



Assemblée générale

Distr. LIMITÉE

A/CN.9/WG.IV/WP.73
12 décembre 1997

FRANÇAIS
Original : ANGLAIS

COMMISSION DES NATIONS UNIES
POUR LE DROIT COMMERCIAL INTERNATIONAL
Groupe de travail sur le commerce électronique
Trente-deuxième session
Vienne, 19-30 janvier 1998

PROJET DE RÈGLES UNIFORMES SUR LES SIGNATURES ÉLECTRONIQUES

Note du Secrétariat

TABLE DES MATIÈRES

	<i>Paragraphes</i>	<i>Page</i>
INTRODUCTION	1 - 8	3
I. OBSERVATIONS GÉNÉRALES	9 - 11	4
II. PROJET DE DISPOSITIONS SUR LES SIGNATURES NUMÉRIQUES, LES AUTRES SIGNATURES ÉLECTRONIQUES, LES TIERS AUTHENTICATEURS ET LES QUESTIONS JURIDIQUES CONNEXES	12 - 75	5
CHAPITRE PREMIER. CHAMP D'APPLICATION ET DISPOSITIONS GÉNÉRALES	12 - 15	5
CHAPITRE II. SIGNATURES ÉLECTRONIQUES	16 - 46	6
Section I. Signatures électroniques sûres	16 - 36	6
Article premier. Définitions	16 - 27	6
Article 2. Présomptions	28 - 32	9
Article 3. Attribution	33 - 36	11
Section II. Signatures numériques	37 - 45	13
Article 4. Définition	37 - 38	13
Article 5. Effets	39 - 44	14
[Article 6. Signature par des personnes morales	45	16
Section III. Autres signatures électroniques	46	16

TABLE DES MATIÈRES (*suite*)

	<i>Paragraphes</i>	<i>Page</i>
CHAPITRE III. TIERS AUTHENTICATEURS ET QUESTIONS CONNEXES	47 - 72	17
Article 7. Tiers authentificateur	47 - 49	17
Article 8. Certificat	50 - 57	18
Article 9. Déclaration relative aux pratiques d'authentification	58 - 60	20
Article 10. Garanties données au moment de l'émission d'un certificat ..	61 - 63	21
Article 11. Responsabilité contractuelle	64 - 65	23
Article 12. Responsabilité du tiers authentificateur envers les parties se fiant aux certificats	66 - 67	23
Article 13. Annulation d'un certificat	68	25
Article 14. Suspension d'un certificat	69	26
Article 15. Registre des certificats	70 - 71	26
Article 16. Relations entre les parties se fiant aux certificats et le tiers authentificateur	72	27
CHAPITRE IV. RECONNAISSANCE DES SIGNATURES ÉLECTRONIQUES ÉTRANGÈRES	73 - 75	28
Article 17. Tiers authentificateurs étrangers offrant des services en vertu des présentes Règles	73	28
Article 18. Approbation des certificats étrangers par les tiers authentificateurs nationaux	74	29
Article 19. Reconnaissance des certificats étrangers	75	29

INTRODUCTION

1. À sa vingt-neuvième session (1996), la Commission a décidé d'inscrire à son ordre du jour les questions des signatures numériques et des tiers authentificateurs. Le Groupe de travail sur le commerce électronique a été prié d'examiner l'opportunité et la faisabilité de l'établissement de règles uniformes sur ces questions. Il a été convenu que, dans le cadre des travaux de sa trente et unième session, le Groupe de travail pourrait élaborer un projet de règles sur certains de leurs aspects. Il a été prié de fournir à la Commission des éléments d'information suffisants pour permettre à cette dernière de se prononcer en toute connaissance de cause sur le champ d'application des règles uniformes à élaborer. S'agissant de donner un mandat plus précis au Groupe de travail, il a été convenu que les règles uniformes devraient porter sur des questions telles que le fondement juridique des opérations de certification, y compris les nouvelles techniques d'authentification et de certification numériques; l'applicabilité de la certification; la répartition des risques et des responsabilités entre utilisateurs, prestataires et tiers dans le contexte de l'utilisation de techniques de certification; les questions spécifiques à la certification sous l'angle de l'utilisation de registres; et l'incorporation par référence¹.

2. À sa trentième session (1997), la Commission était saisie du rapport du Groupe de travail sur les travaux de sa trente et unième session (A/CN.9/437). S'agissant de l'opportunité et de la faisabilité de l'élaboration de règles uniformes sur les questions des signatures numériques et des tiers authentificateurs, le Groupe de travail a indiqué à la Commission qu'il était parvenu à un consensus quant à l'importance et à la nécessité de travailler à l'harmonisation du droit dans ce domaine. Bien que n'ayant pas pris de décision ferme sur la forme et la teneur de ces travaux, il était parvenu à la conclusion préliminaire qu'il était possible d'entreprendre l'élaboration d'un projet de règles uniformes tout au moins sur les questions concernant les signatures numériques et les tiers authentificateurs, et éventuellement sur des questions connexes. Le Groupe de travail a rappelé que, outre les signatures numériques et les tiers authentificateurs, les travaux dans le domaine du commerce électronique devaient peut-être concerner aussi les questions touchant des techniques autres que la cryptographie à clef publique, les questions générales concernant les fonctions exercées par les tiers fournisseurs de services et les contrats électroniques (A/CN.9/437, par. 156 et 157). S'agissant de la question de l'incorporation par référence, le Groupe de travail a conclu qu'il n'y avait pas besoin de nouvelle étude du Secrétariat, car les problèmes fondamentaux étaient bien connus, et il était clair que de nombreux aspects du conflit de formulaires et des contrats d'adhésion devraient être réglés par les lois applicables en raison, par exemple, de la protection du consommateur et d'autres considérations d'ordre public. Le Groupe de travail a donc été d'avis que cette question devrait être la première des questions de fond inscrite à l'ordre du jour de sa prochaine session (A/CN.9/437, par. 155).

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

4. S'agissant du champ d'application et de la forme exacts de ces règles uniformes, il a été généralement convenu qu'aucune décision ne pouvait être prise à un stade aussi précoce. On a estimé qu'il était justifié que le Groupe de travail axe son attention sur les questions relatives aux signatures numériques étant donné le rôle apparemment prédominant joué par la cryptographie à clef publique dans la nouvelle pratique du commerce électronique mais les règles uniformes devraient être compatibles avec l'approche techniquement neuve adoptée dans la Loi type de la CNUDCI sur le commerce électronique. Ainsi, les règles uniformes ne devraient pas décourager l'utilisation d'autres techniques d'authentification. En outre, s'agissant de la cryptographie à clef publique, il pourrait être nécessaire de prendre en considération, dans ces règles uniformes, divers niveaux de sécurité et de reconnaître les divers effets juridiques et niveaux de responsabilité correspondant aux différents types de services fournis dans le contexte des signatures numériques. S'agissant des tiers authentificateurs, la

Commission a certes reconnu la valeur des normes issues du marché mais il a été largement considéré que le Groupe de travail pourrait utilement envisager l'établissement d'un ensemble minimum de normes que les tiers authenticateurs devrait respecter, en particulier dans les cas de certification internationale.

5. On a en outre émis l'avis que dans le cadre des travaux futurs relatifs au commerce électronique, le Groupe de travail pourrait être amené, à un stade ultérieur, à examiner les questions de la compétence, de la loi applicable et du règlement des conflits sur l'Internet. La Commission a été informée qu'un colloque sur les questions de la compétence et de la loi applicable sur l'Internet se tiendrait en juin 1997 sous les auspices de la Conférence de La Haye de droit international privé. La Commission a également été informée qu'une conférence internationale organisée par l'OCDE en novembre 1997 tenterait de définir une approche coordonnée sur les questions du commerce électronique entre les gouvernements, les organisations intergouvernementales, les organisations non gouvernementales et les groupes du secteur privé intéressés. La Commission a exprimé l'espoir que le Secrétariat pourrait assister à ces deux manifestations et faire un rapport².

6. La présente note contient un projet révisé de dispositions devant être examinées en vue de leur incorporation éventuelle dans les Règles uniformes. Ces dispositions traitent des signatures numériques, d'autres signatures électroniques, des tiers authenticateurs et de questions juridiques connexes. Elles ont été élaborées à la suite des délibérations et des décisions du Groupe de travail à sa trente et unième session, dont il est rendu compte dans le rapport sur les travaux de cette session (A/CN.9/437), et à la suite des délibérations et des décisions de la Commission à sa trentième session, dont il est rendu compte ci-dessus. Le projet de dispositions est fondé, en particulier, sur le principe adopté par le Groupe de travail selon lequel ses travaux dans le domaine des signatures numériques prendraient la forme de projets de dispositions juridiques (A/CN.9/437, par. 27). Il tient également compte de la décision prise par le Groupe de travail à sa session précédente selon laquelle les éventuelles règles uniformes concernant les signatures numériques devraient s'inspirer de l'article 7 de la Loi type de la CNUDCI sur le commerce électronique (dénommée ci-après "la Loi type") et être considérées comme définissant la manière dont une méthode fiable pourrait servir à "identifier une personne" et "signifier qu'une personne approuve" l'information contenue dans un message électronique. De façon plus générale, en attendant une décision finale sur la relation entre la Loi type, les règles uniformes et d'éventuelles règles sur l'incorporation par référence (voir A/CN.9/437, par. 151 à 155), le projet de dispositions doit être conforme aux principes énoncés et à la terminologie employée dans la Loi type (A/CN.9/437, par. 26).

7. La présente note ne traite pas les questions de la compétence, de la loi applicable et du règlement des conflits sur l'Internet, de la formation et de l'exécution des contrats dans un environnement électronique, non plus que toute autre question qui pourrait devoir être examinée par le Groupe de travail à une future session. Un rapport oral sera présenté au Groupe de travail concernant le colloque sur les questions de la compétence et de la loi applicable sur l'Internet, qui s'est tenu en juin 1997 sous les auspices de la Conférence de La Haye de droit international privé et la Conférence internationale organisée par l'OCDE en novembre 1997 (voir ci-dessus, par. 5).

8. Pour établir la présente note, le Secrétariat a bénéficié de l'aide d'un groupe d'experts dont certains avaient été invités par lui et d'autres désignés par les pays et les organisations internationales intéressés.

