NATIONS
UNIES

A

Assemblée générale

Distr. LIMITEE

A/CN.9/WG.IV/WP.71
31 décembre 1996

FRANÇAIS
Original : ANGLAIS

COMMISSION DES NATIONS UNIES
POUR LE DROIT COMMERCIAL INTERNATIONAL
Groupe de travail sur le
commerce électronique
Trente-et-unième session
New-York, 18-28 février 1997

PLANIFICATION DES TRAVAUX A VENIR EN MATIERE DE COMMERCE ELECTRONIQUE : SIGNATURES NUMERIQUES, TIERS AUTHENTIFICATEURS ET QUESTIONS JURIDIQUES CONNEXES

Note du Secrétariat

TABLE DES MATIERES

INTRODUCTION

1. Une fois adoptée la Loi-type de la CNUDCI sur le commerce électronique, la Commission, à sa vingt-neuvième session, a procédé à un débat sur les travaux futurs dans ce domaine, à partir des discussions préliminaires qu'avait eu le Groupe de travail sur les échanges de données informatisées à sa trentième session (A/CN.9/421, para. 109-119). D'une manière générale, il a été convenu que la CNUDCI devrait continuer son travail d'élaboration de normes juridiques susceptibles de rendre l'échange de données électroniques plus prévisible, renforçant ainsi les échanges dans toutes les régions.

2. De nouvelles propositions ont porté sur d'éventuelles questions à incorporer dans les travaux futurs et sur les priorités de celles-ci. On a proposé que la Commission commence à élaborer des règles sur les signatures numériques. Il a été dit que la mise en place de lois sur les signatures numériques, mais aussi de lois reconnaissant les actions des "tiers authentificateurs", ou d'autres personnes autorisées à délivrer des certificats électroniques ou autres formes d'assurance quant à l'origine et l'attribution de messages comportant une "signature" numérique était, dans de nombreux pays, jugée indispensable à l'essor des échanges électroniques. D'aucuns ont fait valoir que la possibilité de se fier aux signatures numériques déterminerait la multiplication des contrats ainsi que la cessibilité de droits sur des marchandises ou d'autres intérêts au moyen des communications électroniques. Dans un certain nombre de juridictions, de nouvelles lois régissant les signatures numériques sont actuellement en cours d'élaboration. On a signalé que déjà, il y avait manque d'uniformité dans de domaine. Si la Commission décidait d'entreprendre des travaux sur cette question, il lui serait possible d'harmoniser les nouvelles lois, ou du moins d'élaborer des principes communs s'agissant des signatures numériques et, ainsi, de constituer une infrastructure internationale pour cette activité commerciale.

3. Cette proposition a recueilli une large adhésion. De manière générale, on a toutefois estimé que, si la Commission décidait d'entreprendre des travaux sur les signatures numériques dans le cadre de son Groupe de travail sur les échanges de données informatisées, il faudrait confier au Groupe de travail un mandat spécifique en ce sens. On a également pensé qu'étant donné qu'il n'était pas possible pour la CNUDCI de se lancer dans l'élaboration de normes techniques, il importait de veiller à ce que la CNUDCI ne s'associe pas aux questions techniques ayant trait aux signatures numériques. Il a été rappelé qu'à sa trentième session, le Groupe de travail avait estimé que des travaux pourraient être nécessaires en ce qui concerne les tiers authentificateurs et qu'il faudrait probablement les effectuer dans le contexte des registres et des prestataires de services. Cependant, le Groupe de travail a également estimé qu'il ne devrait pas se lancer dans des considérations techniques concernant l'opportunité d'utiliser telle ou telle norme précise (A/CN.9/421, para. 111). On s'est inquiété du fait que les travaux sur les signatures numériques pourraient dépasser la simple sphère du droit commercial et mettre en jeu des questions générales de droit civil ou de droit administratif. En réponse à cette inquiétude, on a fait valoir que cela était vrai également des dispositions de la Loi-type et que la Commission ne devait pas craindre de rédiger des règles utiles du fait que ces règles pourraient également s'avérer utiles en dehors de la sphère des relations commerciales.

4. Une autre proposition, s'appuyant sur la discussion préliminaire du Groupe de travail, était que les travaux futurs devraient être axés sur les fournisseurs de services. Les questions suivantes ont été évoquées comme celles méritant d'être examinées : normes minima de performance en l'absence d'accord entre les parties ; étendue des risques supportés par les destinataires ; effet de ces régles ou accords sur les tiers ; répartition des risques d'intrusion ou d'actes non autorisés ; 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, para. 116).

5. De l'avis d'un grand nombre de participants, il conviendrait que la CNUDCI examine la relation entre les fournisseurs de services, les utilisateurs et les tiers. Il serait très important d'orienter les travaux sur ce sujet vers la mise

au point de normes internationales de conduite commerciale visant à favoriser le commerce par des moyens électroniques et non de prendre pour objectif l'établissement d'un régime réglementaire applicable aux fournisseurs de services ou d'autres règles qui pourraient engendrer des coûts inacceptables pour les applications commerciales de l'EDI (voir A/CN.9/421, para. 117). Cependant, un certain nombre de participants ont estimé que la question des fournisseurs de services était peut-être un peu trop vaste et englobait trop de situations objectives différentes pour relever d'un seul point de l'ordre du jour. De manière générale, on s'est accordé à penser que les questions ayant trait aux fournisseurs de services pouvaient être examinées de manière appropriée dans le contexte de chaque nouveau domaine de travail examiné par le Groupe de travail.

6. On a par ailleurs proposé que la Commission commence un travail d'élaboration des nouvelles règles d'ordre général devenues nécessaires pour clarifier la manière dont les fonctions traditionnelles du contrat peuvent être remplies au moyen des échanges électroniques. On a fait valoir le nombre d'incertitudes entourant la signification exacte des termes "performance", "livraison" et d'autres termes encore dans le contexte du commerce électronique, dès lors que l'offre, l'acceptation et la livraison de marchandises pouvaient intervenir dans le monde entier à partir de réseaux informatisés ouverts. La croissance rapide des échanges sur ordinateur ainsi que les transactions sur Internet et sur d'autres systèmes font qu'il s'agit là d'un thème prioritaire. On a lancé l'idée qu'une étude réalisée par le Secrétariat pourrait préciser la portée d'un tel travail. A supposer que la Commission, après examen de l'étude, décide de poursuivre sur cette lancée, une des solutions possibles consisterait à incorporer de telles règles dans la section "Dispositions spéciales" de la Loi-type de la CNUDCI sur le commerce électronique.

7. Il a par ailleurs été proposé que la Commission s'intéresse à la question de l'incorporation par référence. Il a été rappelé que le Groupe de travail était convenu que cette question pouvait être traitée de manière appropriée dans le cadre de travaux plus généraux sur les questions des registres et des fournisseurs de services (A/CN.9/421, para. 114). La Commission, dans son ensemble, est convenue que la question peut être traitée dans le cadre de travaux sur les tiers authentificateurs.

8. Après discussion, la Commission a décidé qu'il était opportun d'inscrire la question des signatures numériques et des tiers authentificateurs à son ordre du jour, à condition que ce point soit l'occasion d'examiner d'autres questions suggérées par le Groupe de travail pour des travaux futurs. Il a également été décidé de spécifier le mandat du Groupe de travail ; dans ce contexte, les règles uniformes à élaborer devraient traiter de questions telles que : le fondement juridique sur lequel les processus de certification s'appuient, y compris la technologie naissante qui permet l'authentification et la certification numérique ; l'applicabilité du processus de certification ; l'attribution des risques et des responsabilités des usagers, des fournisseurs de services et des tiers dans le contexte de l'utilisation des techniques de certification ; les questions spécifiques de certification dans le cadre de l'utilisation des registres ; et l'incorporation par référence.

9. La Commission a prié le Secrétariat de réaliser une étude de fond sur les questions relatives aux signatures numériques et aux fournisseurs de services, en partant de l'analyse des lois actuellement en cours d'élaboration dans divers pays. En se fondant sur cette étude, le Groupe de travail devrait réfléchir à l'opportunité et à la possibilité de rédiger des règles uniformes sur les questions sus-mentionnées. On est convenu qu'à l'occasion de sa trente-et-unième session, le Groupe de travail pourrait entreprendre d'élaborer des projets de règles touchant certains aspects des sujets sus-mentionnés. Le Groupe de travail a été prié de communiquer à la Commission suffisamment d'éléments d'information permettant à celle-ci de prendre une décision en toute connaissance de cause sur le champ d'application des règles uniformes à rédiger. Etant donné l'ampleur des activités visées par la Loi-type de la CNUDCI sur certains aspects juridiques de l'échange de données informatisées et par les travaux futurs dans le domaine du commerce

électronique, il a été décidé que le Groupe de travail sur les échanges de données informatisées serait rebaptisé "Groupe de travail sur le commerce électronique"[1].

10. La présente note comporte une étude préliminaire de la question des signatures numériques et des questions connexes. Elle a été rédigée dans le contexte de la Loi-type de la CNUDCI sur les échanges électroniques, et tient compte également des textes législatifs récemment adoptés, ou en cours d'élaboration dans certains pays. Par ailleurs, l'étude s'inspire de travaux réalisés par d'autres organisations, et notamment du Projet de Pratiques internationales uniformes en matière d'authentification et de certification, actuellement élaboré par la Chambre de commerce internationale (CCI) et les Directives relatives aux signatures numériques publiées par l'American Bar Association, et rend compte des conclusions d'une réunion d'un groupe d'experts ad hoc qui a regroupé des spécialistes du domaine des signatures numériques et le Secrétariat de la CNUDCI.

