



## Assemblée générale

Distr.: Générale  
16 avril 2007

Français  
Original: Anglais

---

### Commission des Nations Unies pour le droit commercial international

Quarantième session  
New York, 25 juin-12 juillet 2007

#### **Travaux futurs possibles dans le domaine du commerce électronique**

#### **Document de référence général sur les éléments nécessaires à l'élaboration d'un cadre juridique favorable au commerce électronique: exemple de chapitre sur l'utilisation internationale des méthodes d'authentification et de signature électroniques**

#### **Note du Secrétariat**

##### **Additif**

L'on trouvera en annexe à la présente note une partie d'un exemple de chapitre (deuxième partie, chapitre II, sections A et B) d'un document de référence général consacré aux aspects juridiques de l'utilisation internationale des méthodes d'authentification et de signature électroniques.



## Annexe

### Table des matières

	<i>Paragraphes</i>	<i>Page</i>
Deuxième partie Utilisation transfrontière de méthodes de signature et d'authentification électroniques ( <i>suite</i> ) . . . . .		
II. Méthodes et critères d'établissement de l'équivalence juridique . . . . .	1-22	3
B. Équivalence des normes de conduite et régimes de responsabilité . . . . .	1-22	3
2. Cas particuliers de responsabilité dans le contexte d'une infrastructure à clé publique . . . . .	1-22	3
Conclusion . . . . .	23-28	11

## Deuxième partie

### Utilisation transfrontière de méthodes de signature et d'authentification électroniques (*suite*)

[...]

## II. Méthodes et critères d'établissement de l'équivalence juridique

### B. Équivalence des normes de conduite et régimes de responsabilité

#### 2. Cas particuliers de responsabilité dans le contexte d'une infrastructure à clé publique

1. Le débat touchant la responsabilité liée à l'utilisation de méthodes de signature et d'authentification électroniques a porté surtout sur les fondements et les caractéristiques de la responsabilité des prestataires de services de certification. L'on considère généralement que l'obligation principale d'un prestataire de services de certification est d'utiliser des systèmes, des procédures et des ressources humaines fiables et d'agir conformément aux politiques et aux pratiques qu'il a lui-même annoncées.<sup>1</sup> En outre, le prestataire de services de certification est censé faire preuve d'une diligence raisonnable pour assurer l'exactitude et la complétude de toutes les déclarations essentielles faites par lui dans le contexte d'un certificat. Toutes ces activités peuvent exposer le prestataire de services de certification à divers degrés de responsabilité, selon le droit applicable. L'on trouvera dans les paragraphes ci-après une série d'exemples de cas qui risquent d'exposer un prestataire de services de certification à une responsabilité accrue et un résumé du régime appliqué par les législations nationales à ce type de responsabilité.

##### a) *Absence d'émission ou émission tardive d'un certificat*

2. Habituellement, un prestataire de services de certification délivre un certificat à la demande du signataire intéressé. Si la demande répond aux critères du prestataire de services, celui-ci peut émettre un certificat. Il est néanmoins concevable que la demande réponde aux critères fixés mais soit néanmoins rejetée ou retardée, soit à la suite d'une simple erreur du prestataire de services de certification, soit parce que, délibérément ou par accident, le mécanisme de demande du prestataire de services n'est pas disponible, soit encore parce que, pour des raisons qui lui sont propres, le prestataire de services souhaite retarder ou refuser l'émission d'un certificat au demandeur. En pareilles circonstances, l'auteur d'une demande refusée ou retardée peut parfois se retourner contre le prestataire de services de certification.<sup>2</sup>

---

<sup>1</sup> Loi type de la CNUDCI sur les signatures électroniques (voir note [...]), alinéas a) et b) du paragraphe 1 de l'article 9.

<sup>2</sup> Smedinghoff, "Certification authority: liability issues" (voir note [...]), section 3.2.1.

3. S'il existe un marché sur lequel plusieurs prestataires de services se font concurrence, le refus par tel ou tel prestataire de services d'émettre un certificat, que ce soit par accident ou délibérément, peut ne pas entraîner de réel préjudice pour le demandeur. Cependant, en l'absence d'une réelle concurrence, le refus d'émission ou l'émission tardive d'un certificat par un prestataire de services peut causer un sérieux préjudice si le demandeur se voit dans l'impossibilité, en l'absence de certificat, d'entreprendre l'activité envisagée. Même si d'autres prestataires de services sont disponibles, il peut se produire un dommage spécifique lorsqu'un certificat a été demandé pour une transaction déterminée et que, l'émission du certificat ayant été refusée ou celui-ci n'ayant été émis que tardivement, le demandeur n'a pas pu mener à bien la transaction potentiellement rémunératrice pour lui.<sup>3</sup>

4. Ce type de situation est peu vraisemblable dans un contexte international étant donné que la plupart des signataires ont généralement recours à des prestataires de services de certification établis dans leurs propres pays.

b) *Négligence dans l'émission d'un certificat*

5. Un certificat a censément pour objet de lier l'identité du signataire à une clé publique. Aussi le principal devoir d'un prestataire de services de certification est-il de vérifier, conformément à ses pratiques officielles, que le demandeur est effectivement le signataire et contrôle la clé privée correspondant à la clé publique indiquée sur le certificat, faute de quoi le prestataire de services risque de voir sa responsabilité engagée à l'égard du signataire ou d'une tierce partie qui fait fond sur le certificat.