I. OBSERVATIONS GÉNÉRALES

9. Les Règles uniformes ont pour objectif, comme le montre le projet de dispositions figurant dans la deuxième partie de la présente note, de faciliter un développement de l'utilisation des signatures numériques dans les transactions commerciales internationales. S'inspirant des nombreux instruments législatifs déjà en

vigueur ou en cours d'élaboration dans un certain nombre de pays, ce projet de dispositions vise à prévenir une discordance des règles juridiques applicables au commerce électronique en offrant un ensemble de normes sur lesquelles se fonder pour reconnaître les effets juridiques des signatures numériques et autres signatures électroniques, avec l'aide éventuelle des tiers authenticateurs, pour lesquels un certain nombre de règles de base sont aussi prévues.

10. Axées sur les aspects de droit privé des transactions commerciales, les Règles uniformes ne tentent pas de régler toutes les questions pouvant surgir dans le cadre d'une utilisation accrue des signatures électroniques. En particulier, elles ne traitent pas des aspects relatifs à l'ordre public, au droit administratif, au droit de la consommation ou au droit pénal que les législateurs nationaux peuvent être appelés à prendre en considération lorsqu'ils établissent un cadre juridique général pour les signatures électroniques.

11. S'inspirant de la Loi type, les Règles uniformes visent à faire ressortir en particulier le principe de la neutralité quant aux techniques employées, se fondent sur une approche ne désavantageant pas les équivalents fonctionnels des concepts et pratiques traditionnels fondés sur le papier et font une large place à l'autonomie des parties. Elles devraient constituer à la fois des normes minimales dans un environnement "ouvert" (c'est-à-dire où les parties communiquent par des moyens électroniques sans convention préalable) et des règles par défaut dans un environnement "fermé" (c'est-à-dire où les parties sont liées par des règles et procédures contractuelles préexistantes qu'elles doivent suivre lorsqu'elles communiquent par des moyens électroniques).

II. PROJET DE DISPOSITIONS SUR LES SIGNATURES NUMÉRIQUES, LES AUTRES SIGNATURES ÉLECTRONIQUES, LES TIERS AUTHENTICATEURS ET LES QUESTIONS JURIDIQUES CONNEXES

CHAPITRE PREMIER. CHAMP D'APPLICATION ET DISPOSITIONS GÉNÉRALES

12. Lorsqu'il étudiera le projet de dispositions qu'il est proposé d'inclure dans les Règles uniformes, le Groupe de travail souhaitera peut-être examiner, de manière plus générale, la relation entre ces Règles uniformes et la Loi type. Il voudra peut-être, en particulier, formuler des propositions à la Commission sur la question de savoir si des règles uniformes relatives aux signatures numériques devraient constituer un instrument juridique à part entière où si elles devraient être incorporées dans une version élargie de la Loi type, comme troisième partie, par exemple.

13. Que les Règles uniformes soient élaborées en tant qu'instrument séparé ou qu'elles soient ajoutées à la Loi type, il est proposé qu'elles comprennent des dispositions s'inspirant des articles premier (Champ d'application), 2 a), c) et e) (Définition des termes "message de données", "expéditeur" et "destinataire"), 3 (Interprétation), 7 (Signature) et 13 (Attribution des messages de données) de ladite Loi. Ces articles ne sont pas reproduits dans la présente note, mais on observera que, pour ses travaux, le Secrétariat est parti du principe que de telles dispositions feraient partie des Règles uniformes. En ce qui concerne le champ d'application de ces Règles, il faut se rappeler que, compte tenu de l'article premier de la Loi type, les transactions dans lesquelles interviennent des consommateurs, sans être l'élément principal des Règles uniformes, ne seraient pas exclues de leur champ d'application sauf si la loi applicable à ce type de transactions dans l'État adoptant était incompatible avec les Règles uniformes (voir A/CN.9/WG.IV/WP.71, par. 49 et 50).

14. En ce qui concerne l'autonomie des parties, la simple référence à l'article 4 (Dérogation conventionnelle) de la Loi type, peut ne pas constituer à elle seule une solution satisfaisante, étant donné que cet article établit une distinction entre les dispositions de la Loi type auxquelles il peut être librement dérogé par contrat et celles qui doivent être considérées comme des règles de droit, sauf si la loi applicable en dehors de la Loi type autorise

une telle dérogation conventionnelle. En ce qui concerne les signatures électroniques, il est nécessaire, étant donné l'importance pratique des réseaux "fermés", de prévoir une large reconnaissance de l'autonomie des parties. Toutefois, il pourrait aussi être nécessaire de tenir compte des restrictions à la liberté contractuelle liées à l'ordre public, y compris les lois protégeant les consommateurs contre des contrats d'adhésion excessifs. Le Groupe de travail pourrait ainsi souhaiter inclure dans les Règles uniformes une disposition s'inspirant de l'article 4-1 de la Loi type, à savoir que, sauf disposition contraire des Règles uniformes ou d'une autre loi applicable, les signatures électroniques et les certificats qui ont été émis, reçus ou sur lesquels une partie s'est fondée conformément aux procédures convenues entre les parties à une transaction produisent les effets indiqués dans la convention. En outre, le Groupe de travail pourrait envisager d'établir une règle d'interprétation en vertu de laquelle il faudrait, lorsque l'on détermine si un certificat, une signature électronique ou un message de données vérifié par référence à un certificat est suffisamment fiable pour un objet particulier, tenir compte de toutes les conventions pertinentes liant les parties, toute conduite à laquelle se sont conformées ces dernières et tout usage commercial pertinent.

15. En plus des dispositions susmentionnées, le Groupe de travail souhaitera peut-être examiner la question de savoir si un préambule aux Règles uniformes serait susceptible d'en préciser l'objectif, à savoir 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 les signatures numériques s'agissant de leur effet juridique (voir A/CN.9/WG.IV/WP.71, par. 51).

CHAPITRE II. SIGNATURES ÉLECTRONIQUES

Section I. Signatures électroniques sûres

Article premier. Définitions

Aux fins des présentes Règles :

- a) Le terme "signature" désigne tout symbole employé, ou toute autre procédure de sécurité adoptée par une personne [ou en son nom] en vue d'identifier cette personne et d'indiquer qu'elle approuve les renseignements sur lesquels la signature est apposée;
- b) Les termes "signature électronique" désignent [une signature] [des données] sous forme électronique contenue(s) dans un message de données, ou jointes ou logiquement associées audit message [et utilisée(s) par une personne [ou en son nom] en vue d'identifier cette personne et d'indiquer qu'elle approuve la teneur du message de données] [et utilisée(s) pour satisfaire aux conditions énoncées à [l'article 7 de la Loi type de la CNUDCI sur le commerce électronique]];
- c) Les termes "signature électronique sûre" désignent une signature électronique qui
 - i) est une signature numérique au sens de l'article 4 et satisfait aux conditions énoncées à l'article 5; ou
 - ii) peut, à partir du moment où elle apposée, être authentifiée comme celle d'une personne particulière à l'aide d'une procédure de sécurité qui est liée exclusivement à la personne qui l'utilise; susceptible d'identifier rapidement, objectivement et automatiquement cette personne; créée d'une manière ou à l'aide d'un moyen dont seule la personne l'utilisant a

le contrôle; et liée au message de données auquel elle se rapporte d'une manière qui permette de l'invalider si le message est altéré; ou

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

Références

A/CN.9/437, paragraphes 29 à 50 et 90 à 113 (projet d'articles A, B et C);

A/CN.9/WG.IV/WP.71, paragraphes 52 à 60.

Observations

16. Le projet d'article premier vise à tenir compte de la décision prise par le Groupe de travail à sa trentième session selon laquelle, conformément au principe de la neutralité qui était celui de la Loi type, les Règles uniformes ne devraient décourager l'utilisation d'aucune technique offrant une méthode suffisamment fiable pour remplacer les signatures manuscrites et autres signatures utilisées dans les documents sur papier, conformément à l'article 7 de la Loi type. Même si les Règles uniformes portent essentiellement sur les questions relatives aux signatures numériques, il faudrait adopter une approche plus générale et examiner également les questions relatives à d'autres techniques de signature électronique (voir A/CN.9/437, par. 22)

17. La définition des termes "signature" et "signature électronique", aux alinéas a) et b), permet de délimiter dans ses grandes lignes le champ d'application des Règles uniformes, qui couvrent aussi toutes les techniques applicables pour fournir un équivalent fonctionnel à une signature manuscrite, au sens de l'article 7 de la Loi type. Il convient de noter que la définition du terme "signature", qui reprend simplement le paragraphe 1 a) de l'article 7 de la Loi type sous forme de définition, ne vise pas à remplacer ou à modifier de quelque autre façon toute définition des termes "signature" ou "signature manuscrite" pouvant exister en dehors des Règles uniformes (c'est-à-dire dans la législation nationale ou dans la jurisprudence). Cette définition doit essentiellement servir de base aux définitions ultérieures des termes "signature électronique" et "signature électronique sûre". Elle peut également servir de référence utile dans les pays où n'existe actuellement aucune définition du terme "signature".

18. Les trois niveaux de définition donnés dans le projet d'article premier (c'est-à-dire "signature", "signature électronique" et "signature électronique sûre") devraient fournir au Groupe de travail un outil analytique et correspondent à une distinction devenue courante dans les projets de lois d'un certain nombre de pays. Toutefois, il ne sera peut-être pas nécessaire, selon la teneur des Règles uniformes, de conserver les trois. Si le Groupe de travail décide de se concentrer sur un seul effet juridique de la signature électronique (à savoir sa reconnaissance comme équivalent fonctionnel d'une signature manuscrite), on pourrait n'envisager qu'une seule catégorie de "signatures électroniques". Les notions que définissent actuellement les termes "signature électronique" et "signature électronique sûre" pourraient ainsi être regroupées dans une catégorie juridique unique, quels que soient le nombre et la diversité des techniques envisagés dans cette catégorie.

19. La principale définition à retenir pour délimiter le champ d'application des Règles uniformes est celle qui est actuellement énoncée à l'alinéa c) sous l'intitulé "signature électronique sûre". Pour ce qui est du choix des termes, on pourra noter que le mot "sûre" ne signifie pas que telle ou telle technique peut, en fait ou en droit, offrir une sécurité absolue. Le but recherché est uniquement de qualifier un niveau supérieur de fiabilité d'une

signature électronique par référence à un ensemble de critères qui, une fois satisfaits, produiraient certains effets juridiques.