11. Conformément aux instructions récentes concernant la maîtrise et la gestion plus strictes des documents de l'Organisation des Nations Unies, les explications concernant le projet de dispositions sont aussi brèves que possible. Des explications complémentaires seront données de vive voix.

---

[1] Documents officiels de l'Assemblée générale, Cinquante-et-unième session, Supplément N° 17 (A/51/17), para. 216-224.

I. OBSERVATIONS GENERALES SUR LES SIGNATURES NUMERIQUES

A. Fonctions de la signature

12. L'article 7 de la Loi-type de la CNUDCI sur le commerce électronique est basé sur la reconnaissance des fonctions de la signature dans les documents sur papier. Lors des travaux préparatoires ayant trait à la Loi-type, le Groupe de travail a examiné les fonctions suivantes traditionnellement remplies par les signatures manuscrites : identification d'une personne ; certitude quant à la participation en personne de l'intéressé dans l'acte de signature ; association de cette personne avec la teneur d'un document. Il a été noté qu'en outre, la signature pouvait remplir diverses fonctions, selon la nature du document signé. Par exemple, une signature peut témoigner de l'intention d'une partie d'être liée par la teneur d'un contrat signé ; de l'intention d'une personne d'assumer un texte qu'il a écrit ; de l'intention d'une personne de s'associer au contenu d'un document rédigé par autrui ; du fait que et du moment où une personne se trouvait en un lieu donné.

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

B. Signatures numériques et autres signatures électroniques

14. Lorsque le Groupe de travail examinera s'il est opportun et possible d'élaborer des règles uniformes pour les signatures numériques, et dans l'optique d'aider la Commission à réfléchir au champ d'application de ces éventuelles règles uniformes, il souhaitera peut-être examiner les diverses techniques qui sont actuellement utilisées ou qui sont en cours de mise au point et qui visent à fournir un équivalent fonctionnel à la signature manuscrite et aux autres types de mécanismes d'authentification utilisés dans le cas des documents sur papier.

1. Signatures numériques faisant appel à des techniques autres que la cryptographie à clé publique

15. On peut rappeler que parallèlement aux "signatures numériques" s'appuyant sur la cryptographie fonctionnant par création d'une clé publique - qui constitue l'objet essentiel de la présente note - il existe divers autres mécanismes, souvent qualifiés de "signatures électroniques", qui peuvent être utilisés ou dont on envisage l'utilisation à l'avenir, et ce en vue de remplir une ou plusieurs des fonctions évoquées plus haut qui sont celles de la signature manuscrite. Par exemple, certaines techniques, pour garantir l'authentification, utiliseraient un dispositif biométrique s'appuyant sur les signatures manuscrites. Avec un tel dispositif, le signataire apposerait sa signature manuscrite à l'aide d'un stylo spécial, soit sur l'écran de son ordinateur, soit sur un bloc numérique. La signature manuscrite serait alors analysée par l'ordinateur et mise en mémoire comme une série de valeurs numériques, qui pourrait être ajoutée à un message de données affiché par le destinataire aux fins d'authentification. Ce système d'authentification présupposerait que des échantillons de la signature manuscrite ont été antérieurement analysés et mis en mémoire par le dispositif biométrique.

16. Le Groupe de travail souhaitera peut-être examiner la question de savoir s'il y a lieu d'élargir le champ de ses activités pour couvrir les signatures électroniques de manière générale. Dans l'affirmative, le Secrétariat devra

procéder à des recherches complémentaires sur les incidences techniques et juridiques de l'utilisation de dispositifs de "signature" faisant appel à des techniques autres que la cryptographie à clé publique. Etant donné qu'il existe suffisamment d'informations préliminaires sur les conséquences juridiques des signatures numériques et que des projets de loi sur cette question ont été élaborés dans un certain nombre de pays, la présente note s'intéresse essentiellement aux questions relatives aux signatures numériques faisant appel à la cryptographie à clé publique.

17. Lorsqu'il examinera l'opportunité et la faisabilité d'élaborer des règles uniformes applicables tant aux signatures numériques qu'aux autres formes de signature électronique, le Groupe de travail souhaitera peut-être déterminer si la CNUDCI devrait tenter de mettre au point des règles uniformes à un stade intermédiaire entre le caractère très général de la Loi-type et les règles plus spécifiques régissant le détail d'une ou de plusieurs techniques précises. En tout état de cause, fidèles au principe de la neutralité qui est celui de la Loi-type, les règles uniformes à élaborer, à supposer qu'elles traitent des signatures numériques, ne devraient pas décourager l'utilisation d'autres méthodes.

2. Signatures numériques utilisant la cryptographie à clé publique[2]

a) Notions et terminologie techniques

i) Cryptographie

18. Les signatures numériques sont créées et vérifiées grâce à la cryptographie, cette branche des mathématiques appliquées qui consiste à transformer des messages en des formes apparemment inintelligibles pour les restituer ensuite à leur forme initiale. Les signatures numériques utilisent la cryptographie à clé publique, qui s'appuie souvent sur l'utilisation de fonctions algorithmiques pour créer deux "clés" (c.-à-d. des nombres à plusieurs chiffres créés à l'aide d'une série de formules mathématiques appliquées aux nombres premiers), clés différentes mais mathématiquement liées les unes aux autres. L'une de ces clés est utilisée pour créer une signature numérique ou pour transformer des données en une forme apparemment inintelligible ; l'autre clé est utilisée pour vérifier une signature numérique ou restituer le message dans sa forme initiale. Le matériel et le logiciel informatiques utilisant deux clés de ce type sont souvent appelés collectivement des "cryptosystèmes" ou plus spécifiquement encore, des "cryptosystèmes asymétriques" lorsqu'ils utilisent des algorithmes asymétriques.

19. Bien que le recours à la cryptographie soit l'un des éléments essentiels des signatures numériques, le simple fait qu'une signature numérique soit utilisée pour authentifier un message contenant des données sous forme numérique ne doit pas être assimilée à l'utilisation plus générale de la cryptographie aux fins de confidentialité. La mise en code pour raison de confidentialité est une méthode utilisée pour programmer une communication électronique de telle manière que seuls l'initiateur et le destinataire du message seront en mesure de le lire. Dans un certain nombre de pays, la loi restreint l'utilisation de la cryptographie à cette fin pour des raisons de politique nationale qui peuvent d'ailleurs comporter des considérations relatives à la défense nationale. Cependant, l'utilisation de la cryptographie aux fins d'authentification par création d'une signature numérique n'implique pas nécessairement la mise en code pour garantir le caractère confidentiel d'une communication, étant donné que la signature numérique mise en code peut être tout simplement jointe à un message non codé. Le Groupe de travail souhaitera peut-être se pencher sur la question de savoir dans quelle mesure les éventuelles règles uniformes sur les signatures numériques devraient reconnaître l'utilisation de la cryptographie aux fins d'authentification, à distinguer de son utilisation aux fins de confidentialité.

---

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

20. Afin d'illustrer les raisons pour lesquelles différentes règles peuvent s'imposer dans les cas où la mise en code est utilisée aux fins de confidentialité et dans les cas où elle est utilisée uniquement pour les signatures numériques, il est émis une hypothèse selon laquelle, lorsque la mise en code est utilisée pour garantir le caractère confidentiel d'un message, il importe, dans de nombreuses circonstances, qu'il existe un moyen de retrouver les messages mis en code si la clé privée est perdue, là où le message codé a une valeur juridique ou financière importante ou encore lorsqu'une responsabilité est mise en jeu. La technologie, utilisée à bon escient, permet à l'initiateur de la paire de clés de garder ou de recréer la clé manquante. Cependant, il n'y a peut-être pas lieu de garder ou de recréer la clé privée utilisée pour créer des signatures numériques ; la possibilité technique de le faire pourrait d'ailleurs diminuer la confiance que les utilisateurs et le grand public feraient au système dans son ensemble.

ii) "Clés publiques et clés privées"

21. Les clés complémentaires utilisées pour les signatures numériques sont désignées arbitrairement sous le nom de "clé privée" utilisée uniquement par le signataire pour créer sa signature numérique, et de "clé publique", le plus souvent mieux connue et utilisée par le destinataire pour vérifier la signature numérique[3]. Si un grand nombre de personnes doit vérifier la signature numérique du signataire, la clé publique doit être mise à la disposition ou distribuée à chacun d'entre eux, par exemple par publication dans un répertoire en direct ou sous toute autre forme de répertoire public facilement disponible. Bien qu'il existe une relation mathématique entre les deux clés de la paire, si le cryptosystème asymétrique a été bien conçu et bien mis en oeuvre, il est pratiquement impossible de trouver la clé privée à partir de la clé publique. Les algorithmes les plus communément utilisés pour la mise en code des clés publiques et privées s'appuient sur un caractéristique essentielle des grands nombres premiers : une fois multipliés les uns par les autres pour produire un nouveau numéro, il est pratiquement impossible de déterminer les deux nombres premiers qui ont servi à créer le nouveau nombre, plus élevé[4]. Aussi, bien que la clé publique d'un signataire donné puisse être connue de nombreuses personnes qui l'utiliseront pour vérifier les signatures dudit signataire, ces personnes ne peuvent découvrir la clé privée du signataire et l'utiliser pour contrefaire des signatures numériques.