6. Le signataire peut subir un préjudice, par exemple si un certificat est délivré par erreur à un imposteur utilisant une identité usurpée. Il se peut aussi, par exemple, que les employés ou les sous-traitants de prestataires de services eux-mêmes s'entendent pour délivrer de faux certificats en utilisant la clé de signature du prestataire de services pour certifier des demandes injustifiées de l'imposteur. Il se peut en outre que ces personnes établissent par négligence un certificat erroné, soit en ne suivant pas comme il convient les procédures de validation officielle du prestataire de services pour analyser la demande d'un imposteur, soit en utilisant la clé de signature du prestataire de services pour créer un certificat qui n'a pas été approuvé. Enfin, il se peut qu'un malfaiteur usurpe l'identité d'un signataire en utilisant des documents d'identité falsifiés et apparemment authentiques et réussisse à convaincre le prestataire de services de lui délivrer un certificat, et ce dans le plein respect des politiques officielles de l'émetteur et en l'absence de faute quelconque.<sup>4</sup>

7. La délivrance erronée d'un certificat à un imposteur peut avoir de très graves conséquences. Les parties qui réalisent des transactions en ligne avec l'imposteur risquent de faire fond sur les données inexactes figurant sur le certificat établi irrégulièrement et, de ce fait, expédier les marchandises, virer des fonds, accorder un crédit ou entreprendre toute autre opération dans la conviction qu'elles traitent avec la partie dont l'identité a été usurpée. Lorsque la fraude est découverte, les parties qui ont fait fond sur le certificat risquent d'avoir subi un préjudice très substantiel. En pareils cas, il y a deux parties lésées: la partie qui a été amenée à

---

<sup>3</sup> Ibid.

<sup>4</sup> Ibid.

faire fond sur le certificat délivré irrégulièrement et la personne dont l'identité a été usurpée. L'une et l'autre pourront se retourner contre le prestataire de services de certification. Une autre situation peut être celle d'un certificat délivré par négligence à une personne fictive, auquel cas seule la partie ayant accordé crédit au certificat subirait un dommage.<sup>5</sup>

8. L'article 9 de la Loi type de la CNUDCI sur les signatures électroniques stipule notamment qu'un prestataire de services de certification "prend des dispositions raisonnables pour assurer que toutes les déclarations essentielles qu'il fait concernant le certificat durant tout son cycle de vie ou figurant dans le certificat sont exactes et complètes". Cette obligation de caractère général a été transposée mot pour mot dans la législation interne de plusieurs pays ayant appliqué la Loi type<sup>6</sup> encore que, dans certains pays, la norme fondée sur le caractère "raisonnable" des dispositions à prendre ait été modifiée pour fournir une garantie plus élevée.<sup>7</sup>

9. Le régime établi par la Directive de l'Union européenne relative aux signatures électroniques fait aux États membres de l'Union, "au minimum", l'obligation de veiller à ce que les prestataires de services de certification, en délivrant un certificat au public sous forme de certificat qualifié ou en garantissant qu'un tel certificat a un caractère public, soient responsables des dommages causés à toute entité ou à toute personne physique ou morale qui fait raisonnablement fond sur lesdits certificats: a) en ce qui concerne l'exactitude, au moment de son émission, de toutes les informations figurant dans le certificat qualifié et le fait que le certificat contient tous les détails que doit comporter un certificat qualifié; b) le fait qu'à la date d'émission du certificat, le signataire identifié sur le certificat qualifié avait le contrôle des données de création de signature correspondant aux données de vérification de signature indiquées sur le certificat; et c) le fait que les données afférentes à la création de signature et les données de vérification de la signature peuvent être utilisées de manière complémentaire dans les cas où elles sont générées les unes et les autres par le prestataire de services de certification. Cette responsabilité s'entend à moins que le prestataire de services de certification puisse apporter la preuve qu'il n'a pas agi de manière négligente.<sup>8</sup>

10. Les législations d'autres pays coïncident généralement en imposant aux prestataires de services de certification l'obligation de vérifier l'exactitude des informations sur la base desquelles un certificat est délivré. Dans certains pays, le prestataire de services est généralement tenu pour responsable à l'égard de toute personne qui a raisonnablement fait fond sur l'exactitude de toutes les informations figurant sur le certificat accrédité, à compter de la date à laquelle celui-ci a été

---

<sup>5</sup> Ibid.