20. L'alinéa c), qui doit constituer une base pour les effets juridiques devant découler de l'utilisation de signatures électroniques, vise également à traduire l' "approche double" adoptée par le Groupe de travail à sa précédente session. Cette approche résultait des deux formules envisagées, à savoir l'établissement de critères d'agrément des tiers authenticateurs par l'État et la reconnaissance de critères applicables aux tiers authenticateurs ne faisant pas partie d'une infrastructure à clef publique régie par l'État. Le Groupe de travail est parvenu à la conclusion que les deux formules n'étaient pas nécessairement incompatibles. Elles se différenciaient peut-être par les modalités d'application des effets juridiques aux signatures numériques dans l'un ou l'autre cas. Lorsque c'était l'État qui autorisait ("agréait") le tiers authenticateur, il ne le faisait qu'après s'être assuré que ce dernier satisfaisait aux critères, condition indispensable pour que les certificats émis par le tiers authenticateur puissent avoir un effet juridique. Dans le second cas, le tiers authenticateur n'avait pas besoin, pour exercer son activité, de prouver qu'il remplissait les critères. Toutefois, si les certificats qu'il émettait venaient à être contestés (par exemple devant les tribunaux ou une instance d'arbitrage), l'organe appelé à statuer devrait, pour se prononcer sur leur fiabilité, déterminer s'ils émanaient d'un tiers authenticateur répondant bien aux critères (voir A/CN.9/437, par. 48).

21. Outre qu'il permet le recours à des tiers authenticateurs agréés ou non par l'État, l'alinéa c) étend le champ d'application des Règles uniformes aux dispositifs d'authentification ne nécessitant pas le recours à un tiers authenticateur, quel qu'il soit, ou autre "tiers de confiance". Le terme "sûre" permet ainsi de prendre en considération à la fois les systèmes d'agrément donnant aux États adoptants la possibilité de garantir la qualité et la fiabilité des signatures numériques et les pratiques issues du marché qui peuvent être fondées sur d'autres formes de signatures électroniques.

22. En vertu du sous-alinéa c) i), une signature numérique serait réputée sûre en vertu des Règles uniformes si elle était appliquée dans le cadre d'une infrastructure à clef publique établie par l'État adoptant. En l'absence d'une telle infrastructure, ou en complément, tout type de signature électronique (c'est-à-dire des signatures numériques ou d'autres signatures électroniques appliquées avec ou sans l'intervention de tiers authenticateurs ou d'autres tiers de confiance) pourrait être considéré comme sûr, à condition de remplir des conditions minimales. Pour fournir une norme de base servant à évaluer la qualité de ces signatures électroniques, le sous-alinéa c) ii) énumère quatre critères : l'exclusivité, l'identification, la fiabilité et le lien avec l'information signée.

23. La condition selon laquelle une signature électronique sûre doit être liée exclusivement à la personne qui l'utilise vise à éliminer toute probabilité raisonnable de production d'une même signature par plusieurs personnes, sauf cas de fraude ou autre conduite répréhensible. Cette condition pourrait être aussi vraisemblablement remplie par une signature basée sur la biométrie, incorporant certains attributs propres au signataire tel qu'une empreinte digitale ou rétinienne, ou bien encore, pour une signature numérique, lorsque la paire de clefs employée par le signataire a été créée de manière aléatoire et est suffisamment longue pour que la probabilité que toute autre personne crée la même paire de clefs soit extrêmement faible.

24. Une signature sûre devrait permettre d'identifier le signataire, ce qui ne veut pas dire qu'elle doit se composer du nom du signataire ou l'inclure. Il suffirait que l'identification puisse se faire par référence à d'autres sources d'information. Ainsi, une signature numérique peut identifier le signataire par référence à un certificat émis par un tiers authenticateur. L'important est que le processus d'identification soit relativement rapide, objectif et automatique. Par exemple, si l'on peut partir du principe qu'une signature manuscrite permet d'identifier le signataire, en revanche une telle identification n'est normalement ni rapide ni automatique et permet rarement une détermination objective. Il arrive fréquemment que la signature elle-même soit illisible.

Même lorsqu'elle est lisible et peut à terme permettre d'identifier le signataire, les délais et la certitude du processus d'identification ne répondent pas toujours aux exigences du commerce électronique. Ainsi, il n'est pas toujours possible de certifier qu'une signature manuscrite est bien celle de tel ou tel individu (si celui-ci nie, ou en l'absence d'un témoin à la signature) sans le témoignage d'un graphologue ayant comparé les signatures non contestées du signataire supposé avec la signature analysée. Il est alors peu probable que l'on parvienne rapidement et automatiquement à un résultat et la conclusion du graphologue est, à maints égards, plus subjective qu'objective. En revanche, l'utilisation d'un numéro d'identification personnel dans un guichet bancaire automatique permet à la banque d'identifier automatiquement, objectivement et rapidement une personne associée à une adresse particulière et à un numéro de compte particulier en cas de retrait de fonds. Cette personne ne peut nier que la demande de fonds porte sa signature (elle peut nier par contre avoir signé la demande, ce qui fait entrer en jeu le critère de la fiabilité).

25. La procédure utilisée pour signer le message doit non seulement permettre d'identifier une personne comme étant le signataire, mais aussi garantir raisonnablement que ladite personne est bien celle qui a signé le message. Une procédure de sécurité exigeant l'utilisation d'une méthode ou d'un moyen dont seule la personne qui a créé la signature a le contrôle peut satisfaire à ce critère de fiabilité. Le recours à un tiers de confiance peut aussi donner le niveau de fiabilité requis. Il peut exister d'autres moyens encore. Le Groupe de travail pourrait souhaiter examiner d'autres approches permettant de garantir un niveau de fiabilité acceptable.

26. Une signature sûre doit être liée au message de données signé d'une manière qui entraîne son invalidation si le message est modifié. Un tel lien peut être considéré comme une condition fondamentale, puisqu'il serait possible, sinon, d'extraire simplement la signature d'un message de données pour l'insérer dans un autre.

27. Les sous-alinéas c) i) et ii) doivent s'appliquer en l'absence d'un arrangement contractuel préexistant concernant les signatures électroniques entre l'expéditeur et le destinataire du message de données signé. Toutefois, pour suivre l'approche adoptée dans la Loi type, les Règles uniformes devront peut-être réaffirmer la validité des mécanismes contractuels concernant l'authentification des messages de données. L'alinéa c) iii) valide ainsi les accords en système fermé. Le Groupe de travail souhaitera peut-être examiner la question de savoir si le libellé entre crochets ("entre les parties participant à la création, l'envoi, la réception, la conservation ou le traitement de toute autre manière des messages de données dans la conduite ordinaire de leurs affaires"), qui reprend largement le libellé figurant dans la Loi type, est nécessaire pour limiter les effets de l'autonomie des parties sur les utilisations commerciales des signatures électroniques, à l'exclusion des transactions dans lesquelles interviennent des consommateurs (voir A/CN.9/437, par. 24).

Article 2. Présomptions

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

- a) le message de données n'a pas été altéré après que la signature électronique sûre y a été apposée;
- b) la signature électronique sûre est la signature de la personne à laquelle elle se rapporte; et
- c) la signature électronique sûre a été apposée par cette personne dans l'intention de signer le message.

2. En ce qui concerne un message de données authentifié à l'aide d'une signature électronique autre qu'une signature électronique sûre, aucune des dispositions des présentes Règles n'a d'incidence sur les règles

juridiques ou les règles de preuve existantes concernant l'obligation d'établir l'authenticité et l'intégrité d'un message de données ou d'une signature électronique.

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

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

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

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

c) une preuve relative à des faits dont la partie s'étant fiée à la signature avait connaissance, qui tendraient à indiquer que la confiance en la procédure de sécurité n'était pas raisonnable. Le caractère commercialement raisonnable d'une procédure de sécurité convenue par les parties au titre du sous-alinéa c) iii) et de l'article premier doit être déterminé en fonction des objectifs de la procédure et des circonstances commerciales au moment où les parties sont convenues d'adopter la procédure, notamment la nature de la transaction, le niveau technologique des parties, le volume de transactions analogues effectuées par l'une ou l'autre d'entre elles ou les deux, l'existence d'autres formules proposées à la partie mais rejetées par elle, le coût d'autres procédures, et les procédures généralement utilisées pour des types de transactions analogues.]

Références

A/CN.9/437, paragraphes 43, 48 et 92.

Observations

28. Le projet d'article 2 porte essentiellement sur les effets juridiques de la reconnaissance d'une "signature électronique sûre". À sa précédente session, le Groupe de travail avait examiné la possibilité de traiter certaines questions se rapportant aux signatures électroniques (par exemple la fiabilité des tiers authentificateurs et l'attribution des messages de données portant une signature numérique) en énonçant des présomptions (voir A/CN.9/437, par. 58, 70 et 120 et 121).

29. La notion de signature électronique sûre et les présomptions réfragables qui en découlent peuvent être considérées comme fondamentales pour garantir la validité d'un système de commerce électronique. Dans les transactions sur papier, une partie peut déterminer si le document et la signature sont authentiques à partir d'un certain nombre d'indicateurs, notamment le papier (présentant parfois un filigrane, un fond coloré ou d'autres indicateurs de fiabilité) sur lequel figure le message, un en-tête, des signatures manuscrites ou l'envoi par un tiers de confiance (tel que les services postaux) dans des enveloppes scellées. Les communications électroniques, en revanche, n'offrent aucun de ces éléments de fiabilité. Tout ce qui peut être communiqué est une série d'impulsions électroniques identiques en tous points et pouvant être facilement copiées ou modifiées. Dans de nombreux cas, il est donc important que le destinataire et toute autre partie se fondant sur une communication électronique sachent, au moment où ils la reçoivent ou se fondent sur cette dernière, si le message est authentique, si l'intégrité de son contenu a été protégée et s'ils seront en mesure d'établir ces deux faits en cas de différend ultérieur (établir, par exemple, devant le tribunal la non-contestation d'un message de données). À cet égard, des présomptions réfragables concernant les signatures sûres peuvent fournir aux parties

de telles assurances leur permettant de mener des activités commerciales en sachant qu'il leur sera plus facile de faire valoir leurs droits si cela se révélait nécessaire.