22. Il convient toutefois de noter que le concept de cryptographie à clé publique n'entraîne pas nécessairement l'utilisation des algorithmes sus-mentionnés basés sur les nombres premiers. D'autres techniques mathématiques sont actuellement utilisées ou en cours de mise au point, par exemple, les cryptosystèmes à courbes elliptiques, souvent décrites comme offrant un haut degré de sécurité du fait du recours à des longueurs-clés de beaucoup réduites. Lors de l'examen des questions relatives à la cryptographie à clé publique, le Groupe de travail souhaitera peut-être examiner dans quelle mesure cette technique est utilisée en commerce international. En même temps, le Groupe de travail souhaitera peut-être adopter une attitude neutre vis-à-vis des techniques, tenant certes compte de la technologie

---

[3] L'utilisateur d'une clé privée est censé garder secrète la clé privée. Il convient de noter que l'utilisateur individuellement n'a pas nécessairement besoin de connaître la clé privée. Celle-ci figurera vraisemblablement sur une carte à mémoire ou alors sera accessible au moyen d'un numéro d'identification personnel ou encore individuellement, au moyen d'un dispositif d'identification biométrique, p. ex., la reconnaissance d'une empreinte digitale.

[4] Certaines normes existantes, telles que les Directives relatives aux signatures numériques de l'American Bar Association évoquent la notion d'"impossibilité de calcul" pour décrire l'irréversibilité prévue du processus, à savoir l'espoir qu'il sera impossible de trouver la clé privée secrète d'un utilisateur à partir de sa clé publique. "L'impossibilité de calcul" est un concept relatif s'appuyant sur la valeur des données protégées, les moyens informatisés nécessaires pour les protéger, la durée pendant laquelle les données doivent être protégées, et le coût et le temps nécessaires pour s'attaquer aux données, tous ces facteurs étant évalués dès maintenant et à la lumière des percées technologiques à venir (ABA Digital Signature Guidelines, p. 9, note 23).

elliptiques, souvent décrites comme offrant un haut degré de sécurité du fait du recours à des longueurs-clés de beaucoup réduites. Lors de l'examen des questions relatives à la cryptographie à clé publique, le Groupe de travail souhaitera peut-être examiner dans quelle mesure cette technique est utilisée en commerce international. En même temps, le Groupe de travail souhaitera peut-être adopter une attitude neutre vis-à-vis des techniques, tenant certes compte de la technologie actuelle, sans pour autant exclure l'évolution des techniques de calcul utilisées pour créer des paires de clé. Cette ouverture à l'évolution technique dans l'industrie informatique sera en outre compatible avec la décision prise par la Commission, à savoir qu'il était impossible pour la CNUDCI de se lancer dans l'élaboration de normes techniques et qu'il y avait lieu de veiller à ce qu'elle ne s'associe pas aux questions techniques concernant la signature numérique (voir ci-dessus paragraphe 3).

iii) "Fonction contrôle"

23. En plus de la création de couples de clés, on utilise un autre processus fondamental, généralement connu sous le nom de "fonction contrôle", et qui sert à la fois a créer et a vérifier la signature numérique. Cette fonction est un processus mathématique, basé sur un algorithme qui crée une représentation numérique ou forme condensée du message, souvent appelée "message abrégé" ou "empreinte" du message et qui prend la forme d'une valeur contrôle ou d'un résultat contrôle d'une longueur normalisée généralement bien plus courte que le message lui-même mais qui lui est néanmoins unique. Toute modification du message produit systématiquement un résultat contrôle différent lorsque la même fonction est utilisée. Dans le cas d'une fonction contrôle confidentielle, quelquefois appelée fonction contrôle unilatérale, il est pratiquement impossible d'obtenir le message initial en connaissant simplement sa valeur contrôle. Ces fonctions permettent donc au logiciel de création de signatures numériques d'opérer sur des quantités plus petites et plus prévisibles de données, tout en assurant une solide corrélation avec la teneur du message initial, garantissant ainsi de manière efficace qu'aucune modification n'a été apportée au message depuis sa signature sous forme numérique.

iv) "Signature numérique"

24. Pour signer un document ou tout autre élément d'information, les signataires délimitent tout d'abord très précisément les contours de ce qui est à signer. L'information à signer ainsi délimitée peut être appelée "message". Ensuite, une fonction contrôle dans le logiciel du signataire calcule un résultat contrôle associé exclusivement (à toutes fins utiles) au message. Le logiciel du signataire transforme ensuite le résultat contrôle en une signature numérique à l'aide de la clé privée du signataire. La signature numérique qui en est le résultat est donc affectée exclusivement à la fois au message et à la clé privée utilisée pour créer la signature.

25. Le plus souvent, une signature numérique (résultat du message signé numériquement) est jointe au message et mise en mémoire ou transmise avec son message. Cela dit, elle peut également être transmise ou mise en mémoire comme élément de donnée distinct, dès lors qu'il existe une association fiable avec le message. Dans la mesure où une signature numérique vaut exclusivement pour le message qui y correspond, elle est inutile si elle est dissociée de manière permanente de son message.

v) Vérification de la signature numérique

26. La vérification de la signature numérique est le processus de vérification de la signature numérique par référence au message initial et à une clé publique donnée, ce qui permet de déterminer si la signature numérique a été créée pour ce même message à l'aide de la clé privée qui correspond à la clé publique de référence. La vérification de la signature numérique se fait par le calcul d'un nouveau résultat contrôle du message initial au moyen de la même fonction contrôle utilisée pour créer la signature numérique. Ensuite, à l'aide de la clé publique et du nouveau résultat contrôle, la personne chargée de la vérification s'assure que la signature numérique a été créée à l'aide de la clé privée correspondante et

permettra de vérifier uniquement une signature numérique créée à l'aide de la clé privée du signataire ; et 2) si le message ne subit aucune modification, ce qui est avéré si le résultat contrôle calculé par la personne chargée de la vérification est identique au résultat contrôle extrait de la signature numérique lors du processus de vérification.

b) Infrastructure de la clé publique et tiers authentificateurs

28. Pour vérifier une signature numérique, le vérificateur doit avoir accès à la clé publique du signataire et s'assurer que celle-ci correspond bien à la clé privée du signataire. Cependant, le couple clé publique-clé privée n'a aucune association intrinsèque avec une personne quelconque ; il s'agit en effet simplement d'un couple de numéros. Il faut un mécanisme supplémentaire pour associer de manière fiable une personne ou une entité précise au couple de clés. Si on veut que la mise en code de la clé publique remplisse sa fonction prévue, il faut trouver un moyen d'envoyer les clés à un grand nombre de personnes, dont beaucoup sont inconnues de la personne qui procède à cet envoi et alors même qu'aucune relation de confiance n'a pu se forger entre les parties. Pour ce faire, les parties en jeu doivent accorder une très grande confiance aux clés publiques et privées émises.

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

30. En outre, du fait que la mise en code de la clé publique est une technique hautement mathématique, tous les utilisateurs doivent se fier aux compétences, aux connaissances et aux dispositifs en matière de sécurité des parties émettant les clés publiques et privées[5].

31. Un signataire éventuel pourrait faire une déclaration publique indiquant que les signatures vérifiables au moyen d'une clé publique donnée devraient être considérées comme provenant du signataire en question. Cela dit, d'autres parties pourraient refuser d'accepter cette déclaration, notamment dans les cas où il n'existe aucun contrat préalable établissant avec certitude l'effet juridique de cette déclaration publique. Une partie se fiant à une telle déclaration publiée dans un système ouvert mais non étayé courrait alors un grave risque de faire confiance à un imposteur, ou d'avoir à établir qu'il n'y a pas eu véritablement refus de signature (point souvent appelé "non-répudiation") dans les cas où une transaction s'avérerait défavorable pour le signataire.

32. L'une des solutions à ce problème consiste à recourir à un ou plusieurs tiers à qui l'on fait toute confiance et qui associerait un signataire bien identifié ou le nom d'un signataire à une clé publique spécifique. Cette partie tierce éprouvée est généralement appelée "tiers authentificateur" dans la plupart des normes et directives techniques. Dans certains pays, ces tiers authentificateurs sont en train d'être organisées sur un mode hiérarchique dans le cadre de ce que l'on appelle souvent l'infrastructure de la clé publique.

i) L'infrastructure de la clé publique

---

[5] Dans les cas où les clés publiques et privées seraient émises par les utilisateurs eux-mêmes, cette confiance devra peut-être être garantie par ceux qui certifient les clés publiques.

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

34. L'infrastructure de la clé publique s'appuie souvent sur divers niveaux d'autorité. Par exemple, les modèles envisagés dans certains pays pour établir une éventuelle infrastructure se réfèrent notamment aux niveaux d'autorité suivants : 1) une "autorité centrale" unique, qui homologuerait la technologie et les pratiques de toutes les parties autorisées à utiliser les couples de clés cryptographiques ou de certificats permettant l'utilisation de ces couples de clés, et qui homologuerait les tiers authentificateurs subordonnés[6] ; 2) divers tiers authentificateurs, situés en dessous de "l'autorité centrale", qui garantiraient que la clé publique d'un utilisateur correspond effectivement à la clé privée de cet utilisateur (autrement dit, que la clé n'a pas été manipulée) et 3) diverses autorités locales d'enregistrement, placées sous les tiers authentificateurs et chargées de répondre aux demandes des utilisateurs de se voir attribuer des couples de clés cryptographiques ou un certificat relatif à l'utilisation de ces couples de clés et chargées d'exiger une preuve d'identité et de vérifier l'identité d'utilisateurs éventuels. Dans certains pays, il est envisagé de confier aux notaires la fonction d'autorité locale d'enregistrement, ou tout au moins d'apporter leur concours à cette fonction.