<sup>6</sup> Par exemple le paragraphe 2 de l'article 28 de la Loi thaïlandaise de 2001 sur les transactions électroniques et l'article 28 b) de la Loi de 2000 relative aux transactions électroniques des îles Caïmanes (territoire britannique d'outremer).

<sup>7</sup> Par exemple, l'article 22 de la Loi relative aux signatures électroniques de la Chine: "Les prestataires de services électroniques de certification **doivent veiller** à ce que le contenu des certificats de signature électronique soient complets et exacts pendant tout leur cycle de vie et faire en sorte que les parties qui s'en remettent aux signatures électroniques puissent vérifier ou comprendre l'intégralité du contenu des certificats et les autres questions pertinentes" (les caractères gras sont du secrétariat).

<sup>8</sup> Directive de l'Union européenne relative aux signatures électroniques (voir note [...]), article 6, paragraphe 1.

établi,<sup>9</sup> ou de la date à laquelle la véracité de cette information a été garantie,<sup>10</sup> bien que, dans certains de ces pays, le prestataire de services puisse limiter sa responsabilité en insérant dans le certificat une mention appropriée.<sup>11</sup> Toutefois, la législation de certains pays exonère expressément le prestataire de services de certification de responsabilité du fait de l'inexactitude des informations fournies par le signataire, sous réserve de vérification conformément aux pratiques applicables aux certificats, aussi longtemps qu'il peut apporter la preuve qu'il a adopté toutes les mesures raisonnables pour vérifier les informations.<sup>12</sup>

11. D'autres pays parviennent au même résultat non pas une garantie légale, mais en imposant aux prestataires de services de certification l'obligation générale de vérifier les informations fournies par le signataire avant d'établir un certificat<sup>13</sup> ou d'établir des systèmes permettant de vérifier ces informations.<sup>14</sup> Dans certains cas, le prestataire de services est tenu de révoquer immédiatement le certificat s'il constate que les informations sur la base desquelles celui-ci a été établi étaient inexacts ou fausses.<sup>15</sup> Parfois, cependant, la loi est muette sur la délivrance des certificats, se bornant à stipuler que le prestataire de services de certification doit se conformer à ses pratiques déclarées<sup>16</sup> ou délivrer le certificat comme convenu avec le signataire.<sup>17</sup> Cela ne signifie pas que la loi exonère totalement de responsabilité les prestataires de services de certification. Au contraire, la législation de certains États réglemente expressément la responsabilité des prestataires de services de certification en exigeant de ceux-ci qu'ils contractent une police d'assurance aux tiers adéquate pour couvrir tous les dommages contractuels et quasi délictuels causés à des signataires et à des tiers.<sup>18</sup>

---

<sup>9</sup> Paragraphe 1 a) de l'article 20 du Titre 308B de la Loi de 1998 sur les transactions électroniques de la Barbade; article 23 de la Loi de 1999 sur les transactions électronique des Bermudes; article 36 e) de la Loi de 2000 relative aux technologies de l'information de l'Inde; paragraphe 2 d) de l'article 27 de la Loi de 2000 sur les transactions électroniques de Maurice; article 39 de l'Ordonnance relative aux transactions électroniques de la Région administrative spéciale chinoise de Hong Kong; et alinéas a) et c) du paragraphe 2 de l'article 29 et paragraphe 1 de l'article 30 de la Loi relative aux transactions électroniques de Singapour.

<sup>10</sup> Article 18 de la Loi relative aux échanges et au commerce électroniques de la Tunisie; et article 31 d) de la Loi sur les transactions électroniques du Viet Nam.

<sup>11</sup> Par exemple, Barbade, Bermudes, Maurice, RAS de Hong Kong et Singapour.

<sup>12</sup> Article 39 c) de la Loi de 2001 relative aux signatures électroniques de l'Argentine.

<sup>13</sup> Ibid., article 21 o); article 12 e) de la Loi relative aux documents électroniques, aux signatures électroniques et aux services de certification desdites signatures du Chili; paragraphe I) de l'article 104 du Code de commerce du Mexique: Décret de 2003 relatif aux signatures électroniques; et article 35 de la Loi relative aux messages de données et signatures électroniques de la République bolivarienne du Venezuela.

<sup>14</sup> Article 30 d) de la Loi relative au commerce électronique, aux signatures électroniques et aux messages de données de l'Équateur.