30. Il convient de distinguer l'effet des présomptions énoncées dans le projet d'article 2 et l'effet de l'attribution au titre du projet d'article 3. Dans le projet d'article 2, les présomptions ont pour objectif d'alléger la charge de prouver la source d'un message électronique lorsque le destinataire a vérifié la source apparente par l'utilisation d'une signature électronique sûre. La personne à laquelle la signature est associée est donc tenue de prouver que, bien que le destinataire ait vérifié la signature électronique sûre et appliqué la procédure de sécurité, cette signature n'était pas la sienne. L'établissement d'une telle présomption se justifie par le fait que les éléments de preuve nécessaires pour démontrer qui a effectivement envoyé le message sont normalement détenus par la personne à laquelle la signature est associée. Ainsi, dans le cas d'une signature numérique, la personne à laquelle la signature est associée est généralement mieux en mesure que toute autre partie de prouver que la clef privée a été volée, copiée, compromise, ou utilisée sans autorisation par un tiers. Normalement, le destinataire du message n'aura d'autre preuve que la procédure de sécurité appliquée pour prouver que la personne à laquelle la signature est associée a bien envoyé le message. Toutefois, en vertu du projet d'article 3, même si la partie à laquelle la signature est associée peut établir qu'elle n'a pas envoyé le message en question, elle peut néanmoins être tenue responsable des pertes subies par le destinataire qui s'est raisonnablement fié à cette signature, si les conditions énoncées dans cet article sont remplies.

31. Eu égard à l'approche adoptée à l'article 7 de la Loi type, le paragraphe 1 n'établit pas la présomption que le message de données comportant une signature électronique sûre constitue une obligation juridiquement contraignante. Il présume simplement que la signature électronique sûre a été apposée par le signataire supposé avec l'intention de signer le message. S'il est avéré que la personne dont la signature est apposée a été victime d'une erreur ou d'une déclaration fallacieuse ou a agi sous la contrainte, ou s'il existe toute autre cause entraînant la nullité, le message peut perdre ses effets juridiques, mais c'est à la personne qui réfute ces effets qu'incombe la mise en cause.

32. Le paragraphe 2 indique clairement qu'en l'absence de signature électronique sûre, aucune disposition des Règles uniformes ne modifie les règles ordinaires de la preuve concernant l'obligation de prouver la source d'un message. Le paragraphe 3 s'inspire de dispositions analogues de la Loi type. L'objectif est de faciliter l'exclusion de certaines situations du champ d'application du projet d'article 2 lorsqu'un intérêt légitime de l'État adoptant l'exige. Par exemple, les États adoptants peuvent décider que les présomptions établies dans le projet d'article 2 ne s'appliquent pas dans le domaine du droit pénal. Le paragraphe 4 énumère un certain nombre de manières de réfuter la présomption établie au paragraphe 1. Le Groupe de travail souhaitera peut-être examiner s'il est nécessaire d'insérer une telle disposition servant d'illustration dans le texte des Règles uniformes ou s'il serait préférable de l'insérer dans un guide ou un commentaire.

Article 3. Attribution

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

Variante B Pour ce qui est de la relation entre le détenteur d'une clef privée et toute tierce partie se fiant à une signature numérique qui peut être [vérifiée] [authentifiée] à l'aide de la clef publique certifiée correspondante, la signature numérique [est réputée être celle du

détenteur] [satisfait aux conditions énoncées à [l'article 7-1 de la Loi type de la CNUDCI sur le commerce électronique]].

2. Le paragraphe 1 ne s'applique pas si

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

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

Références

A/CN.9/437, paragraphes 188 à 124 (projet d'article E);

A/CN.9/WG.IV/WP.71, paragraphes 64 et 65.

Observations

33. À sa précédente session, le Groupe de travail a généralement estimé qu'il ne fallait pas essayer de reprendre, dans le cadre des Règles uniformes, les principes énoncés à l'article 13 de la Loi type (A/CN.9/437, par. 119 et 120). Il a toutefois été jugé nécessaire de préciser la relation entre les Règles uniformes et les articles 7 et 13 de la Loi type. À cet effet, la variante A du paragraphe 1, qui traduit un principe jugé généralement acceptable par le Groupe de travail à sa précédente session (voir A/CN.9/437, par. 120), est libellée en termes généraux afin d'englober à la fois les signatures numériques et d'autres techniques pouvant être utilisées pour produire une signature numérique sûre.

34. La variante B établit une présomption selon laquelle une signature numérique remplit les conditions de fiabilité énoncées à l'article 7 de la Loi type. Le Groupe de travail souhaitera peut-être examiner la question de savoir si une telle présomption devrait être élargie de façon à englober non seulement les signatures numériques, mais également d'autres cas où une signature électronique sûre est utilisée. Si le Groupe de travail souhaite limiter le champ d'application de la disposition aux signatures numériques, le projet d'article 3 devra être déplacé en conséquence.

35. Le Groupe de travail souhaitera peut-être examiner la question de savoir si le projet d'article 3 pourrait servir à traiter de façon plus précise de la question du moment où une personne peut être tenue comptable de la teneur d'un message de données lorsqu'elle ne l'a en fait pas envoyé et lorsqu'il est communiqué dans un environnement ouvert (c'est-à-dire sans accord préalable direct entre l'expéditeur et le destinataire (ou dans le contexte de "règles de système") quant à la procédure à appliquer pour déterminer l'attribution du message de données). Le paragraphe 3 a) de l'article 13 de la Loi type traite du cas où une "procédure que l'expéditeur avait précédemment acceptée" est appliquée, mais la Loi type ne traite pas expressément des milieux ouverts. Étant donné le niveau de sécurité élevé qu'impliquent les signatures électroniques sûres, le Groupe de travail souhaitera peut-être examiner la possibilité d'établir une règle générale selon laquelle le destinataire d'un messages de données qui se fie raisonnablement à une signature électronique sûre est fondé à considérer que le message émane de l'expéditeur.

36. Le Groupe de travail pourrait souhaiter examiner, comme exemple de disposition à cet effet, le libellé suivant :

Sauf dispositions contraires d'une autre loi applicable, une signature électronique sûre est attribuable à la personne à qui elle apparaît se rattacher, que cette personne l'ait ou non autorisée, si :

- a) elle a résulté d'actes d'une personne ayant obtenu les numéros d'accès, les codes, les logiciels, ou d'autres informations nécessaires pour la créer d'une source dont le signataire supposé a le contrôle, donnant ainsi l'impression d'émaner de cette personne;
- b) l'accès a eu lieu dans des circonstances résultant du fait que le signataire supposé n'a pas fait preuve d'une diligence raisonnable; et
- c) le destinataire s'est fié de bonne foi, à son détriment, à la source apparente du message de données.

Ce libellé a pour effet de répartir le risque de perte entre les deux parties intéressées, à savoir l'expéditeur supposé qui n'a pas signé effectivement le message en question et le destinataire qui s'est fié de bonne foi à ce message après application d'une procédure de sécurité commercialement raisonnable. Le risque de perte est imputé à l'expéditeur supposé uniquement lorsque l'apposition de sa signature résulte d'une faute de sa part. Une telle situation peut se produire lorsque la signature a été créée par une personne ayant obtenu les informations nécessaires d'une source dont l'expéditeur supposé a le contrôle et lorsque cet accès résulte du fait que l'expéditeur n'a pas fait preuve d'une diligence raisonnable. Si le destinataire se fie raisonnablement au message, l'expéditeur supposé se trouve alors lié par ce dernier. Dans tous les autres cas, le risque de perte est supporté par le destinataire, même si sa confiance était raisonnable. La référence à une autre "loi applicable" dans le chapeau peut être nécessaire pour exclure du champ d'application de la disposition proposée les transactions dans lesquelles interviennent des consommateurs.

Section II. Signatures numériques

Article 4. Définition

Aux fins des présentes Règles,

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

- a) si la transformation a été opérée à l'aide de la clef privée du signataire correspondant à sa clef publique; et
- b) si le message de données initial a été altéré après la transformation.

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

- b) Les procédures mathématiques utilisées pour créer les signatures numériques en vertu des présentes Règles sont basées sur le chiffrement à clef publique. Appliquées à un message de données, ces procédures mathématiques opèrent une transformation du

message de telle sorte qu'une personne en possession du message initial et de la clef publique de l'expéditeur peut déterminer avec exactitude :

- i) si la transformation a été opérée à l'aide de la clef privée correspondant à la clef publique de l'expéditeur ; et
- ii) si le message initial a été altéré après la transformation.

Références

A/CN.9/437, paragraphes 30 à 38 (projet d'article A);
A/CN.9/WG.IV/WP.71, paragraphes 18 à 45, 55 et 56.

Observations

37. Les différences entre les variantes A et B sont essentiellement rédactionnelles. La variante B tient compte des conclusions formulées par le Groupe de travail à sa précédente session (voir A/CN.9/437, par. 32), alors que la variante A présente un libellé plus simple, faisant fond sur la définition des termes "signature électronique". Dans les deux variantes, les termes "signature numérique" sont définis sans référence aux "tiers authentificateurs" ou aux "certificats".

38. On n'a pas tenté de donner des définitions des mots "clef privée", "clef publique", "paire de clefs" ou d'autres notions relatives à la cryptographie à clef publique. À la précédente session du Groupe de travail, il avait certes été proposé d'ajouter d'autres définitions, mais on avait mis en garde contre l'insertion, dans des règles uniformes normatives, d'un grand nombre de définitions, ce qui pourrait être contraire à la tradition législative de nombreux pays. Le Groupe de travail souhaitera peut-être examiner dans quelle mesure des définitions supplémentaires seraient nécessaires (voir A/CN.9/437, par. 29).