35. Le Groupe de travail souhaitera peut-être procéder à un débat général sur les questions de l'infrastructure de la clé publique. Cela dit, il se peut bien que ces questions ne se prêtent guère aisément à une harmonisation internationale. En effet, l'organisation d'une infrastructure de la clé publique peut mettre en jeu diverses questions techniques, ainsi que l'action des pouvoirs publics, questions qu'il est peut-être préférable de laisser à la discrétion de chaque Etat[7]. A cet égard, chaque Etat devra peut-être prendre des décisions relatives à l'établissement d'une infrastructure de la clé publique, concernant notamment les éléments suivants : 1) la modalité et le nombre de niveaux d'autorité devant constituer l'infrastructure de la clé publique ; 2) la question de savoir si certaines autorités appartenant à l'infrastructure devraient être autorisées à délivrer les couples de clés cryptographiques ou si ces couples de clés peuvent peut-être être créés par les utilisateurs eux-mêmes ; 3) la question de savoir si les tiers authentificateurs garantissant la validité des couples de clés cryptographiques devraient être des entités publiques ou si des entités privées pourraient agir en cette qualité ; 4) la question de savoir si le processus par

---

[6] La question de savoir si un gouvernement devrait avoir la capacité technique de conserver ou de recréer des clés privées peut être traitée à ce niveau d'autorité.

[7] Cela dit, dans le cadre de la certification croisée, du fait de la nécessité d'une compatibilité mondiale, les infrastructures mises en place dans les différents pays devraient pouvoir communiquer les unes avec les autres.

égard, chaque Etat devra peut-être prendre des décisions relatives à l'établissement d'une infrastructure de la clé publique, concernant notamment les éléments suivants : 1) la modalité et le nombre de niveaux d'autorité devant constituer l'infrastructure de la clé publique ; 2) la question de savoir si certaines autorités appartenant à l'infrastructure devraient être autorisées à délivrer les couples de clés cryptographiques ou si ces couples de clés peuvent peut-être être créés par les utilisateurs eux-mêmes ; 3) la question de savoir si les tiers authentificateurs garantissant la validité des couples de clés cryptographiques devraient être des entités publiques ou si des entités privées pourraient agir en cette qualité ; 4) la question de savoir si le processus par lequel on autorise une entité donnée à agir en qualité du tiers authentificateur devrait se faire sous forme d'autorisation expresse, ou d'octroi d'une "licence" par l'Etat, ou si d'autres méthodes devraient être utilisées pour veiller à la qualité des tiers authentificateurs si ceux-ci sont autorisés à opérer en l'absence d'une autorisation spécifique ; 5) la mesure dans laquelle une utilisation de la cryptographie devrait être autorisée aux fins de confidentialité ; et 6) la question de savoir si l'Etat doit conserver l'accès à l'information chiffrée, au moyen d'un mécanisme de "blocage" de la clé ou autrement. Le Groupe de travail souhaitera peut-être recommander que les questions sus-mentionnées ne soient pas traitées dans le cadre des travaux à venir de la Commission portant sur les signatures numériques.

ii) Tiers authentificateurs

36. Pour associer une paire de clés avec un signataire éventuel, le tiers authentificateur délivre un certificat, enregistrement électronique qui précise la clé 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 clé privée correspondante. La fonction essentielle d'un certificat est d'associer une clé publique à un détenteur précis. Un "destinataire" du certificat souhaitant se fier à une signature numérique créée par le détenteur cité dans le certificat peut utiliser la clé publique figurant dans le certificat pour vérifier que la signature numérique a bel et bien été créée avec la clé privée correspondante. Si cette vérification est positive, le destinataire est assuré que la signature numérique a effectivement été créée par le détenteur de la clé publique citée dans le certificat, et que le message correspondant n'a pas été modifié depuis qu'on y a apposé une signature numérique.

37. Pour assurer l'authenticité du certificat s'agissant tant de sa teneur que de sa source, le tiers authentificateur y appose une signature numérique. La signature numérique du tiers authentificateur qui délivre le certificat peut être vérifiée au moyen de la clé publique du tiers authentificateur figurant sur un autre certificat délivré par un autre tiers authentificateur (qui peut être mais qui n'est pas nécessairement une autorité hiérarchique supérieure), et cet autre certificat peut à son tour être identifié par la clé publique figurant sur un autre certificat encore, et ainsi de suite, jusqu'à ce que la personne devant s'assurer de la signature numérique est satisfaite de son authenticité. Dans chaque cas, le tiers authentificateur délivrant le certificat doit apposer une signature numérique sur son propre certificat lors de la durée de fonctionnement de l'autre certificat utilisé pour vérifier la signature numérique du tiers authentificateur.

38. Une signature numérique correspondant à un message, qu'elle soit créée par le détenteur de la paire de clés pour identifier un message ou par le tiers authentificateur pour authentifier son certificat, devrait généralement être datée pour permettre au vérificateur de déterminer de manière fiable si la signature numérique a bien été créée durant la "période opérationnelle" citée dans le certificat, qui est une des conditions de la vérification d'une signature numérique.

39. Pour que la clé publique et son association à un détenteur spécifique soit aisément disponible pour vérification, le certificat peut être publié dans un répertoire ou mis à disposition par d'autres moyens. Le plus souvent, les répertoires sont des bases de données en ligne regroupant les certificats et autres informations disponibles qui peuvent être appelées et utilisées pour vérifier la signature numérique. Selon le mode de mise en oeuvre, l'interrogation d'un

certificat peut se faire automatiquement, le programme de vérification interrogeant directement le répertoire pour obtenir les certificats selon que de besoin.

40. Une fois délivré, un certificat peut se révéler sujet à caution, par exemple dans des situations où le détenteur a donné une identité fausse au tiers authentificateur. Dans d'autres circonstances, un certificat peut être fiable au moment où il est délivré mais devenir sujet à caution par la suite. Si la clé privée est "compromise", par exemple parce que le détenteur de la clé privée en a perdu le contrôle, le certificat peut perdre sa fiabilité, et alors le tiers authentificateur (à la demande du détenteur ou même sans son consentement, selon les circonstances) peut suspendre (interrompre provisoirement la période de validité) ou retirer (annuler de manière permanente) le certificat. Dès la suspension ou l'annulation d'un certificat, le tiers authentificateur doit généralement publier une notification de l'annulation ou de la suspension ou notifier les personnes qui l'interrogent ou que l'on sait avoir reçu une signature numérique vérifiable au moyen du certificat douteux.

41. On peut concevoir que les tiers authentificateurs relèvent des pouvoirs publics ou bien de prestataires de services du secteur privé. Dans un certain nombre de pays, on envisage, pour des raisons propres aux pouvoirs publics, que seuls les organismes d'Etat devraient être autorisés à faire office de tiers authentificateur. Dans d'autres pays, on considère que les services d'authentification doivent être l'objet d'une libre concurrence sur le marché privé. Indépendamment du fait que les tiers authentificateurs relèvent d'organismes publics ou de prestataires de services privés, et du fait qu'ils auraient besoin de se faire délivrer une licence pour fonctionner, il y a, le plus souvent, plus d'un tiers authentificateur fonctionnant dans l'infrastructure de la clé publique. Tout particulièrement importante est la relation qui existe entre les différents tiers authentificateurs. Les tiers authentificateurs d'une infrastructure de la clé publique peuvent être établis au sein d'une structure hiérarchique, où certains tiers authentificateurs ne feraient que vérifier d'autres tiers authentificateurs qui assureraient les services directement aux usagers. Dans une telle structure, les tiers authentificateurs sont subordonnés à d'autres. Dans d'autres structures envisageables, certains tiers authentificateurs peuvent fonctionner sur un pied d'égalité avec d'autres tiers authentificateurs. Dans toute infrastructure importante il y aura vraisemblablement des tiers authentificateurs et des autorités supérieures. En tout état de cause, en l'absence d'une infrastructure internationale, un certain nombre de questions peuvent se poser s'agissant de la reconnaissance des certificats par les tiers authentificateurs d'autres pays. La reconnaissance de certificats étrangers est souvent appelée "certification croisée". En de tels cas, il est indispensable que des tiers authentificateurs pour l'essentiel égaux (ou acceptant tout au moins de prendre certains risques s'agissant des certificats délivrés par d'autres tiers authentificateurs) reconnaissent les services assurés par l'un et l'autre, de telle sorte que leurs usagers respectifs puissent communiquer entre eux de manière plus efficace et en accordant une plus grande confiance aux certificats émis.

42. Des questions juridiques peuvent se poser dans le cadre de la certification croisée ou des certificats en chaîne lorsque des politiques de sécurité multiples sont en jeu. Il peut s'agir notamment de déterminer quel méfait à causé une perte, ou sur qui l'usager a compté. Il convient de noter que les règles juridiques envisagées dans certains pays disposent que, là où les politiques en vigueur et les questions de sécurité sont connues des usagers, et qu'il n'y a aucune négligence de la part des tiers authentificateurs, nulle responsabilité ne peut être engagée.

43. Il peut incomber au tiers authentificateur ou à l'autorité centrale de veiller à ce que ces prescriptions soient systématiquement respectées. Si la sélection des tiers authentificateurs peut se faire en fonction d'un certain nombre de facteurs dont la solidité de la clé publique utilisée et l'identité de l'usager la crédibilité de tout tiers authentificateur peut également dépendre de son respect des normes de délivrance de certificats et de la justesse de son évaluation des données communiquées par les usagers qui demandent le certificat. D'une importance toute particulière : le régime de responsabilité s'appliquant au tiers authentificateur s'agissant de son respect des prescriptions en matière de politique générale et de sécurité mises en place par l'autorité centrale ou le

tiers authentificateur supérieur, ou de toute autre prescription applicable, et ce de manière continue.