<sup>15</sup> Article 19 e) 2) de la Loi de 2001 relative aux signatures numériques de l'Argentine.

<sup>16</sup> Article 29 a) du Décret d'application de la Loi relative aux signatures et certificats numériques du Pérou.

<sup>17</sup> Article 32 a) de la Loi No. 527 relative au commerce électronique de la Colombie; paragraphe 7 de l'article 49 de la Loi de 2001 relative aux signatures numériques du Panama; et l'article 40 a) de la Loi de 2002 relative au commerce électronique, aux documents et aux signatures numériques de la République dominicaine.

<sup>18</sup> Article 32 de la Loi relative aux messages et aux signatures électroniques de la République bolivarienne du Venezuela.

12. L'obligation du prestataire de services de certification de vérifier l'exactitude des informations communiquées est complétée par celle qu'a le signataire "de prendre des mesures raisonnables pour garantir l'exactitude et la complétude de toutes les informations communiquées par lui aux fins du certificat pendant tout son cycle de vie ou des informations figurant dans ledit certificat".<sup>19</sup> Le signataire pourrait par conséquent être tenu pour responsable à l'égard du prestataire de services de certification et de la partie ayant fait fond sur le certificat s'il fournit des informations fausses ou inexactes au prestataire de services lorsqu'il demande l'émission d'un certificat. Parfois, ce principe est présenté sous forme d'une obligation générale de communiquer des informations exactes au prestataire de services de certification,<sup>20</sup> ou de prendre toutes les mesures raisonnables pour garantir l'exactitude des informations fournies;<sup>21</sup> le signataire est dans certains cas expressément tenu pour responsable des dommages résultant de son inobservation de cette obligation spécifique.<sup>22</sup>

c) *Utilisation non autorisée de dispositifs de création de signature ou utilisation de dispositifs de certification ayant perdu leur fiabilité*

13. La question de l'utilisation non autorisée de dispositifs de création de signature et de certificats comporte deux aspects. D'une part, il se peut qu'un dispositif de création de signature ne soit pas conservé en lieu sûr ou perde sa fiabilité, par exemple si un agent du signataire s'en est approprié. D'un autre côté, la hiérarchie de signature effective du prestataire de services de certification peut être devenue peu fiable, par exemple si la clé de signature ou la clé principale du prestataire de services se trouvent perdues, sont divulguées à des personnes non autorisées ou utilisées par de telles personnes ou se trouvent pour d'autres raisons être dépourvues de fiabilité.

14. La sécurité de la hiérarchie de signature peut se trouver compromise de différentes façons. Il se peut que le prestataire de services de certification ou l'un de ses employés ou sous-traitants détruise la clé ou en perde le contrôle par inadvertance, que le centre de données détenant la clé privée soit endommagé par un accident ou que la clé du prestataire de services de certification soit délibérément détruite ou détournée à des fins illicites (par exemple par un pirate). Cette atteinte à l'intégrité de la hiérarchie de signature peut avoir de très graves conséquences. Par exemple, si la clé de signature privée ou les clés principales tombent entre les mains d'un malfaiteur, celui-ci pourrait générer de faux certificats et les utiliser pour assumer l'identité de signataires réels ou fictifs, au détriment des parties qui croient en l'intégrité de la signature. De plus, une fois les dommages découverts, tous les

<sup>19</sup> Loi type de la CNUDCI sur les signatures électroniques (voir note [...]), article 8, paragraphe 1 c).

<sup>20</sup> Article 25 de la Loi de 2001 relative aux signatures numériques de l'Argentine; article 24 de la Loi de 2002 relative aux documents électroniques, aux signatures électroniques et aux services de certification de telles signatures du Chili; et article 99 (III) du Code de commerce du Mexique: Décret de 2003 relatif aux signatures électroniques.

<sup>21</sup> Article 31 c) de la Loi de 2000 relative aux transactions électroniques des îles Caïmanes.

<sup>22</sup> Article 40 de la Loi No. 527 relative au commerce électronique de la Colombie; article 99 (III) du Code de commerce du Mexique: Décret de 2003 relatif aux signatures électroniques; article 39 de la Loi de 2001 relative aux signatures numériques du Panama; et article 55 de la Loi de 2002 relative au commerce électronique, aux documents et aux signatures numériques de la République dominicaine.

certificats établis par les prestataires de services en question devraient être révoqués, ce qui pourrait entraîner un déluge de réclamations de la part de l'ensemble de la communauté des signataires.

