, un ensemble de règles générales s'imposaient.

154. Selon une opinion, élaborer des règles régissant l'incorporation par référence en milieu électronique pourrait se révéler difficile vu la complexité des questions en jeu. L'incorporation par référence et les questions connexes, comme les contrats d'adhésion et le conflit de formulaires, avaient donné naissance à toute une variété de règles juridiques concernant les documents sur support papier, et toutes les questions juridiques y afférentes n'avaient pas été résolues de façon satisfaisante. Le sujet même obligeait à concilier des intérêts antagoniques. D'une part, il était nécessaire de reconnaître l'autonomie des parties. De l'autre, il fallait limiter les abus auxquels pouvaient donner lieu les contrats d'adhésion. Étant donné les difficultés que l'on s'attendait à rencontrer dans le domaine de l'incorporation par référence, l'on a proposé d'accorder un rang de priorité plus élevé à d'autres aspects du commerce électronique qui mériteraient également un examen plus approfondi. Selon un autre avis, l'on ne pouvait entamer un examen de l'incorporation par référence que si l'on disposait de nouvelles études du Secrétariat sur les aspects juridiques comparatifs des contrats d'adhésion, du conflit de formulaires et des questions connexes de responsabilité.

155. L'opinion la plus répandue était qu'il n'y avait pas besoin de nouvelle étude du Secrétariat, car les problèmes fondamentaux étaient bien connus, et il était clair qu'il faudrait laisser nombre d'aspects du conflit de formulaires et des contrats d'adhésion aux dispositions législatives nationales applicables en raison, par exemple, de la protection du consommateur et d'autres considérations d'intérêt général. Après en avoir discuté, le Groupe de travail a décidé que cette question devrait être la première des questions de fond qu'il examinerait à sa prochaine session.

IV. TRAVAUX FUTURS

156. Le Groupe de travail a rappelé que la Commission lui avait demandé de déterminer s'il était souhaitable et possible d'élaborer des règles uniformes concernant les signatures numériques et les tiers authentificateurs. À la clôture de sa session, le Groupe de travail a estimé qu'il devait indiquer dans son rapport à la Commission qu'il était parvenu à un consensus quant à l'importance et 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 parvenu à la conclusion préliminaire qu'il était possible d'entreprendre l'élaboration d'un projet de règles uniformes sur les questions concernant les signatures numériques.

---

[2]Ibid., cinquante et unième session, Supplément n° 17 (A/51/17), par. 222.

157. Dans le cadre de l'examen des travaux futurs, il a été rappelé que, outre les signatures numériques et les tiers authentificateurs, les travaux dans le domaine du commerce électronique devaient peut-être porter aussi sur les questions touchant des techniques autres que la cryptographie à clef publique, les questions générales concernant les fonctions exercées par les tiers fournisseurs de services et les contrats électroniques (voir A/51/17, par. 219 à 221).