44. Le Groupe de travail souhaitera peut-être examiner les facteurs suivants dont il convient de tenir compte lorsque l'on évalue la fiabilité d'un tiers authentificateur : 1) indépendance (c.-à-d. l'absence d'intérêts financiers ou autres dans les transactions en jeu ; 2) ressources et capacité financières d'assumer le risque d'avoir sa responsabilité mise en jeu en cas de perte ; 3) maîtrise de la technologie des clés publiques et familiarité avec les procédures de sécurité en jeu ; 4) durée (les tiers authentificateurs peuvent en effet être amenés à donner des preuves de certification ou à décrypter des clés plusieurs années après la fin de la transaction, p. ex. dans le cadre d'une action en justice ou d'un litige relatif à la propriété) ; 5) homologation du matériel et du logiciel ; 6) mise en place d'une vérification à rebours et vérification par une entité indépendante ; 7) existence d'un plan de contingence (p. ex. logiciel de "récupération catastrophe" ou mécanisme de "blocage" de la clé) ; 8) sélection et gestion du personnel ; 9) dispositif de protection s'agissant de la clé privée du tiers authentificateur ; 10) sécurité interne ; 11) arrangements pour la fin des opérations, y compris notification aux utilisateurs ; 12) garanties et responsabilités (consenties ou exclues) ; 13) limites de la responsabilité ; 14) assurance ; 15) compatibilité avec d'autres tiers authentificateurs ; 16) procédures d'annulation (dans les cas où les clés cryptographiques viendraient à être perdues ou compromises).

c) Résumé du processus de signature numérique

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

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

2) l'expéditeur rédige un message (p. ex. sous forme d'un courrier électronique) sur l'ordinateur ;

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

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

5) l'expéditeur, le plus souvent, attache ou ajoute sa signature numérique au message ;

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

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

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

9) le destinataire compare les deux abrégés de message. S'ils sont identiques, alors le destinataire sait que le message n'a pas été modifié après avoir été signé. Même si le message a subi une très légère modification après avoir reçu

une signature numérique, l'abrégé de message créé par le destinataire sera différent de celui créé par l'expéditeur ;

10) le destinataire se voit délivrer un certificat par le tiers authentificateur (ou par l'intermédiaire de l'initiateur du message) qui confirme la signature numérique apposée sur le message de l'expéditeur. Le tiers authentificateur est le plus souvent un tiers inspirant toute confiance qui administre la certification du système de signature numérique. Le certificat comporte la clé publique et le nom de l'expéditeur (et éventuellement des renseignements complémentaires), signés par signature numérique par le tiers authentificateur.

II. QUESTIONS JURIDIQUES ET DISPOSITIONS EVENTUELLES A INSERER DANS LES REGLES UNIFORMES SUR LES SIGNATURES NUMERIQUES

A. Portée des travaux

46. Lorsque la Commission a décidé, à sa vingt-neuvième session, d'inscrire la question des signatures numériques et des tiers authentificateurs à son ordre du jour, elle a par ailleurs décidé que cette question devait également constituer une occasion de traiter d'autres sujets proposés par le Groupe de travail dans le cadre de ses travaux futurs (voir ci-dessus paragraphe 8). Avant d'examiner les questions ayant trait aux signatures numériques, le Groupe de travail souhaitera peut-être examiner l'opportunité d'une décision limitant la portée de ses travaux aux signatures numériques ou, au contraire, de l'amplifier pour couvrir également d'autres mécanismes d'authentification qui existeraient déjà ou qui seraient bientôt disponibles pour utilisation dans le commerce électronique (voir ci-dessus paragraphes 15-17). On se souviendra que, lors de l'élaboration de la Loi-type, le Groupe de travail s'était soucié de la nécessité d'établir des règles juridiques non liées à un stade donné de l'évolution technique et commerciale mais bien de faire émerger des principes généraux susceptibles de rester applicables au fil des ans, quelle que soit l'évolution technologique.

47. L'utilisation généralisée des signatures numériques, ainsi que le risque de voir les pays adopter des démarches législatives différentes s'agissant des signatures numériques, permet de penser que des dispositions législatives uniformes s'imposent pour créer un cadre juridique spécifique à cette technique d'authentification. Cependant, conformément à la démarche neutre qu'il a adopté vis-à-vis des différents types de médias lors de son élaboration de la Loi-type, le Groupe de travail souhaitera peut-être soulever la question de savoir s'il est opportun de se lancer dans l'élaboration de règles uniformes qui s'appliqueraient uniquement aux signatures numériques ou si des règles uniformes devraient également être rédigées pour s'appliquer à d'autres techniques d'authentification. Si le Groupe de travail parvenait à la conclusion que le risque sus-mentionné de voir les pays adopter des lois différentes justifiait l'élaboration de règles uniformes applicables aux signatures numériques, et ce de manière urgente, le Groupe de travail souhaitera également peut-être examiner les moyens de rédiger des règles uniformes sur les signatures numériques permettant d'éviter le risque que lesdites règles soient mal interprétées dans le sens où l'on pourrait croire qu'elles favorisent l'utilisation de signatures numériques aux dépens d'autres techniques en concurrence avec les signatures numériques, et qui pourraient tout aussi être considérées comme des illustrations acceptables du concept de "méthode fiable", consacré à l'article 7 de la Loi-type.

48. Pour ce qui est des tiers authentificateurs, le Groupe de travail souhaitera peut-être également tenir compte du fait que, dans de nombreuses situations pratiques, les activités d'une entité commerciale agissant en qualité de tiers authentificateur ne constituent qu'un des éléments d'un ensemble plus vaste d'activités de cette entité commerciale en tant que prestataire de services. Le Groupe de travail voudra donc peut-être examiner la question de savoir si les règles uniformes relatives aux tiers authentificateurs devraient se limiter à des règles de conduite applicables dans le seul contexte des activités d'un prestataire

de services agissant en qualité de tiers authentificateur ou s'il serait opportun et faisable d'élaborer des règles applicables à un ensemble plus vaste d'activités des prestataires de services ou des "tiers approuvés" dans le commerce électronique.

B. Champ d'application des règles uniformes relatives aux signatures numériques et dispositions générales

49. La présente note a été rédigée à partir de l'hypothèse selon laquelle les règles éventuelles relatives aux signatures numériques devraient s'inspirer directement de l'article 7 de la Loi-type et devraient être considérées comme un moyen de donner des renseignements précis sur la notion de "méthode fiable" utilisée pour identifier "une personne" et pour indiquer "qu'elle approuve l'information" contenue dans le message de données. Lors de l'examen des dispositions générales à inclure éventuellement dans un ensemble de règles uniformes sur les signatures numériques, le Groupe de travail souhaitera peut-être examiner de manière plus générale les relations qui existent entre ces règles uniformes et la Loi-type de la CNUDCI sur le commerce électronique. Plus particulièrement, le Groupe de travail souhaitera peut-être faire des propositions à la Commission s'agissant de savoir si les règles uniformes sur les signatures numériques devraient ou non constituer un instrument juridique distinct ou s'il y a lieu de les incorporer dans une version élargie de la Loi-type, par exemple en tant que chapitre distinct à inclure dans la deuxième partie de la Loi-type.

50. Que les règles uniformes sur les signatures numériques soient rédigées en tant qu'instrument distinct ou comme complément de la Loi-type, l'idée est émise que les règles uniformes devront se fonder sur des dispositions suivant de près les articles 1 (Champ d'application), 2 a), c) et e) (Définition de "message de données", "expéditeur" et "destinataire"), 3 (Interprétation), 4 (Dérogation conventionnelle), 6 (Ecrit) et 7 (Signature) de la Loi-type. Bien que ces dispositions ne soient pas reproduites expressément dans la présente note, il convient de noter que le projet de règles uniformes sur les signatures numériques ont été rédigées par le Secrétariat à partir de l'hypothèse que de telles dispositions faisaient partie intégrante des règles uniformes. A cet égard, il y a lieu également de noter qu'il existe des dispositions s'alignant sur les articles 2, 4, 6 et 7 de la Loi-type dans des lois relatives aux signatures numériques actuellement en cours d'élaboration dans de nombreux pays, alors que la Loi-type est également évoquée dans d'autres textes, par exemple les Digital Signature Guidelines rédigées par l'American Bar Association.

51. En plus des dispositions sus mentionnées, le Groupe de travail souhaitera peut-être examiner le point de savoir si un préambule aux règles uniformes serait susceptible de préciser la fiabilité de ces règles, à savoir de promouvoir l'utilisation efficace des communications numériques par la mise en place d'une structure de sécurité et l'affirmation de l'égalité entre les signatures manuscrites et numériques s'agissant de leur effet juridique.

C. Questions juridiques spécifiques et projet de dispositions sur les signatures numériques

1. Définitions

52. Les lois, règlements et directives déjà mis en place ou en cours d'élaboration dans le domaine des signatures numériques et des tiers authentificateurs divergent sensiblement en ce qui concerne le nombre de définitions ou en fonction de la tradition juridique de l'Etat édictant la loi. Les questions de signature numérique peuvent être traitées soit à l'aide de définitions, soit ne comporter aucune définition.

53. Conformément à la démarche adoptée lors de l'élaboration de la Loi-type, le Groupe de travail souhaitera peut-être examiner un nombre limité de définitions de notions essentielles, telles que la "signature numérique", les "tiers authentificateurs", et les "certificats".