15. Cette question n'est pas traitée en détail dans la Loi type de la CNUDCI sur les signatures électroniques. Certes, l'obligation générale qu'a le prestataire de services de certification en vertu de la Loi type d'utiliser "des systèmes, des procédures et des ressources humaines fiables pour la prestation de ses services"<sup>23</sup> peut être interprétée comme lui imposant l'obligation de prendre toutes les mesures nécessaires pour empêcher que sa propre clé (et par conséquent l'ensemble de la hiérarchie de signature) se trouve compromise. La législation interne de plusieurs États prévoit expressément une telle obligation, laquelle est fréquemment combinée à celle qui est imposée au prestataire de services de certification d'utiliser des systèmes fiables.<sup>24</sup> Parfois, la législation impose une obligation spécifique d'adopter des mesures pour éviter la falsification des certificats.<sup>25</sup> Le prestataire de services de certification a l'obligation de s'abstenir de créer les données afférentes à la création de signature des signataires ou d'y avoir accès et peut voir sa responsabilité engagée si ses employés le font délibérément.<sup>26</sup> Si ses données afférentes à la création de signature étaient compromises, le prestataire de services de certification aurait l'obligation de demander la révocation de son propre certificat.<sup>27</sup>

16. Le signataire, quant à lui, a également l'obligation de prendre toutes les précautions possibles. Aux termes de la Loi type de la CNUDCI sur les signatures électroniques, par exemple, le signataire doit prendre "des dispositions raisonnables pour éviter toute utilisation non autorisée de ses données afférentes à la création de signature".<sup>28</sup> Une obligation semblable est imposée par la législation interne de la plupart des États, bien qu'avec certaines variations. Dans certains cas, la loi impose au signataire l'obligation rigoureuse de conserver le contrôle exclusif des dispositifs de création de signature et d'empêcher qu'ils soient utilisés sans autorisation,<sup>29</sup> ou rend le signataire exclusivement responsable de la bonne garde du dispositif de

---

<sup>23</sup> Loi type de la CNUDCI sur les signatures électroniques (voir note [...]), article 9, paragraphe 1 f).

<sup>24</sup> Alinéas c) et d) de l'article 21 de la Loi de 2001 sur les signatures numériques de l'Argentine; article 32 b) de la Loi No. 527 relative au commerce électronique de la Colombie; article 24 de la Loi de 2000 relative aux transactions électroniques de Maurice; paragraphe 5 de l'article 49 de la Loi de 2001 relative aux signatures numériques de Panama; paragraphe 6 de l'article 28 de la Loi de 2001 sur les transactions électroniques de la Thaïlande, et article 13 de la Loi relative aux échanges et au commerce électroniques de la Tunisie.

<sup>25</sup> Article 35 de la Loi relative aux messages de données et signatures électroniques de la République bolivarienne du Venezuela.

<sup>26</sup> Article 21 b) de la Loi de 2001 relative aux signatures numériques de l'Argentine.

<sup>27</sup> Ibid., article 21 p).

<sup>28</sup> Loi type de la CNUDCI sur les signatures électroniques (voir note [...]), article 8, paragraphe 1 a).

<sup>29</sup> Article 25 a) de la Loi de 2001 relative aux signatures numériques de l'Argentine; paragraphe 3 de l'article 39 de la Loi No. 527 relative au commerce électronique de la Colombie; paragraphe 1 de l'article 12 de la Loi fédérale de 2002 relative aux signatures numériques et électroniques de la Fédération de Russie; paragraphe 4 de l'article 37 de la Loi de 2001 relative aux signatures numériques du Panama; article 53 d) de la Loi de 2002 relative au commerce électronique, aux documents et aux signatures numériques de la République dominicaine; et article 15 e) de l'Ordonnance relative aux procédures et principes applicables à la mise en œuvre de la Loi de 2005 relative aux signatures électroniques de la Turquie.

création de signature.<sup>30</sup> Fréquemment, toutefois, cette obligation est nuancée et consiste simplement à maintenir le contrôle adéquat sur le dispositif de création de signature ou à adopter les mesures appropriées pour en conserver le contrôle,<sup>31</sup> à faire preuve de diligence pour éviter qu'il soit utilisé sans autorisation<sup>32</sup> ou à prendre les mesures raisonnables pour éviter que son dispositif de signature soit utilisé sans autorisation.<sup>33</sup>

d) *Non-suspension ou non-révocation d'un certificat*

17. Le prestataire de services de certification peut également voir sa responsabilité engagée s'il s'abstient de suspendre ou de révoquer un certificat ayant perdu sa fiabilité. Si l'on veut qu'une infrastructure de signatures numériques fonctionne comme il convient et inspire confiance, il est indispensable qu'il existe un mécanisme permettant de déterminer en temps réel si tel ou tel certificat est valable ou s'il a été suspendu ou révoqué. Lorsqu'une clé privée a perdu son caractère confidentiel, par exemple, la révocation du certificat constitue le principal mécanisme grâce auquel le signataire peut se protéger contre les transactions frauduleuses entreprises par un imposteur pouvant avoir obtenu copie de sa clé privée.