Article 5. Effets

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

- a) elle a été créée pendant la période d'effet d'un certificat [valide] et est vérifiée par référence à la clef publique indiquée dans ce certificat; et
- b) le certificat est considéré comme rattachant avec précision une clef publique à l'identité d'une personne pour les raisons suivantes :
 - i) le certificat a été émis par un tiers authentificateur agréé [accrédité] par [l'État adoptant indique l'organe ou l'autorité habilités à agréer le tiers authentificateur et à promulguer des règles concernant les fonctions des tiers authentificateurs agréés]; ou
 - ii) le certificat a été émis d'une autre manière par un tiers authentificateur conformément aux normes établies par ... [l'État adoptant indique l'organe ou l'autorité habilités à établir des normes reconnues concernant les fonctions des tiers authentificateurs agréés].

2. Lorsqu'une signature numérique apposée sur la totalité ou sur toute partie d'un message de données ne satisfait pas aux conditions énoncées au paragraphe 1, cette signature est considérée comme une signature

électronique sûre pour la partie du message considérée s'il existe des preuves suffisantes montrant que le certificat rattache avec précision la clef publique à l'identité de son détenteur.

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

Références

A/CN.9/437, paragraphes 43, 48 et 92.

Observations

39. Les signatures numériques devraient, si elles sont correctement mises en œuvre, constituer des signatures électroniques sûres. Encore faut-il déterminer quand la mise en œuvre d'une signature numérique a été effectuée d'une manière qui permette de qualifier cette dernière de sûre. Les signatures numériques vérifiables par référence à un certificat ne sont pas toutes sûres, en particulier lorsque l'on n'est pas certain que l'identification ou l'authentification du détenteur ou de la clef publique soit exacte. Les principaux facteurs permettant de déterminer la sûreté d'une signature numérique sont les suivants : 1) le tiers authenticateur a-t-il correctement identifié le détenteur ? 2) le tiers authenticateur a-t-il correctement authentifié la clef publique du détenteur ? 3) la clef publique du détenteur a-t-elle été compromise ? et 4) la procédure est-elle fiable (à savoir, l'algorithme de la clef publique et la longueur de cette clef sont-ils appropriés) ?

40. Le paragraphe 1 énonce deux critères fondamentaux pour déterminer si une signature numérique peut être considérée comme une signature électronique sûre. Selon le premier, il faut que la signature soit créée pendant la période d'effet d'un certificat valide et soit vérifiée par référence à la clef publique donnée dans le certificat. La période d'effet d'un certificat commence normalement au moment de son émission et se termine à son expiration, son annulation ou sa suspension.

41. Selon le second, il faut garantir que le certificat lui-même identifie exactement une personne comme le détenteur de la clef privée correspondant à la clef publique donnée dans le certificat. La fiabilité du certificat peut être évaluée par référence à des normes, des procédures et d'autres conditions stipulées par des autorités reconnues dans l'État adoptant. Ces normes peuvent être établies par accréditation d'organismes de certification par des tierces parties, ou par l'agrément volontaire des tiers authenticateurs, ou exiger l'application des règles établies par l'État adoptant.

42. Une autre possibilité est énoncée au paragraphe 2, à savoir que si un tribunal ou un juge des faits détermine que selon toute évidence, l'information donnée dans le certificat est effectivement exacte, la fiabilité du certificat est manifeste. À ce stade, toutefois, le juge des faits doit déterminer au cas par cas si le certificat a été émis par un tiers authenticateur ayant identifié correctement le détenteur et authentifié la clef publique de ce dernier.

43. Le projet d'article 5, conformément à la "double approche" adoptée par le Groupe de travail, vise à laisser autant de latitude que possible pour ce qui est de déterminer la fiabilité d'un certificat émis par un tiers authenticateur. Cette souplesse est particulièrement importante du fait que le recours aux signatures numériques est récent et que les modèles et la réglementation, dans ce domaine, ne sont pas encore bien établis. Il importe donc de favoriser le développement des signatures numériques dans le commerce électronique tout en arrêtant les normes nécessaires pour déterminer par présomption la fiabilité d'un message portant une signature numérique.

44. Il faut aussi noter que, si la première option énoncée dans le projet d'article 5 comprend une détermination judiciaire de l'exactitude d'un certificat, la seconde, par contre, présume cette exactitude si le certificat a été émis par un tiers authentificateur accrédité par l'État adoptant ou s'il satisfait d'une autre manière à certaines normes établies par ledit État. Une détermination judiciaire de l'exactitude n'est alors pas requise pour considérer la signature électronique comme sûre. La seconde option peut être utile pour les personnes pratiquant le commerce électronique qui sauraient, avant d'agir sur la foi d'une communication, si cet acte peut être exécuté. Il est toutefois possible de réfuter la présomption d'exactitude en démontrant qu'un certificat émis par un tiers authentificateur accrédité n'est en fait ni exact ni fiable.

[Article 6. Signature par des personnes morales

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

Références

A/CN.9/437, paragraphes 114 à 117 (projet d'article D);
A/CN.9/WG.IV/WP.71, paragraphes 61 à 63.

Observations

45. À la précédente session, il avait été largement estimé que le projet d'article 6 devrait être supprimé. Toutefois, après un débat, le Groupe de travail avait décidé qu'il devait être mis entre crochets, afin d'être examiné à une session ultérieure (A/CN.9/437, par. 115 à 117). On peut certes juger qu'une disposition telle que le projet d'article 6 empiète de façon injustifiée sur d'autres domaines du droit (par exemple le droit de la représentation et les dispositions du droit des sociétés traitant de la représentation par des personnes physiques), mais elle peut aussi être utile au stade actuel de l'élaboration des Règles uniformes pour rappeler que le Groupe de travail pourrait avoir à débattre de façon plus approfondie de la mesure dans laquelle les Règles uniformes devraient valider les activités des "agents électroniques" pour l'authentification automatique des messages de données.

Section III. Autres signatures électroniques

46. Aucune information n'ayant été communiquée au Secrétariat sur la façon de traiter les techniques d'authentification autres que les signatures numériques dans le cadre des Règles uniformes, aucune disposition particulière n'a été élaborée aux fins d'insertion dans la section III. Le Groupe de travail pourrait souhaiter examiner la question de savoir si de telles techniques d'authentification devraient être traitées plus en détail dans les Règles uniformes. S'il parvient à la conclusion qu'elles ne devraient pas l'être, les Règles uniformes n'en favoriseraient pas moins le développement, grâce au principe de non-discrimination énoncé dans les définitions des termes "signature" et "signatures électroniques sûres", et grâce au statut juridique reconnu à toute technique d'authentification pouvant être considérée comme une "signature électronique sûre".

CHAPITRE III. TIERS AUTHENTIFICATEURS ET QUESTIONS CONNEXES

Article 7. Tiers authentificateur

1. Aux fins des présentes Règles, les termes "tiers authentificateur" désignent :

a) Toute personne ou entité agréée [accréditée] par ... [*l'État adoptant indique l'organe ou l'autorité compétents habilités à agréer les tiers authentificateurs et à promulguer des règles concernant les fonctions des tiers authentificateurs agréés*] pour agir en application des présentes Règles;

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

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

Références

A/CN.9/437, paragraphes 39 à 50 et 90 à 97 (projet d'article B)

A/CN.9/WG.IV/WP.71, paragraphes 18 à 45, 57 et 58.

Observations

47. Comme il a été indiqué dans le contexte du projet d'article premier, les Règles uniformes devraient prévoir la reconnaissance juridique à la fois dans le cas où un État adoptant souhaite réglementer les activités des tiers authentificateurs par une infrastructure à clef publique ou d'autres systèmes d'agrément, et dans le cas où des tiers authentificateurs non agréés peuvent exercer leur activité librement en se conformant à des normes issues du marché (voir ci-dessus par. 17 et 18).

48. Le paragraphe 1 ne tente pas, en ce qui concerne les tiers authentificateurs agréés, de définir les critères à appliquer par les États adoptants dans la mise en œuvre d'une infrastructure à clef publique ou d'un autre système d'agrément. Une des raisons est peut-être la place importante faite à l'ordre public dans ces infrastructures, qui ne se prêtent peut-être pas facilement à une harmonisation internationale par voie de dispositions législatives types. Si le Groupe de travail examine plus en détail les critères à appliquer dans le cadre d'un système d'agrément, il souhaitera peut-être réfléchir aux facteurs indiqués ci-après dont il convient de tenir compte lorsque l'on évalue la fiabilité d'un tiers authentificateur : 1) indépendance (c'est-à-dire absence d'intérêts financiers ou autres dans les transactions en jeu); 2) ressources et capacité financières d'assumer le risque de voir sa responsabilité mise en jeu en cas de préjudice; 3) compétence du personnel de direction, maîtrise de la technologie des clefs publiques et familiarité avec les procédures de sécurité requises; 4) durée (les tiers authentificateurs peuvent en effet être amenés à donner des preuves d'authentification ou à décrypter des clefs plusieurs années après la fin de la transaction, par exemple 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 comptable par une entité indépendante; 7) existence d'un dispositif d'urgence (par exemple logiciel de "récupération catastrophe" ou mécanisme de "blocage" de la clef); 8) sélection et gestion du personnel; 9) dispositifs de protection pour la clef privée du tiers authentificateur; 10) sécurité interne; 11) arrangements pour la cessation des opérations, y compris avis aux utilisateurs; 12) garanties (données 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 clefs cryptographiques

viendraient à être perdues ou compromises); 17) isolement de la fonction d'authentification des autres activités éventuelles du tiers authentificateur (voir A/CN.9/WG.IV/WP.71, par. 44 et A/CN.9/437, par. 45).

49. L'alinéa b) du paragraphe 1 définit le "tiers authentificateur", sans faire mention de l'autorisation de l'État, par référence à sa fonction d'émetteur de certificats. Une telle disposition, associée au paragraphe 2, a aussi pour objectif de tenir compte du fait que le tiers authentificateur peut avoir d'autres utilités et offrir des services autres que l'émission de certificats, mais que ces activités et services n'entrent pas dans le champ d'application des Règles uniformes et ne doivent pas être pris en considération lorsque l'on traite les effets juridiques des signatures électroniques. Le Groupe de travail souhaitera peut-être étudier si une disposition telle que le paragraphe 2, qui est essentiellement descriptif, devrait faire partie des Règles uniformes ou si elle devrait plutôt être insérée dans un guide ou un commentaire.