54. Le Groupe de travail souhaitera peut-être utiliser les définitions suivantes comme base de ses délibérations.

a) Signature numérique

55. "Projet d'article A

1) Une signature numérique est une valeur numérique apposée à un message de données et qui, grâce à une procédure mathématique bien connue associée à la clé cryptographique privée de l'expéditeur, permet de déterminer que cette valeur numérique a été créée à partir de la clé 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 clé 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 clé publique de l'expéditeur peut déterminer avec exactitude

a) si la transformation a été opérée à l'aide de la clé 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'Etat qui édicte la loi] adoptera des règles spécifiques régissant les prescriptions techniques à respecter s'agissant des signatures numériques et leur vérification".

Observations

56. Conformément à la démarche fonctionnelle adoptée lors de l'élaboration de la Loi-type, les paragraphes 1) et 2) de la proposition de disposition met l'accent sur une brève description des fonctions techniques remplies par le chiffrement à l'aide de la clé publique. Les paragraphes 3) et 4) correspondent au principe selon lequel les signatures numériques ne sont valables que si elles sont utilisées dans le contexte d'une infrastructure de la clé publique mise en place par les autorités publiques.

b) Tiers authentificateurs homologués

57. "Projet d'article B

1) ...[c'est l'Etat 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'Etat 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 clés 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'Etat 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.

Observations

58. Le Groupe de travail souhaitera peut-être examiner la question de savoir si les règles uniformes à élaborer devraient mentionner expressément les critères dont il convient de tenir compte lorsque l'on autorise les tiers authentificateurs à fonctionner. On peut rappeler que, dans le cadre de l'élaboration de la Loi-type, ces critères ont été inclus dans le Guide pour l'incorporation de la Loi-type.

c) Certificats

59. "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) clé cryptographique de l'utilisateur ;

f) toute information nécessaire indiquant la manière dont la clé 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.

Observations

60. Les projets de loi sur les signatures numériques actuellement élaborés dans certains pays énumèrent une partie ou la totalité des éléments mentionnés dans la projet d'article C, jugés le minimum indispensable dans tout certificat émis par un tiers authentificateur. Cependant, conformément à la décision prise par le Groupe de travail lors de l'élaboration de la Loi-type de ne pas s'immiscer dans les questions de protection des données personnelles, le Groupe de travail souhaitera peut-être tenir compte du fait que, dans de nombreux pays, les informations - concernant, par exemple, la date de naissance d'une personne - seraient protégées en tant que renseignements personnels et que des règles spécifiques pourraient s'appliquer à leur divulgation par voie électronique.

2. Signature par des personnes morales ou physiques

61. "Projet d'article D

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

2) Une personne morale peut identifier un message de données en apposant à ce message la clé 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.

Observations

62. La disposition ci-dessus vise à préciser les conditions dans lesquelles les signatures numériques peuvent servir à lier une personne morale. Elle établit une distinction entre les deux fonctions remplies par la "signature" en vertu de l'article 7 1) a) de la Loi-type, à savoir identifier l'auteur d'un message et indiquer qu'elle approuve l'information contenue dans le message. Alors que les deux fonctions seraient normalement remplies au moyen d'une clé unique certifiée pour une personne physique, les clés publiques certifiées pour les personnes morales serviraient uniquement à donner une assurance quant à l'identité de la personne morale, en sa qualité d'expéditeur du message. La "signature numérique" d'une personne morale aurait donc un effet limité. Pour que le message soit approuvé, il faudrait, en plus de la "signature numérique" (à savoir l'identification) de la personne morale, la signature numérique de la personne physique, qui servirait à la fois à identifier cette personne et à indiquer, au nom de la personne morale, l'intention d'approuver le contenu du message.

63. S'il est vrai que le projet de disposition renvoie bien à "une personne physique habilitée à agir au nom de" une personne morale, il n'est 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 continue ainsi à relever des règles juridiques appropriées indépendamment des règles uniformes.

3. Affectation des messages de données à signature numérique

64. "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 en fonction de cette supposition si :

a) afin de s'assurer que le message de données est bien celui de l'expéditeur, le destinataire a appliqué correctement la clé publique de l'expéditeur au message de données tel que reçu et que l'application de la clé publique de l'expéditeur a permis de conclure : que le message de données reçu avait été chiffré à l'aide de la clé privée de l'expéditeur ; et que le message initial n'a pas été altéré après avoir été chiffré à l'aide de la clé 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 clé cryptographique privée de l'expéditeur.

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

a) dès lors que le destinataire avait, ou aurait dû savoir, s'il s'était renseigné auprès du tiers authentificateur ou s'il avait pris des dispositions raisonnables, que la validité de la clé 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 dispositions raisonnables ou utilisé une procédure convenue, que le message de données n'émanait pas de l'expéditeur".

Observations

65. Le Groupe de travail souhaitera peut-être examiner la question de savoir si la question de l'attribution des messages à signature numérique ne pourrait être traitée simplement par analogie avec l'article 13 de la Loi-type. Le projet d'article E, qui prend comme modèle l'article 13 de la Loi-type, vise à illustrer les principes énoncés à l'article 13 dans le cadre des signatures numériques. Il s'appuie sur l'idée de la nécessité d'une certitude quant à l'effet juridique des signatures numériques, actuellement considérées comme une procédure d'authentification très sûre. Le projet de disposition attribue une grande responsabilité à l'expéditeur d'un message sur lequel est apposée sa signature numérique. On peut rappeler que, en vertu de l'alinéa c) de l'article 2) de la Loi-type, le terme "expéditeur" désigne la personne par laquelle, ou au nom de laquelle, le message de données est réputé avoir été envoyé. Le projet de disposition illustre la nécessité pour tout usager d'une signature numérique de protéger sa clé privée qui, si elle est appliquée pour chiffrer un message, créera une présomption absolue que le message était bien celui de l'expéditeur réputé avoir envoyé le message.

4. Annulation des certificats

66. "Projet d'article F

1) Le détenteur d'un couple certifié de clés 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 clés est tenu d'annuler le certificat correspondant lorsqu'il apprend que la clé cryptographique privée a été perdue, compromise ou risque d'être utilisée à mauvais escient à d'autre 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".

Observations

67. Le Groupe de travail souhaitera peut-être noter qu'au cas où il serait prévu dans les règles uniformes sur les signatures numériques que l'annulation d'un certificat devient effectif dès que celui-ci a été reçu par le tiers authentificateur, le paragraphe 4) du projet d'article H (responsabilité) pourrait 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.

5. Registre des certificats

68. "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 dix ans après la date d'annulation ou d'expiration de la période de validité de tout certificat émis par ce tiers authentificateur".

Observations

69. Le Groupe de travail voudra peut-être examiner la question de savoir si le registre des certificats doit être mis à la disposition du public ou si l'accès à ce registre doit d'une manière ou d'une autre être limité aux seules parties intéressées. Quant à la durée durant laquelle ce registre devra être conservé, le Groupe de travail voudra peut-être décider si une durée déterminée doit être l'objet d'une règle uniforme, si le choix de cette durée doit être laissé à la discrétion des Etats ou s'il y a lieu de prévoir un critère plus souple, par exemple, la simple indication qu'il devrait être possible d'accéder au registre pour vérifier les certificats durant la période de validité de chaque certificat, et ce jusqu'à la fin de la période durant laquelle les messages comportant une signature numérique relevant des certificats délivrés par le tiers authentificateur seraient utilisés ou auraient besoin d'être vérifiés, solution qui obligerait peut-être à prévoir plusieurs périodes, en fonction des lois existantes en matière de limitation et de prescription.

6. Responsabilité

70. "Projet d'article H

1) Un tiers authentificateur homologué sera responsable devant toute personne ayant agi de bonne foi et s'étant fiée à un certificat délivré par le 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 [même si la perte n'est pas imputable] [si la perte est imputable] à une négligence de la part du tiers authentificateur.

2) Variante X La responsabilité pour toute perte individuelle ne dépassera pas [montant]. ... [l'Etat qui édicte la loi choisit l'organe ou l'autorité compétente chargée de réviser le montant maximum] peut modifier ce montant tous les deux pour tenir compte de l'évolution des prix.

Variante Y ... [l'Etat qui édicte la loi choisit l'organe ou l'autorité compétente chargée de promulguer des règlements ayant trait 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 y est pour quelque chose, soit délibérément, soit par négligence, l'indemnisation peut être réduite, voire ne pas être accordée du tout.

[4) Lorsqu'un tiers authentificateur homologué a été notifié de l'annulation d'un certificat, l'autorité enregistrera cette annulation immédiatement. Si l'autorité faillit à cette tâche, elle sera responsable de toute perte encourue par l'utilisateur].

Observations

71. Le Groupe de travail souhaitera peut-être se pencher sur la question de savoir si une disposition sur la responsabilité devrait être assez vaste pour englober les cas autres que ceux de négligence dont se serait rendue coupable le tiers authentificateur. Il voudra peut-être également déterminer si, et dans quelle mesure, l'autonomie des parties devrait jouer, pour permettre aux tiers authentificateurs de contrôler, au moyen d'accords commerciaux avec les utilisateurs, l'étendue de leur responsabilité.

72. Le Groupe de travail voudra peut-être envisager l'élaboration d'une disposition "sécurité" dans le sens que voici :

"Un tiers authentificateur qui applique [cette loi] [ces règles] et toute autre loi ou contrat applicable n'est pas tenue responsable en cas de perte

1) encourue par le détenteur d'un certificat délivré par ce tiers authentificateur du fait que le détenteur a fait confiance à ce certificat, ou

2) causée par la confiance en un certificat délivré par ce tiers authentificateur à une signature numérique vérifiable au moyen d'une clé publique énumérée dans un certificat émis par ce tiers authentificateur, ou à une information figurant dans un tel certificat".

7. Questions de certification croisée

73. "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'Etat 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.