18. De ce fait, la rapidité avec laquelle le prestataire de services de certification peut révoquer ou suspendre un certificat à la demande du signataire revêt une importance critique. Le laps de temps qui s'écoule entre la demande de révocation d'un certificat présentée par un signataire, sa révocation effective et la publication de l'avis de révocation peut permettre à un imposteur de mener à bien sa transaction frauduleuse. En conséquence, si le prestataire de services de certification tarde sans raison à mentionner la révocation sur la liste de certificats révoqués ou omet de le faire, aussi bien le signataire que la partie lésée qui a fait fond sur les signatures risque de subir un sérieux préjudice pour s'être fié à un certificat apparemment valable. En outre, les prestataires de services de certification peuvent, dans le cadre des services qu'ils offrent, proposer de tenir un répertoire et des listes de certificats révoqués auxquels les parties puissent avoir accès en ligne. Cependant, l'administration d'une telle base de données comporte essentiellement un double risque: celui que le répertoire ou la liste de certificats révoqués soient inexacts, ce qui peut conduire la partie qui les consulte à faire fond à ses dépens sur les informations erronées; et celui que le répertoire ou la liste de certificats révoqués ne

<sup>30</sup> Article 21 de la Loi relative aux échanges et au commerce électroniques de la Tunisie.

<sup>31</sup> Article 24 de la Loi de 2002 sur les documents électroniques, les signatures électroniques et les services de certification de telles signatures du Chili; et paragraphe 2 a) de l'article 25 de la Loi relative aux transactions électroniques du Viet Nam.

<sup>32</sup> Article 19 de la Loi relative aux messages de données et signatures électroniques de la République bolivarienne du Venezuela.

<sup>33</sup> Article 17 b) de la Loi relative au commerce électronique, aux signatures électroniques et aux messages de données de l'Équateur; article 39 a) de la Loi de 2000 relative aux transactions électroniques des îles Caïmanes; paragraphe 1 de l'article 42 de la Loi de 2000 relative aux technologies de l'information de l'Inde; alinéas a) et b) du paragraphe 1 de l'article 35 de la Loi de 2000 relative aux transactions électroniques de Maurice; article 99 (II) du Code de commerce du Mexique; Décret de 2003 relatif aux signatures électroniques; article 39 (titre 88) de la Loi relative aux transactions électroniques de Singapour; et paragraphe 1 de l'article 27 de la Loi de 2001 sur les transactions électroniques de la Thaïlande.

soient pas disponibles (par exemple par suite d'une panne du système), empêchant ainsi les signataires et leurs cocontractants de mener à bien leurs transactions.

19. Comme indiqué ci-dessus, la Loi type de la CNUDCI sur les signatures électroniques prend pour hypothèse que le prestataire de services de certification peut émettre des certificats de divers niveaux caractérisés par des degrés divers de fiabilité et de sécurité. En conséquence, la Loi type n'impose pas toujours à un prestataire de services l'obligation de mettre en place un système de révocation, ce qui pourrait ne pas être commercialement viable pour certains types de certificats de faible valeur. La Loi type se borne par conséquent à stipuler que le prestataire de services de certification doit fournir "des moyens raisonnablement accessibles" pour permettre à toute partie se fiant au certificat de déterminer à partir de celui-ci, notamment, "s'il existe des moyens pour le signataire d'adresser une notification" que les données afférentes à la création de signature ont été compromises et "la disponibilité d'un service de révocation en temps utile".<sup>34</sup> Si tel est le cas, le prestataire de services de certification a l'obligation de veiller à ce qu'il soit disponible.<sup>35</sup>

20. Le régime établi par la Directive de l'Union européenne sur les signatures électroniques fait aux États membres de l'Union, "au minimum", l'obligation de veiller à ce que le prestataire de services de certification ayant établi un certificat qualifié au public soit, à charge pour lui de prouver qu'il n'a pas agi par négligence, responsable des dommages causés à toute entité ou à toute personne physique ou morale s'étant raisonnablement fiée au certificat s'il n'a pas publié la révocation de celui-ci.<sup>36</sup> La législation interne de certains États fait au prestataire de services de certification l'obligation d'adopter des mesures pour prévenir la falsification des certificats<sup>37</sup> ou pour révoquer immédiatement un certificat dès qu'il apprend que les informations sur la base desquelles le certificat a été émis étaient inexactes ou fausses.<sup>38</sup>

21. Le signataire et les autres personnes autorisées peuvent également être soumis à une obligation semblable. La Loi type de la CNUDCI sur les signatures électroniques, par exemple, stipule que chaque signataire "sans retard injustifié, utilise les moyens fournis par le prestataire de services de certification" ou "fait d'une autre manière des efforts raisonnables pour aviser toute personne dont il peut raisonnablement penser qu'elle se fie à la signature électronique ou qu'elle fournit des services visant à étayer la signature électronique" s'il sait "que les données afférentes à la création de signature ont été compromises" ou s'il estime "au regard des circonstances connues de lui, qu'il y a un risque important que les données afférentes à la création de signature aient été compromises".<sup>39</sup>

---

<sup>34</sup> Loi type de la CNUDCI sur les signatures électroniques (voir note [...]), article 9, alinéas d), v) et vi) du paragraphe 1.