Article 8. Certificat

Aux fins des présentes Règles, le terme "certificat" désigne un message de données [ou un autre document] qui, au minimum :

- a) identifie le tiers authentificateur qui l'émet;
- b) nomme ou identifie son détenteur ou un dispositif ou un agent électronique sous le contrôle du détenteur;
- c) contient une clef publique correspondant à une clef privée dont le détenteur a le contrôle;
- d) spécifie sa période d'effet [et, le cas échéant, les restrictions à l'utilisation de la clef publique]; et
- e) est signé [numériquement] par le tiers authentificateur qui l'émet.

Références

A/CN.9/437, paragraphes 98 à 113 (projet d'article C);
A/CN.9/WG.IV/WP.71, paragraphes 18 à 45, 59 et 60.

Observations

50. Un certificat peut avoir diverses fonctions et communiquer des informations n'entrant pas dans le champ d'application des Règles uniformes. Cependant, la seule fonction traitée dans les Règles uniformes est le rattachement d'une clef publique à un détenteur donné. Ce rattachement peut être effectué directement, par la désignation du détenteur de la clef publique dans le certificat. Il peut l'être aussi indirectement par l'indication de certains éléments caractérisant le détenteur (par exemple, responsable des achats habilité à contracter à concurrence d'un certain montant), ou par l'indication d'une machine, d'un dispositif ou d'un logiciel sous le contrôle du détenteur. Par exemple, une société peut délivrer à un employé chargé des achats un certificat précisant uniquement les limites des pouvoirs de cet employé. Ce certificat peut ensuite être utilisé dans des transactions avec des partenaires commerciaux où l'identité de l'employé importe peu, la principale question étant de savoir s'il est habilité à agir au nom d'une personne désignée (par exemple, l'employeur) et quelle est la limite de l'autorité qui lui a été conférée. Dans tous les cas, cependant, il existe une personne, dénommée "détenteur", qui a le contrôle de la clef privée correspondant à la clef publique donnée dans le certificat et à laquelle doivent être attribués les messages portant une signature numérique et vérifiés par référence au

certificat. Si une telle personne n'est pas désignée, le certificat ne peut pas servir à vérifier qu'une signature numérique est bien celle de la personne spécifiée.

51. Le projet d'article 8 vise à tenir compte des éléments considérés par le Groupe de travail comme les caractéristiques essentielles d'un certificat, à savoir le fait : d'être un message de données; de désigner le tiers authentificateur; de contenir la clef publique du détenteur; de désigner le détenteur; et de comporter la signature numérique du tiers authentificateur (voir A/CN.9/437, par. 101). Pour ce qui est de savoir si un certificat doit nécessairement prendre la forme d'un message de données, le Groupe de travail pourrait souhaiter étudier si les Règles uniformes devraient également couvrir les certificats sur papier.

52. À la précédente session, le Groupe de travail a décidé qu'il pourrait être amené à examiner si l'établissement d'une règle obligatoire concernant les informations minima à fournir dans un certificat pourrait aller à l'encontre de la loi applicable sur la protection des données. La nature des éléments énumérés au projet d'article 8 permet, semble-t-il, d'éviter un tel conflit éventuel.

53. La définition du terme "certificat" n'établit pas de distinction entre les différents niveaux de sécurité pouvant être assurés commercialement dans ce type de document. Toutefois, lors de l'élaboration des Règles uniformes, le Groupe de travail pourrait garder à l'esprit le fait que les tiers authentificateurs offrent généralement diverses catégories de certificats. À la précédente session, plusieurs propositions ont été faites afin de tenir compte dans les Règles uniformes des divers niveaux de sécurité pouvant découler de l'utilisation de ces certificats (voir A/CN.9/437, par. 20, 56, 138 et 145). Pour illustrer cette diversité, les trois classes de "certificats" énumérées ci-après seraient disponibles sur le marché.

54. Les certificats de la catégorie I confirment que le nom et l'adresse électronique d'un utilisateur forment, dans le registre ou la banque de données tenus par un tiers authentificateur, une entrée ne comportant aucune ambiguïté. Normalement, ils sont utilisés essentiellement pour parcourir l'Internet et pour le courrier électronique personnel et ont pour objectif d'améliorer modestement la sécurité de ces environnements. Ils n'ont pas pour but d'authentifier l'identité du détenteur, mais plutôt de vérifier simplement l'absence d'ambiguïté de l'entrée figurant dans la banque de données et d'effectuer une vérification limitée de l'adresse électronique. Le nom du détenteur indiqué dans un certificat de catégorie I est considéré comme une information non vérifiée. Ces certificats offrent un niveau de sécurité très faible. Ils ne sont pas destinés à un usage commercial où la preuve de l'identité est nécessaire et il ne faut pas y recourir pour de telles utilisations.

55. Les certificats de la catégorie II confirment que l'information fournie par le détenteur lors de la demande de certificat concorde avec l'information accessible dans des bases de données pour consommateurs largement reconnues. Ils sont généralement utilisés aux fins suivantes : 1) courrier électronique interorganisations; 2) transactions à faible valeur et faible risque; 3) courrier électronique personnel; 4) remplacement de mots de passe; 5) validation de logiciels; et 6) services d'abonnement en ligne. Ils offrent un certain niveau de sécurité quant à l'identité du détenteur, grâce à un processus automatique en ligne.

56. Les certificats de catégorie III offrent des garanties importantes quant à l'identité du détenteur. Il est exigé, par exemple, que ce dernier se présente personnellement (physiquement) à l'agent du tiers authentificateur ou que son identité soit vérifiée par des documents d'identité appropriés. La clef privée correspondant à la clef publique contenue dans un certificat de catégorie III doit être créée et conservée de manière fiable en respectant les conditions établies par le tiers authentificateur. Les certificats de catégorie III sont utilisés dans la pratique pour certaines applications du commerce électronique telles que les services bancaires électroniques, l'échange de données informatisées et les services en ligne réservés à leurs membres. Diverses procédures sont appliquées pour obtenir une preuve de l'identité de chaque abonné. Ces procédures

de validation offrent de plus grandes garanties que les certificats de la catégorie II quant à l'identité d'un demandeur.

57. Les exemples précédents montrent clairement que seuls les certificats de la catégorie III entreraient dans le champ d'application actuel des Règles uniformes. Le Groupe de travail souhaitera peut-être examiner la question de savoir si le champ des Règles uniformes devrait être étendu à des catégories de certificats inférieures, auquel cas une décision devrait être prise concernant les divers effets juridiques des différentes catégories de certificats, en particulier pour ce qui est du niveau de fiabilité à imposer aux tiers authenticateurs pour l'émission de certificats de catégorie inférieure. Il pourrait être, sinon, nécessaire de modifier la définition du terme "certificat" dans les Règles uniformes de façon à indiquer clairement que les certificats de catégorie inférieure n'entrent pas dans leur champ d'application.

Article 9. Déclaration relative aux pratiques d'authentification

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

Références

A/CN.9/437, paragraphes 60 à 62, 70, 110, 111 et 149 (projet d'article J);
A/CN.9/WG.IV/WP.71, paragraphe 89.

Observations

58. La mesure dans laquelle toute partie se fondant sur un certificat peut se fier au lien entre une personne et une clef publique, telle qu'attesté par un certificat, dépend de plusieurs facteurs, à savoir notamment : les pratiques et procédures suivies par le tiers authenticateur pour authentifier le détenteur de la paire de clefs, ses méthodes de travail, ses procédures et ses contrôles de sécurité. Les tiers authenticateurs présentent souvent les déclarations relatives à leurs pratiques d'authentification comme l'un des principaux éléments leur permettant de promouvoir la confiance dans la fiabilité des certificats qu'ils émettent et, plus généralement, comme la norme de qualité et de fiabilité qui devrait régir la relation entre eux et leurs clients.

59. Une déclaration relative aux pratiques d'authentification est une déclaration du tiers authenticateur dans laquelle ce dernier expose la politique qu'il suit ou donne des détails sur les pratiques, procédures et systèmes qu'il applique dans son activité, venant à l'appui de l'émission, de la gestion et de l'annulation d'un certificat. Les sujets traités dans cette déclaration peuvent être les suivants : 1) procédures employées pour authentifier l'identité d'une personne requérant un certificat (avant l'émission du certificat); 2) contrôle matériel et contrôle des procédures et du personnel effectués par le tiers authenticateur pour créer des clefs, émettre et annuler des certificats, effectuer des vérifications et archiver en toute sécurité ; 3) mesures de sécurité prises par le tiers authenticateur pour protéger ses clefs cryptographiques; et 4) toute information connexe. Ces questions sont importantes à la fois pour le détenteur qui reçoit le certificat et pour les parties qui s'y fieront pour effectuer des transactions avec ce dernier.

60. La déclaration relative aux pratiques d'authentification peut prendre diverses formes, comme un contrat entre toutes les parties intéressées, ou un avis public à toutes les parties intéressées. Le principal élément, toutefois, est la notification aux parties qui se fonderont sur le certificat. La déclaration devrait constituer une notification du tiers authenticateur à toutes les parties (y compris les détenteurs) indiquant les pratiques qu'il suit pour émettre, gérer et annuler des certificats.

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

Variante A

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

- a) qu'il s'est conformé à toutes les conditions applicables prévues dans les présentes Règles pour l'émission du certificat et, s'il a publié le certificat ou l'a mis de toute autre manière à la disposition de cette personne, que le détenteur désigné dans le certificat [et possédant légitimement la clef privée correspondante] l'a accepté;
- b) que le détenteur désigné dans le certificat détient [légitimement] la clef privée correspondant à la clef publique indiquée dans le certificat;
- c) que la clef publique et la clef privée du détenteur sont appariées;
- d) que toutes les informations données dans le certificat sont exactes à la date de son émission, sauf si le tiers authentificateur a déclaré dans le certificat [ou fait savoir par incorporation par référence dans le certificat] que l'exactitude de certaines informations n'est pas confirmée; et
- e) qu'à la connaissance du tiers authentificateur, n'a été omis du certificat aucun fait matériel connu qui, s'il était connu, compromettrait la fiabilité des garanties ci-dessus.