Observations

74. Le projet d'article I s'appuie sur la notion selon laquelle la reconnaissance des certificats étrangers devrait relever de l'autorité locale de certification, sur le mode de la réciprocité. Lors de son examen des questions de certification croisée, le Groupe de travail souhaitera peut-être examiner la question de savoir si une réciprocité pleine et entière doit être garantie ou si des garanties quant à l'exactitude et à la validité des certificats étrangers n'ont pas nécessairement à être donnés au même niveau par toutes les autorités faisant partie du mécanisme de certification croisée. Le Groupe de travail souhaitera peut-être également déterminer si l'intervention de l'Etat s'imposerait nécessairement s'agissant de la reconnaissance des certificats étrangers.

75. A titre de variante du projet d'article I, le Groupe de travail pourrait envisager la démarche adoptée dans les projets de loi de certains pays, dans le

cadre desquels la reconnaissance de certificats étrangers ne peut intervenir que sur la base d'accords internationaux bilatéraux ou multilatéraux.

8. Relations entre utilisateurs et tiers authentificateurs

76. "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) A 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'utilisations 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.

2) 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].

3) 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.

4) 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.

III. INCORPORATION PAR REFERENCE

A. Le point du débat

77. A la vingt-huitième session du Groupe de travail, il a été proposé d'inclure dans le projet de Loi-type de la CNUDCI sur certains aspects juridiques de l'échange de données informatisées (EDI) et des moyens connexes de communication une disposition aux termes de laquelle certains termes et conditions, qui

pourraient être incorporés dans un enregistrement de données par simple référence, se verraient reconnaître les mêmes effets juridiques que s'ils avaient été énoncés expressément dans le texte de l'enregistrement de données. Il a été déclaré que la question de l'incorporation par référence de certains termes dans des messages EDI était essentielle pour les utilisateurs de l'EDI et qu'il importait d'éviter toute incertitude lorsque cette méthode était utilisée. Il a été déclaré que l'on pouvait avancer que l'EDI était essentiellement un système d'incorporation par référence, car les messages EDI seraient sans objet et auraient peu de valeur contractuelle si n'y étaient pas incorporées par référence les normes pertinentes de communication. Il a été décidé que le Groupe de travail, à une session ultérieure, examinerait la question de l'incorporation de termes et conditions dans un message de données par simple référence à ces termes et conditions (A/CN.9/406, para. 90 et 178).

78. A la vingt-neuvième session du Groupe de travail, deux projets de disposition sur l'incorporation par référence ont été proposés, l'un par l'Observateur de la Chambre de commerce internationale (A/CN.9/WG.IV/PW.65) et l'autre par le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord (A/CN.9/WG.IV/WP.66). L'opinion dominante a été que la question n'était pas encore prête à être incluse dans la Loi-type et méritait une étude plus approfondie. Il a été dit que les deux propositions présentées au Groupe de travail devaient être précisées davantage sur un certain nombre de points tels que le point de savoir quels termes seraient incorporés et dans quelles circonstances. De plus, il a été dit que les deux propositions risquaient de paraître empiéter sur les règles générales du droit des contrats. Il a été déclaré en outre que l'incorporation par référence en milieu électronique n'avait pas à être traitée dans la Loi-type puisqu'elle soulevait essentiellement les mêmes questions que l'incorporation par référence en milieu papier, lesquelles étaient traitées dans le droit général des contrats. Enfin, il a été dit qu'une disposition faisant une distinction entre l'incorporation par référence dans les communications sur papier et dans les communications EDI serait incompatible avec l'approche suivie jusqu'à présent par le Groupe de travail, laquelle visait à assurer la "neutralité" quant aux moyens employés. Il a été dit, en réponse, qu'il y avait, parmi les praticiens, le sentiment que le problème de l'incorporation par référence était plus complexe en milieu EDI qu'en milieu papier, notamment parce que le nombre des communications en jeu était plus grand et que les termes incorporés par référence risquaient d'être plus difficiles à déterminer s'ils prenaient la forme de messages de données. Des praticiens pensaient aussi qu'il y avait besoin de dispositions spécifiques traitant de l'incorporation par référence dans le contexte des communications électroniques. Une autre question était qu'en raison du nombre des messages de données intervenant dans une relation contractuelle particulière menée par EDI, le problème de la "bataille des formules" risquait particulièrement de surgir dans le contexte des communications électroniques. Le Groupe de travail est convenu que la question de l'incorporation par référence aurait peut-être besoin d'être examinée davantage dans le cadre de travaux à venir (A/CN.9/407, para. 100 à 105 et 117).

79. A sa trentième session, le Groupe de travail a été généralement d'avis que des travaux sur l'incorporation par référence dans le contexte de l'EDI étaient nécessaires. Selon une opinion, il faudrait, si l'on tentait d'établir des normes juridiques pour l'incorporation de clauses de référence dans des messages de données, que les trois conditions suivantes soient respectées : 1) la clause de référence devrait être insérée dans le message de données ; 2) le document référencé, par exemple des conditions générales, devrait être effectivement connu de la partie contre laquelle il peut être invoqué ; et 3) le document référencé devrait 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, para. 114). De l'avis général de la vingt-neuvième session de la Commission, la question pourrait être traitée dans le cadre des travaux sur les tiers authentificateurs (A/51/17, para. 222).

B. Eventuelle nécessité de prévoir des règles uniformes relatives à l'incorporation par référence

80. L'incorporation par référence est un moyen concis de renvoyer de manière générale, dans un document, à des dispositions énoncées ailleurs, plutôt que de les reproduire intégralement. Par exemple, ce moyen rend inutile d'énoncer des termes normalisés fort longs, lors de la négociation ou de la conclusion d'un contrat. Les termes peuvent ainsi être incorporés dans le document ou le message de données qui y renvoie par le simple fait d'identifier suffisamment les termes et d'indiquer l'intention de les inclure. Dans un milieu électronique, l'incorporation par référence peut être définie comme la méthode au moyen de laquelle un message ou un enregistrement de données (ou une partie de l'information qui y figure) devient partie intégrante d'un autre message de données ou enregistrement distinct en renvoyant dans le premier au second, et en déclarant que le premier sera considéré comme partie intégrante du second comme s'il y était énoncé intégralement.

1. Règles classiques élaborées dans un milieu papier

a) Incorporation par référence

81. Les questions juridiques que posent l'incorporation par référence sont bien connues dans le contexte des communications sur papier, et de nombreux systèmes juridiques comportent des règles précises déterminant les conditions juridiques dans lesquelles une information qui ne figure pas expressément et intégralement dans un document écrit peut être considérée, au plan juridique, comme faisant partie intégrante de ce document. Par exemple, dans certaines conditions, le renvoi à un ou plusieurs INCOTERMS, tels que "port payé jusqu'à" ou "port payé assurance comprise jusqu'à" peut être utilisé dans un bon de commande ou une facture, en conséquence de quoi les INCOTERMS seront considérés comme étant l'un des termes du contrat de vente correspondant, sans que la définition effective de l'un ou l'autre terme ne soit énoncée intégralement dans l'un ou l'autre des documents contractuels. L'incorporation par référence des INCOTERMS peut être facilitée par le fait que ces termes ont été établis par la Chambre de commerce internationale (CCI), spécifiquement pour figurer dans des contrats sous une désignation en abrégé ou un acronyme qui sont largement connus et dont la CCI et la CNUDCI recommandent tous deux l'utilisation. Un autre exemple d'un texte souvent incorporé par référence est celui des Règles et usances uniformes relatives aux crédits documentaires (RUU 500), élaborées par la CCI. Le raisonnement juridique permettant qu'un texte tel que les RUU 500 soit incorporé par référence dans un contrat serait fondé sur la reconnaissance qu'un tel texte englobe une pratique largement connue et acceptée dans le monde entier et est censée être connue par toutes les parties en jeu.

82. En l'absence d'une telle présomption, les conditions énoncées dans les lois nationales visant à reconnaître l'incorporation par référence peuvent comporter des prescriptions strictes, telles que la connaissance effective de l'information incorporée par référence par toutes les parties, voire l'approbation expresse de cette information par la partie contre laquelle elle peut être invoquée. Cela dit, en vertu de certaines autres lois nationales, les prescriptions autorisant l'incorporation par référence sont plus souples. Par exemple, certaines des conditions juridiques prévues pour l'incorporation par référence peuvent insister sur la clarté de la clause au moyen de laquelle l'incorporation par référence est effectuée ou sur la facilité d'accès de l'information incorporée par référence.

b) "Bataille des formules"

83. Il y a lieu de ne pas confondre la question de l'incorporation par référence et celle, plus générale, connue sous le nom de "bataille des formules". Cette bataille de formules peut intervenir, par exemple, lorsque les conditions générales

proposés par un acheteur figurent en petits caractères au dos de son bon de commande, alors qu'un ensemble différent de conditions générales figure au dos de la facture du vendeur. Dans le cas où acheteur et vendeur n'ont conclu aucun accord quant aux conditions régissant un contrat donné, et où deux séries de conditions incompatibles ont été communiquées par les parties au dos de leurs documents contractuels, il faudra peut-être mettre fin à l'incertitude quant aux conditions censées régir la transaction. Dans de nombreux pays, des règles de droit des contrats ont été élaborées aux fins de mettre fin à cette ambiguïté.