<sup>35</sup> Ibid., article 9, paragraphe 1 e).

<sup>36</sup> Directive de l'Union européenne relative aux signatures électroniques (voir note [...]), article 6, paragraphe 2; voir également l'alinéa b) de l'annexe II à la Directive.

<sup>37</sup> Paragraphe 6 de l'article 49 de la Loi de 2001 relative aux signatures numériques de Panama.

<sup>38</sup> Article 19 e) 2) de la Loi de 2001 relative aux signatures numériques de l'Argentine.

<sup>39</sup> Loi type de la CNUDCI sur les signatures électroniques (voir note [...]), article 8, alinéas i) et ii) du paragraphe 1 b).

22. Les législations nationales stipulent fréquemment que le signataire a l'obligation de demander la révocation du certificat lorsque la confidentialité des données afférentes à la création de signature risque d'avoir été compromise,<sup>40</sup> bien que, dans certains cas, les signataires soient simplement tenus de communiquer ce fait au prestataire de services de certification.<sup>41</sup> Les législations de plusieurs États ont adopté la formulation figurant dans la Loi type de la CNUDCI sur les signatures électroniques, qui fait au signataire l'obligation d'aviser toute personne dont il peut raisonnablement penser qu'elle se fie à la signature électronique ou qu'elle fournit des services visant à étayer la signature électronique.<sup>42</sup> Bien que, dans un certain nombre de systèmes juridiques, les conséquences d'un manquement à cette obligation ne soient pas expressément réglementées, la loi stipule expressément, dans certains pays, que le signataire peut voir sa responsabilité engagée s'il ne notifie pas la perte de contrôle sur la clé privée ou ne demande pas la révocation du certificat.<sup>43</sup>

## Conclusion

23. L'utilisation de plus en plus généralisée des méthodes d'authentification et de signature électroniques pourra beaucoup contribuer à réduire la documentation commerciale et les coûts connexes dans le contexte des transactions internationales. Si, dans une très large mesure, le rythme du progrès dans ce domaine dépendra surtout de la qualité et de la sécurité de solutions technologiques, le droit peut beaucoup faciliter l'utilisation des méthodes d'authentification et de signature électroniques.

---

<sup>40</sup> Article 25 c) de la Loi de 2001 sur les signatures numériques de l'Argentine; paragraphe 4 de l'article 39 de la Loi No. 527 relative au commerce électronique de la Colombie; article 17 f) de la Loi relative au commerce électronique, aux signatures électroniques et aux messages de données de l'Équateur; paragraphe 1 de l'article 12 de la Loi fédérale de 2002 relative aux signatures électroniques numériques de la Fédération de Russie; article 36 de la Loi de 2000 relative aux transactions électroniques de Maurice; paragraphe 5 de l'article 37 de la Loi de 2001 relative aux signatures numériques de Panama; articles 49 et 53 e) de la Loi de 2002 sur le commerce électronique, les documents et les signatures numériques de la République dominicaine; et article 40 (titre 88) de la Loi relative aux transactions électroniques de Singapour.

<sup>41</sup> Paragraphe 2 de l'article 42 de la Loi de 2000 relative aux technologies de l'information de l'Inde; et alinéas f) et i) de l'article 15 de l'Ordonnance de 2005 relative aux procédures et principes applicables à l'application de la Loi relative aux signatures électroniques de la Turquie.

<sup>42</sup> Article 15 de la Loi sur les signatures électroniques de la Chine; article 31 b) de la Loi de 2000 relatives aux transactions électroniques des îles Caïmanes; paragraphe 2 de l'article 27 de la Loi de 2001 sur les transactions électroniques de la Thaïlande; et paragraphe 2 b) de l'article 25 de la Loi sur les transactions électroniques du Viet Nam.

<sup>43</sup> Article 27 de la Loi sur les signatures électroniques de la Chine; article 17 e) de la Loi relative au commerce électronique, aux signatures électroniques et aux messages de données de l'Équateur; paragraphe 2 de l'article 12 de la Loi fédérale de 2002 relative aux signatures électroniques numériques de la Fédération de Russie; article 39 de la Loi de 2001 relative aux signatures numériques de Panama; article 40 de la Loi relative aux messages de données et signatures électroniques de la République bolivarienne du Venezuela; et article 55 de la Loi de 2002 sur le commerce électronique, les documents et les signatures numériques de la République dominicaine.