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

Variante B

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

- a) qu'il a [traité] [approuvé] [émis] le certificat et le gérera et l'annulera, le cas échéant, conformément :
 - i) aux présentes Règles;
 - ii) à toute autre loi applicable régissant l'émission du certificat; et
 - iii) à toute déclaration applicable relative aux pratiques d'authentification figurant ou incorporée par référence dans le certificat, ou dont la personne a été avisée, le cas échéant;
- b) qu'il a vérifié l'identité du détenteur dans la mesure indiquée dans le certificat ou dans toute déclaration applicable relative aux pratiques d'authentification ou, en l'absence d'une telle déclaration, qu'il a vérifié l'identité du détenteur de manière fiable;

- c) qu'il a vérifié que la personne demandant le certificat détient la clef privée correspondant à la clef publique indiquée dans le certificat;
- d) qu'à sa connaissance, sous réserve de ce qui est stipulé dans le certificat ou toute déclaration applicable relative aux pratiques d'authentification, toutes les autres informations figurant dans le certificat sont exactes à la date d'émission dudit certificat;
- e) que, s'il a publié le certificat, le détenteur qui y est désigné l'a accepté.

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

Références

A/CN.9/437, paragraphes 51 à 73 (projet d'article H);
A/CN.9/WG.IV/WP.71, paragraphes 70 à 72.

Observations

61. Le projet d'article 10 vise à tenir compte de la décision du Groupe de travail selon laquelle le projet de Règles uniformes devrait, en principe, comporter des dispositions régissant la responsabilité des tiers authentificateurs, pour autant que ceux-ci interviennent dans des systèmes de signature numérique (A/CN.9/437, par. 55). La norme minimale en matière de responsabilité énoncée au projet d'article 10 ne doit s'appliquer qu'à l'émission de certificats à des fins de signature numérique, au sens du projet d'article 4. Le projet de Règles uniformes ne tente pas de traiter des autres activités ou services éventuels des tiers authentificateurs, qui peuvent être régis par des arrangements contractuels entre ces derniers et leurs clients, ou par toute autre loi applicable (ibid., par. 71).

62. À sa trente et unième session, le Groupe de travail a généralement convenu qu'un libellé allant dans le sens du paragraphe 1 de la variante A était, dans une large mesure, acceptable quant au fond en tant que point de départ de futures discussions. Bien qu'il n'établisse pas expressément de règle en matière de responsabilité, ce paragraphe énonce une norme minimale à laquelle les parties ne devraient pas être autorisées à déroger par convention privée. En particulier, aucune clause limitant la responsabilité du tiers authentificateur ne devrait être considérée comme relevant de la protection ou des avantages prévus au titre des Règles uniformes si elle est incompatible avec les conditions susmentionnées. En cas d'allégation de la responsabilité d'un tiers authentificateur, ce dernier est présumé responsable des conséquences de l'émission d'un certificat, sauf s'il peut prouver qu'il a satisfait aux conditions énumérées au paragraphe 1. Toutefois, s'il souhaite s'imposer des obligations plus strictes que les garanties énoncées au paragraphe 1, il devrait être autorisé à le faire, soit en insérant des clauses à cet effet dans sa déclaration relative aux pratiques d'authentification, soit de toute autre manière (A/CN.9/437, par. 70). Le paragraphe 2 traite les cas où les déclarations relatives aux pratiques d'authentification contiennent des normes plus strictes.

63. La variante B s'inspire de la variante A, mais insiste davantage sur l'autorégulation des tiers authentificateurs. À l'alinéa b), en particulier, le tiers authentificateur ne garantit pas que le détenteur détient légitimement la clef privée. Il garantit par contre qu'aux fins de l'établissement du lien entre le détenteur et la clef privée, il a appliqué tout au moins les procédures énoncées dans la déclaration relative à ses pratiques d'authentification ou utilisé des méthodes "fiabiles" pour identifier le détenteur. Le paragraphe 2 de la variante B énonce clairement que le sous-alinéa a) ii) du paragraphe 1 s'applique également lorsque le certificat

émis est régi par les lois d'une autre juridiction. Le Groupe de travail souhaitera peut-être prendre une décision quant à l'insertion d'une telle précision soit dans les Règles uniformes, soit dans un guide ou un commentaire.

Article 11. Responsabilité contractuelle

1. Entre un tiers authentificateur émettant un certificat et le détenteur de ce certificat [ou toute autre partie ayant une relation contractuelle avec le tiers authentificateur], les droits et obligations des parties sont déterminés par convention.
2. Sous réserve de l'article 10, un tiers authentificateur peut, par convention, s'exonérer de sa responsabilité en cas de préjudice dû à des erreurs dans les informations contenues dans le certificat, à des défaillances techniques ou à d'autres circonstances de même nature. Toutefois, la clause limitant ou excluant la responsabilité du tiers authentificateur ne peut être invoquée dans le cas où l'exclusion ou la limitation de la responsabilité contractuelle serait manifestement inéquitable eu égard à l'objet du contrat.
3. Le tiers authentificateur n'est pas autorisé à limiter sa responsabilité s'il est prouvé que le préjudice a résulté de l'acte ou de l'omission dudit tiers agissant avec l'intention de causer un préjudice ou téméairement et en sachant qu'un préjudice pourrait en résulter.

Références

A/CN.9/437, paragraphes 51 à 73 (projet d'article H);
A/CN.9/WG.IV/WP.71, paragraphes 70 à 72.

Observations

64. Le paragraphe 1 énonce à nouveau le principe de l'autonomie des parties concernant le régime de responsabilité applicable au tiers authentificateur. Le paragraphe 2 porte sur la question des clauses d'exonération, qui sont généralement déclarées admissibles, à deux exceptions près. La première découle d'une référence au projet d'article 10, qui vise à établir un norme minimale à laquelle les tiers authentificateurs ne doivent pas être autorisés à déroger (voir par. 58 ci-dessus). La seconde, qui est inspirée des Principes d'UNIDROIT relatifs aux contrats de commerce international (art. 7.1.6), tente d'établir une norme uniforme pour l'évaluation de l'acceptabilité générale des clauses d'exonération. On notera que le fait d'indiquer que la limitation ou l'exclusion de la responsabilité peut être "manifestement inéquitable" dénote une approche souple en la matière. Cette approche pourrait aboutir à une reconnaissance des clauses limitatives et exclusives plus large que cela ne serait le cas si les Règles uniformes mentionnaient uniquement la loi applicable en dehors d'elles.

65. Le paragraphe 3 traite des cas où une faute du tiers authentificateur ou de ses agents entraînerait une perte ou un autre préjudice. Pour ce qui est du fond, la règle proposée s'inspire d'un libellé analogue employé dans de nombreuses conventions internationales sur les transports et utilisé récemment dans l'article 18 de la Loi type de la CNUDCI sur les virements internationaux.

Article 12. Responsabilité du tiers authentificateur envers les parties se fiant aux certificats

1. Sauf convention contraire, un tiers authentificateur qui émet un certificat est responsable envers toute personne se fiant raisonnablement à ce certificat dans les cas suivants :

- a) [rupture de la garantie au titre de l'article 10] [négligence par fausse présentation de l'exactitude des renseignements donnés dans le certificat];
- b) enregistrement de l'annulation d'un certificat promptement après réception de la notification de l'annulation dudit certificat; et
- c) [conséquences de la non] [négligence dans l'] application :
 - i) de toute procédure énoncée dans la déclaration relative aux pratiques d'authentification publiée par le tiers authentificateur; ou
 - ii) de toute procédure énoncée dans la loi applicable.

2. Nonobstant le paragraphe 1, un tiers authentificateur n'est pas responsable s'il peut démontrer que lui-même ou ses agents ont pris toutes les mesures nécessaires pour éviter des erreurs dans le certificat ou qu'il était impossible, à lui-même ou à ses agents, de prendre de telles mesures.

3. Nonobstant le paragraphe 1, un tiers authentificateur peut limiter, dans le certificat [ou de toute autre manière], l'objet dudit certificat. Le tiers authentificateur n'est pas tenu responsable du préjudice découlant de l'utilisation du certificat pour tout autre objet.

4. Nonobstant le paragraphe 1, un tiers authentificateur peut limiter, dans le certificat [ou de toute autre manière], la valeur des opérations pour lesquelles le certificat est valide. Il n'est pas tenu responsable du préjudice dépassant cette limite.

Références

A/CN.9/437, paragraphes 51 à 73 (projet d'article H);
A/CN.9/WG.IV/WP.71, paragraphes 70 à 72.

Observations

66. Le projet d'article 12 tient compte de l'opinion exprimée à la précédente session, selon laquelle les Règles uniformes devraient contenir une disposition énonçant une présomption simple de responsabilité. En vertu de cette disposition, par exemple, en cas d'identification erronée d'une personne ou d'attribution par erreur d'une clef publique à une personne, le tiers authentificateur serait tenu responsable du préjudice subi par toute partie lésée, à moins qu'il ne puisse démontrer qu'il s'était efforcé de son mieux d'éviter l'erreur. Un tel régime de responsabilité vise à conférer un surcroît de protection à tout utilisateur des services d'un tiers authentificateur, sans pour autant imposer une responsabilité objective audit tiers (voir A/CN.9/437, par. 58).

67. Dans le cadre du débat sur les projets d'articles 10 à 12, le Groupe de travail pourrait souhaiter examiner la question de savoir si la responsabilité du tiers authentificateur devrait être assortie de limites et comment ces limites pourraient être fixées (voir A/CN.9/437, par. 63 à 67). À sa précédente session, le Groupe de travail avait examiné plusieurs propositions concernant les moyens de limiter la responsabilité incombant au tiers authentificateur. Il serait possible par exemple de déterminer un montant fixe. Selon d'autres approches, la limitation de la responsabilité pourrait se fonder sur un multiple du droit payé par le détenteur, sur un pourcentage de la valeur de la transaction ou sur un pourcentage du préjudice effectivement subi par la partie lésée. On a toutefois fait remarquer que le préjudice qui pouvait résulter des actes d'un tiers authentificateur n'était pas suffisamment facile à quantifier pour pouvoir servir de critère objectif permettant d'assigner un

montant fixe. Par ailleurs, le service offert par un tiers authentificateur et les droits qu'il prélevait n'avaient souvent aucun rapport avec la valeur des transactions auxquelles ils se rapportaient ni avec le préjudice que pouvaient subir les parties (ibid., par. 65). Pour ce qui est de la comparaison proposée entre la situation d'un tiers authentificateur et celle d'un transporteur en vertu des conventions internationales applicables au transport de marchandises et au transport de passagers (ibid., par. 67), un examen préliminaire de ces textes tend à montrer que les limites de la responsabilité sont généralement établies par référence à un montant fixe (par exemple dans le cas du transport de passagers), éventuellement en association avec une référence à la valeur des biens transportés. Il pourrait être nécessaire que le Groupe de travail examine cette question à une session future après une étude plus approfondie par le Secrétariat.