2. Questions soulevées dans le cadre du commerce électronique

a) Utilisation généralisée de l'incorporation par référence

84. L'incorporation par référence est indispensable à l'usage généralisé de l'échange de données électroniques (EDI), au courrier électronique, aux certificats numériques et à d'autres modalités de commerce électronique. Par exemple, les communications au moyen de messages EDI normalisés et les communications électroniques de manière générale, sont le plus souvent structurées de telle sorte que des nombres importants de messages sont échangés, chaque message comportant une information et comptant bien plus souvent que dans le cas des documents papier sur le renvoi à des informations disponibles ailleurs. L'EDI et d'autres types de données très structurées et répondant à des formats très précis utilisent très largement l'incorporation par référence pour rendre le traitement de données plus efficace. Lors de séances antérieures du Groupe de travail, il a été dit que l'EDI et divers autres moyens de commerce électroniques étaient, essentiellement, des systèmes d'incorporation par référence. Sur un plan très pratique, les messages EDI risquent d'être assortis d'un degré de certitude juridique moindre, à moins que l'on précise la validité et l'effectivité de l'incorporation par référence aux termes, conditions, clauses, accords, normes, règles ou directives juridiques, techniques et administratifs pertinents qui peuvent s'appliquer à ces messages.

85. S'agissant des situations où une "bataille des formules" aurait lieu dans un milieu papier, il ne faut pas oublier que les communications électroniques ne sont pas prévues, et moins encore équipées, pour transmettre avec chaque message des textes tels que les conditions générales qui figurent le plus souvent au dos des documents papier. Il serait à la fois coûteux et peu efficace d'inclure toutes les conditions pertinentes. Procéder de la sorte ralentirait, voire bloquerait la communication électronique, et peut-être même réduirait l'efficacité de la notification de l'information en obligeant les parties en jeu à imprimer ou à consulter des textes aussi longs. Il est donc indispensable d'élaborer des règles déterminant les moyens par lesquels ce genre de texte pourrait être considéré comme étant incorporé dans un message. L'objectif de telles règles, si possible, serait de limiter, en milieu électronique, les difficultés qui résultent d'une bataille des formules en milieu papier ou, tout au moins, de faire en sorte que les solutions élaborées par de nombreuses lois nationales dans le but de résoudre ces difficultés dans un environnement papier puissent également jouer dans l'environnement électronique. Il y a lieu de noter que l'élaboration de telles règles n'obligerait pas forcément à modifier les solutions susceptibles de découler des lois nationales quant à la question de savoir comment résoudre une "bataille des formules".

86. Les normes permettant l'incorporation par référence de messages de données dans d'autres messages de données peuvent également être essentielles s'agissant de l'utilisation des certificats de clés publiques étant donné que ces certificats sont généralement des enregistrements brefs ayant un contenu strictement prescrit et de taille limitée. Par contre, le tiers éprouvé qui émet le certificat exigera vraisemblablement d'y faire figurer les termes pertinents limitant sa responsabilité. Le champ d'application, la finalité et l'effet d'un certificat en pratique commerciale, serait donc ambigu et empreint d'incertitude si des termes externes n'y étaient pas incorporés par référence. C'est le cas notamment dans le contexte de communications internationales mettant en jeu diverses parties qui suivent des pratiques et coutumes commerciales diverses.

87. Il a été dit à maintes reprises lors de sessions antérieures du Groupe de travail que l'élaboration de normes permettant l'incorporation de messages de données par référence dans d'autres messages de données est indispensable à la croissance de l'infrastructure commerciale sur ordinateur. Sans la certitude juridique découlant de ces normes, les transactions commerciales informatisées s'alourdiraient d'énormes quantités de matériel, difficiles à manier par les parties en jeu ainsi que par le système au moyen duquel la transaction se fait. En l'absence de telles normes uniformes, il y aurait un risque important que l'application des tests traditionnels pour déterminer la possibilité d'appliquer les termes que l'on cherche à incorporer par référence soient inefficaces une fois appliqués aux termes correspondants du commerce électronique étant donné les différences entre les mécanismes du commerce classique et ceux du commerce électronique. Par exemple, certains moyens juridiques classiques permettent de vérifier l'incorporation par référence concernent la question de savoir si les termes incorporés sont "clairs et évidents", s'ils contiennent "des mots de référence témoignant d'une intention explicite d'incorporer" ou si l'incorporation prévue est "claire et convaincante". Ces moyens pourraient créer des obstacles involontaires au désir de faciliter le commerce international. Des règles spécifiques s'imposent peut-être étant donné que les méthodes utilisées pour notifier et assurer l'accès à l'information peuvent ne pas être les mêmes dans le commerce électronique et dans le milieu papier, d'où l'éventualité que, dans certains juridictions, les règles classiques régissant l'incorporation par référence pourraient avoir comme effet une discrimination injustifiée dont le commerce électronique ferait les frais.

b) Facilité d'accès au texte incorporé

88. Le commerce électronique compte beaucoup sur le mécanisme de l'incorporation par référence. Cependant, et en même temps, la facilité d'accès au texte intégral de l'information auquel il est fait référence peut être améliorée de beaucoup par le recours aux communications électroniques. Par exemple, un message peut comporter des releveurs uniformes de ressources qui orientent le lecteur vers un document référencé. Ces releveurs uniformes de ressources peuvent constituer des "liaisons hypertexte" qui permettent au lecteur de pointer et cliquer (p. ex. à l'aide d'une souris) sur un mot clé associé au releveur uniforme de ressources, faisant alors apparaître le texte référencé.

89. Les mêmes méthodes peuvent être utilisées dans le contexte électronique pour assurer la facilité d'accès de tous les utilisateurs à un ensemble varié de textes, tels que : 1) les textes consacrant la pratique commerciale établie (p. ex. RUU 500) ; 2) les normes techniques régissant la communication ; 3) les certificats de pratique émis par les tiers authentificateurs, et 4) des renseignements plus spécifiques tels que les termes et conditions d'une entreprise. On ne saurait toutefois se fier entièrement à l'effet juridique de ces méthodes sans disposer de normes au moyen desquelles des messages de données peuvent être incorporés par référence dans d'autres messages de données.

90. La nécessité d'établir des règles sur l'incorporation par référence dans un milieu électronique provient tant de la fréquence avec laquelle les messages de données se réfèrent à des renseignements enregistrés ailleurs que de la disponibilité des moyens techniques qui font que la vérification de cette information est plus facile et plus rapide que dans un environnement papier

C. Dispositions éventuelles

91. Lors de l'élaboration d'éventuelles dispositions relatives à l'incorporation par référence en commerce électronique, le Groupe de travail souhaitera peut-être garder à l'esprit que, dans certaines juridictions, les règles existantes destinées à être utilisées dans un milieu papier s'inspirent de la notion que les termes ou autres renseignements incorporés devraient être appelés de manière appropriée à l'attention du destinataire, ou d'un tiers, selon que de besoin. Lorsque ces règles existent, il serait peut-être opportun qu'elles jouent, que l'incorporation par référence se fasse au moyen de l'EDI ou par tout autre moyen de communication.

92. Il semblerait néanmoins possible d'établir un principe général précisant que l'incorporation par référence est efficace en commerce électronique, à condition qu'il soit précisé que ce principe n'a aucun effet sur des règles déjà existantes ayant trait : 1) à l'obligation selon laquelle le contenu des termes ou de tout autre renseignement ou le lieu où on peut les trouver soit appelé à l'attention de toute partie à qui il doit s'appliquer, ou soit accessible à cette partie ; ou 2) à toute disposition juridique en vertu de laquelle ces termes doivent être acceptés avant qu'ils ne puissent faire partie d'un contrat. Le principe essentiel est que l'utilisation de l'incorporation par référence doit être reconnu de telle sorte que le fait que l'information figure ailleurs et seulement ailleurs n'empêche pas en soi que l'information fasse partie du message de données dans lequel il y est fait référence.

93. Le Groupe de travail souhaitera peut-être reprendre son examen des questions de l'incorporation par référence en se fondant sur les deux variantes suivantes :

Variante A

A moins qu'il n'en soit décidé autrement, lorsque des termes, conditions, clauses, accords, normes, règles ou directives [suffisamment] [raisonnablement] faciles d'accès sont référencés en totalité ou en partie dans un message de données, dans l'intention [manifeste] de les incorporer comme étant partie intégrante du contenu ou d'être lié par eux, ces termes seront considérés comme étant incorporés par référence dans ce message de données. Entre les parties, ces termes auront les mêmes effets juridiques et auront force de loi, comme s'ils avaient été énoncés intégralement dans le message de données, et ce dans la mesure autorisée par la loi.

Variante B

1) Cet article s'applique lorsque l'information enregistrée ou communiquée dans un message de données se réfère, ou n'est entièrement vérifiable que par référence, à une information enregistrée ailleurs ("l'information complémentaire").

2) Sous réserve du paragraphe 4), le message de données aura le même effet que si l'information complémentaire figurait expressément dans le message de données et était vérifiable uniquement par référence, si le message de données :

a) identifie l'information complémentaire :

i) au moyen d'un nom ou d'une description générique ; et

ii) en identifiant l'enregistrement, ainsi que les parties de cet enregistrement, contenant l'information complémentaire et, lorsque cet enregistrement n'est pas ouvertement disponible, le lieu où il peut se trouver ; et

b) indique expressément ou comporte l'implication claire que le message de données devrait avoir le même effet que si l'information complémentaire était exprimée intégralement dans le message de données.

3) Rien dans le présent article n'affecte :

a) toute règle de droit en vertu de laquelle il faut donner notification suffisante du contenu d'une information enregistrée ailleurs, ou de l'enregistrement ou de l'endroit où cette information peut se trouver, ou en vertu de laquelle cet enregistrement ou emplacement doit être accessible à une autre personne ; ou

b) toute règle de droit ayant trait à l'acceptation d'une offre aux fins de l'établissement d'un contrat.