24. Un grand nombre de pays ont déjà adopté des mesures nationales allant dans ce sens en promulguant des lois reconnaissant la valeur juridique des communications électroniques et en définissant les critères de leur équivalence avec les documents sur support papier. Les dispositions réglementant les méthodes électroniques d'authentification de signature constituent fréquemment un élément important de ces lois. La Loi type de la CNUDCI sur le commerce électronique<sup>44</sup> est devenue l'instrument de référence le plus communément utilisé pour la promulgation de législations dans ce domaine et sa large application a contribué à harmoniser les régimes applicables au plan international. Une large ratification de la Convention des Nations Unies sur l'utilisation des communications électroniques dans les contrats internationaux<sup>45</sup> encouragerait encore plus le mouvement d'harmonisation en offrant une série déterminée de règles pour les transactions internationales.

25. L'utilisation au plan international des méthodes d'authentification et de signature électroniques pourra se trouver facilitée aussi par l'adoption de ces normes de la CNUDCI. En particulier, la flexibilité des critères d'équivalence fonctionnelle entre signatures électroniques et signatures sur support papier reflétée dans la Convention des Nations Unies sur l'utilisation des signatures électroniques dans les contrats internationaux pourra offrir un cadre international commun permettant aux méthodes d'authentification et de signature électroniques de répondre aux exigences étrangères de forme des signatures. Néanmoins, il se peut que certains problèmes persistent, en particulier pour ce qui est de l'utilisation au plan international de méthodes d'authentification des signatures électroniques qui exigent l'implication de tierces parties fiables dans le processus d'authentification ou de signature.

26. Les problèmes qui se posent dans ce domaine spécifique découlent pour une très large part du manque de cohérence de normes techniques et de la non-compatibilité des matériels ou des logiciels, ce qui se traduit par un manque d'interopérabilité au plan international. Les efforts entrepris pour harmoniser les normes et améliorer la compatibilité technique pourront déboucher sur une solution des difficultés qui existent actuellement. Néanmoins, il y a aussi des difficultés de caractère juridique liées à l'utilisation des méthodes électroniques d'authentification des signatures, en particulier dans le contexte des législations nationales qui soit prescrivent, soit privilégient, l'emploi d'une technologie déterminée pour les signatures électroniques, habituellement les techniques de signature numérique.

27. Les législations qui reconnaissent la valeur juridique des signatures numériques n'attribuent habituellement la même valeur juridique aux signatures étayées par des certificats étrangers que dans la mesure où ceux-ci sont considérés comme équivalant à des certificats nationaux. Il ressort de la présente étude que, pour apprécier comme il convient l'équivalence juridique, il faut comparer non seulement les normes techniques et de sécurité qui caractérisent une technologie de signature déterminée, mais aussi les règles qui régiraient la responsabilité des différentes parties en cause. La Loi type de la CNUDCI sur les signatures électroniques contient une série de règles fondamentales communes régissant certaines des obligations des parties qui interviennent dans le processus d'authentification des signatures et qui peuvent avoir un impact sur leur

---

<sup>44</sup> Voir note [...] [publication des Nations Unies, numéro de vente: F.99.V.4].

<sup>45</sup> Voir note [...] [Résolution 60/21 de l'Assemblée générale, annexe].

responsabilité individuelle. Il existe en outre des textes de caractère régional, comme la Directive de l'Union européenne relative aux signatures électroniques, qui offrent un cadre législatif semblable s'agissant de définir le régime de responsabilité des prestataires de services de certification qui opèrent dans la région. Cependant, aucun de ces deux textes ne se réfère aux questions de responsabilité découlant de l'utilisation au plan international de certaines électroniques d'authentification et de signature méthodes.

28. Il importe pour les législateurs et pour les décideurs de mieux saisir les différences entre les régimes nationaux de responsabilité et les éléments qui leur sont communs de manière à pouvoir établir des méthodes et procédures appropriées en matière de reconnaissance de signatures étayées par des certificats étrangers. La législation nationale des divers pays peut déjà apporter des réponses essentiellement équivalentes aux diverses questions évoquées dans le présent document de référence, par exemple parce qu'elles partagent une tradition juridique commune ou appartiennent à un cadre d'intégration régionale. Il se peut que ces pays aient intérêt à mettre au point des normes communes de responsabilité ou même harmoniser leurs règles nationales, de manière à faciliter l'utilisation transfrontière des méthodes d'authentification et de signature électroniques.

---