Article 13. Annulation d'un certificat

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

- a) réception d'une demande d'annulation par le détenteur désigné dans le certificat, et confirmation que la personne demandant l'annulation en est le détenteur légitime, ou est un agent du détenteur habilité à demander l'annulation;
- b) réception d'une preuve fiable du décès du détenteur si ce dernier est une personne physique; ou
- c) réception d'une preuve fiable que le détenteur a été dissous ou a cessé d'exister, lorsqu'il s'agit d'une personne morale.

2. Le détenteur d'une paire de clefs certifiée est tenu d'annuler le certificat correspondant lorsqu'il apprend que la clef privée a été perdue, compromise ou risque d'être utilisée à mauvais escient à d'autres égards. Si le détenteur n'annule pas le certificat dans un tel cas, il est responsable de tout préjudice encouru par des tiers s'étant fié au contenu des messages du fait que le détenteur a failli à son obligation d'annuler le certificat.

3. Que si le détenteur indiqué dans le certificat consente ou non à l'annulation, le tiers authentificateur qui a émis le certificat doit l'annuler rapidement après avoir appris :

- a) qu'un fait matériel présenté dans le certificat est faux;
- b) que la clef privée ou le système informatique du tiers authentificateur a été compromis d'une manière qui compromet la fiabilité du certificat; ou
- c) que la clef privée ou le système informatique du détenteur a été compromis.

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

4. [Entre le détenteur et le tiers authentificateur,] l'annulation prend effet à partir du moment où elle est [reçue] [enregistrée] par le tiers authentificateur.

[5. Entre le tiers authentificateur et toute autre partie se fiant au certificat, l'annulation prend effet à partir du moment où elle est [enregistrée] [publiée] par le tiers authentificateur.]

Références

A/CN.9/437, paragraphes 125 à 139 (projet d'article F);

A/CN.9/WG.IV/WP.71, paragraphes 66 et 67.

Observations

68. Le projet d'article 13 tient compte des différentes vues exprimées à la précédente session du Groupe de travail en énonçant une norme par défaut régissant l'annulation des certificats. Toutefois, un tiers authentificateur peut à tout moment contourner la norme par défaut en établissant dans la déclaration relative à ses pratiques d'authentification des procédures qui régissent l'annulation et en les appliquant. En ce qui concerne le moment auquel l'annulation prend effet, le Groupe de travail pourrait souhaiter prendre une décision quant à la nécessité d'établir une distinction entre la situation du détenteur et celle de toute autre partie se fondant sur le certificat (voir A/CN.9/437, par. 130).

Article 14. Suspension d'un certificat

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

Références

A/CN.9/437, paragraphes 133 à 135 (projet d'article F).

Observations

69. À sa précédente session, le Groupe de travail a décidé que les Règles uniformes devaient contenir une disposition sur la suspension des certificats (voir A/CN.9/437, par. 113 et 134). En ce qui concerne le moment où une suspension prend effet, il pourra souhaiter décider s'il est nécessaire d'ajouter des dispositions s'inspirant des paragraphes 4 et 5 du projet d'article 13.

Article 15. Registre des certificats

1. Le tiers authentificateur tient un registre électronique des certificats émis accessible au public et indiquant la date d'expiration de chaque certificat, ou la date de suspension ou d'annulation.

2. Le registre est tenu par le tiers authentificateur

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

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

à compter de la date d'annulation ou d'expiration de la période d'effet de tout certificat émis par le tiers authentificateur.

Variante C conformément aux politiques et procédures spécifiées par le tiers authentificateur dans la déclaration applicable relative aux pratiques d'authentification.

Référence

A/CN.9/437, paragraphes 140 à 148 (projet d'article G);
A/CN.9/WG.IV/WP.71, paragraphes 68 et 69.

Observations

70. À la précédente session, aucune objection de principe n'a été soulevée contre l'inclusion dans les Règles uniformes d'une disposition concernant l'inscription des certificats dans un registre (voir A/CN.9/437, par. 142). La bonne tenue d'un registre largement accessible (parfois appelé banque de données) comprenant en particulier une liste des annulations de certificats peut être considérée comme un élément important de la fiabilité des signatures numériques. En ce qui concerne la façon dont les tiers authentificateurs devraient tenir ces registres et ces listes, le Groupe de travail pourrait souhaiter examiner la question de savoir si les parties devraient être tenues de vérifier la situation du certificat en consultant le registre ou la liste pertinente avant de se fonder sur sa validité.

71. Plus généralement, le Groupe de travail souhaitera peut-être étudier si les Règles uniformes, en établissant des règles minima concernant les activités des tiers authentificateurs, devraient traiter également les droits et obligations des parties se fiant aux certificats.

Article 16. Relations entre les parties se fiant aux certificats et le tiers authentificateur

[1. Un tiers authentificateur n'est autorisé à demander que les renseignements qui lui sont nécessaires pour identifier l'utilisateur.

2. Sur demande, le tiers authentificateur divulgue les renseignements suivants :

- a) les conditions dans lesquelles le certificat peut être utilisé;
- b) les conditions déterminant l'utilisation des signatures numériques;
- c) le coût des services fournis par le tiers authentificateur;
- d) la politique ou les pratiques du tiers authentificateur concernant l'utilisation, la conservation et la communication de renseignements d'ordre personnel;
- e) les prescriptions techniques du tiers authentificateur concernant le matériel de communication devant être utilisé par les parties se fiant aux certificats;

- f) les conditions dans lesquelles le tiers authentificateur met en garde les parties se fiant aux certificats en cas d'irrégularité ou de défaut de fonctionnement du matériel de communication;
- g) toute limite de la responsabilité du tiers authentificateur;
- h) toutes restrictions imposées par le tiers authentificateur à l'utilisation du certificat;
- i) les conditions dans lesquelles le détenteur est autorisé à restreindre l'utilisation du certificat.

3. Les renseignements énumérés au paragraphe 1 sont 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 relative aux pratiques d'authentification.

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

5. Avec un préavis [de trois mois], le tiers authentificateur peut mettre fin à l'accord établissant une connexion avec le tiers authentificateur. L'avis prend effet dès qu'il est reçu.]

Références

A/CN.9/437, paragraphes 149 et 150 (projet d'article J);
A/CN.9/WG.IV/WP.71, paragraphe 76.

Observations

72. À sa session précédente, le Groupe de travail a noté que les divers éléments énumérés dans le projet d'article 15 devraient être placés entre crochets, pour être examinés à un stade ultérieur (voir A/CN.9/437, par. 150).

CHAPITRE IV. RECONNAISSANCE DES SIGNATURES ÉLECTRONIQUES ÉTRANGÈRES

Article 17. Tiers authentificateurs étrangers offrant des services en vertu des présentes Règles

Variante A

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

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

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

Variante B Le ... [*l'État adoptant indique l'organe ou le tiers authentificateur habilité à établir des règles concernant l'approbation des certificats étrangers*] est autorisé à approuver les certificats étrangers et à établir des règles spécifiques régissant cette approbation.

Références

A/CN.9/437, paragraphes 74 à 89 (projet d'article I);
A/CN.9/WG.IV/WP.71, paragraphes 73 à 75.

Observations

73. En permettant à des entités étrangères de s'établir comme tiers authentificateurs, le projet d'article 17 énonce simplement le principe selon lequel les entités étrangères ne doivent pas faire l'objet d'une discrimination, à condition qu'elles satisfassent aux normes applicables aux tiers authentificateurs locaux. Même si ce principe est généralement accepté, il peut être particulièrement utile de l'énoncer en ce qui concerne les tiers authentificateurs, dans la mesure où ces derniers peuvent mener leur activité sans avoir nécessairement une implantation matérielle ou un autre type d'établissement dans le pays où ils mènent cette activité.

Article 18. Approbation des certificats étrangers par les tiers authentificateurs nationaux

Les certificats émis par les tiers authentificateurs d'un autre pays peuvent être utilisés pour des signatures numériques selon les mêmes modalités que les certificats soumis aux présentes Règles s'ils sont reconnus par un tiers authentificateur se conformant à ... [*la loi de l'État adoptant*], et si celui-ci garantit, à l'instar de ce qu'il fait pour ses propres certificats, que les détails figurant dans le certificat sont exacts et, en outre, que le certificat est valide et en vigueur.

Références

A/CN.9/437, paragraphes 74 à 89 (projet d'article I);
A/CN.9/WG.IV/WP.71, paragraphes 73 à 75.

Observations

74. Le projet d'article 18 permet à un tiers authentificateur national de garantir, de la même façon que pour ses propres certificats, que les détails du certificat étranger sont exacts et qu'il est valide et en vigueur. Il fait référence aux questions examinées à la précédente session du Groupe de travail sous le titre "certification transférée". Le projet d'article 18 contient essentiellement une disposition sur l'attribution de la responsabilité au tiers authentificateur national lorsque le certificat étranger comporte un défaut (voir A/CN.9/437, par. 77 et 78).

Article 19. Reconnaissance des certificats étrangers

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

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

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

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

Références

A/CN.9/437, paragraphes 74 à 89 (projet d'article I);

A/CN.9/WG.IV/WP.71, paragraphes 73 à 75.

Observations

75. Le projet d'article 19 porte sur les questions qui, à la précédente session du Groupe de travail, ont été examinées sous le titre "certification transfrontière" (voir A/CN.9/437, par. 77 et 78). Les paragraphes 1 et 2 portent sur les façons d'établir la fiabilité des certificats et des signatures étrangers avant qu'une transaction ne soit effectuée (et avant qu'un litige n'ait surgi quant au niveau de fiabilité d'une signature). Le paragraphe 3 établit la norme par rapport à laquelle évaluer les signatures et certificats étrangers en l'absence de toute détermination préalable de leur fiabilité. Le paragraphe 4 préserve le droit des organismes publics de déterminer les procédures à suivre pour communiquer électroniquement avec eux.

Notes

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

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