Nations Unies A/CN.9/630

Assemblée générale

Distr.: Générale
25 avril 2007

Français
Original: Anglais

Commission des Nations Unies pour le droit commercial international
Quarantième session
Vienne, 25 juin-12 juillet 2007

Travaux futurs possibles dans le domaine du commerce électronique

Document de référence général sur les éléments requis pour créer un cadre juridique favorable pour le commerce électronique: spécimen de chapitre sur l'utilisation internationale des méthodes d'authentification et de signature électroniques

Note du secrétariat*

1. En 2004, ayant achevé ses travaux sur la Convention sur l'utilisation de communications électroniques dans les contrats internationaux, le Groupe de travail IV (Commerce électronique) de la Commission des Nations Unies pour le droit commercial international (CNUDCI) a prié le secrétariat de continuer à suivre diverses questions liées au commerce électronique, notamment les questions liées à la reconnaissance transfrontière des signatures électroniques, et de publier les résultats de ses recherches en vue de faire des recommandations à la Commission sur le point de savoir s'il serait possible d'entreprendre des travaux dans ces domaines (voir A/CN.9/571, par. 12).

2. En 2005, la Commission a pris note des travaux entrepris par d'autres organisations dans divers domaines liés au commerce électronique et prié le secrétariat de réaliser une étude plus détaillée, qui devrait contenir des propositions sur la forme et la nature d'un document de référence général examinant les divers éléments requis pour créer un cadre juridique favorable au commerce électronique, que la Commission pourrait envisager d'élaborer dans l'avenir afin d'aider les

* Ce document du secrétariat de la Commission des Nations Unies pour le droit commercial international a été soumis avec retard pour cause de sous-effectif.

V.07-82775 (F) 240507 250507

législateurs et les responsables politiques du monde entier[1]. En 2006, la CNUDCI a examiné une note établie par son secrétariat conformément à cette demande (A/CN.9/604). Cette note identifiait les domaines suivants comme éléments possibles d'un document de référence général: a) authentification et reconnaissance internationale des signatures électroniques; b) responsabilité et normes de conduite pour les fournisseurs d'accès à Internet; c) facturation électronique et questions juridiques liées aux chaînes logistiques dans le commerce électronique; d) transfert de droits sur des biens meubles corporels et d'autres droits par des communications électroniques; e) concurrence déloyale et pratiques commerciales trompeuses dans le commerce électronique; et f) vie privée et protection des données dans le commerce électronique. La note indiquait aussi d'autres questions qui, bien que de façon abrégée, pourraient être traitées dans un tel document: a) protection des droits de propriété intellectuelle; b) communications électroniques non sollicitées (spams); et c) cybercriminalité.

3. Selon un avis, qui a été appuyé, la tâche des législateurs et des responsables politiques, en particulier dans les pays en développement, se trouverait considérablement facilitée si la Commission élaborait un document de référence général traitant des questions mises en évidence par le secrétariat. Un tel document, a-t-on ajouté, pourrait aussi aider la Commission à identifier des domaines dans lesquels elle pourrait entreprendre elle-même des travaux d'harmonisation dans l'avenir. Selon un autre point vue, cependant, l'éventail des questions proposées était trop large et il faudrait peut-être réduire la portée du document de référence général. La Commission est finalement convenue de demander à son secrétariat de préparer un spécimen de chapitre du document de référence général traitant spécifiquement de questions liées à l'authentification et à la reconnaissance internationale des signatures électroniques, pour examen à sa quarantième session, en 2007[2].

4. L'annexe de la présente note contient la partie introductive d'un spécimen de chapitre traitant des questions juridiques liées à l'utilisation internationale de méthodes d'authentification et de signature électroniques (ci-après "le spécimen de chapitre"). Les additifs à la présente note examinent le traitement juridique de l'authentification et des signatures électroniques ainsi que des problèmes juridiques découlant de leur utilisation internationale.

5. La Commission voudra peut-être examiner la structure, le niveau de détail, la nature de la discussion et le type de conseils donnés dans le spécimen de chapitre et se demander s'il serait souhaitable et utile que le secrétariat rédige d'autres chapitres sur le même modèle, pour traiter d'autres questions que la Commission pourrait choisir parmi celles qui ont été proposées antérieurement (voir par. 2 ci-dessus). Une alternative serait que la Commission demande au secrétariat de continuer à suivre de près les développements juridiques dans les domaines pertinents en vue de faire des suggestions appropriées en temps utile. Dans ce cas, elle souhaitera peut-être se demander s'il faudrait prier le secrétariat de publier le spécimen de chapitre, avec toutes modifications qu'elle pourrait juger appropriées, comme publication indépendante.

---

[1] *Documents officiels de l'Assemblée générale, Soixantième session, Supplément n° 17* (A/60/17), par. 214.

[2] Ibid., *Soixantième et unième session, Supplément n° 17* (A/61/17), par. 216.

Annexe

Table des matières

Avant-propos

Le présent document analyse les principales questions juridiques découlant de l'utilisation de méthodes de signatures et d'authentification électroniques dans les opérations internationales. La première partie donne un aperçu d'ensemble de ces méthodes et leur traitement juridique dans divers pays (voir ci-dessous, par. […] à [...])*. La deuxième partie examine leur utilisation dans les opérations internationales et indique les principales questions juridiques liées à leur reconnaissance transfrontière (voir ci-dessous, par. […] à [...]).

On a fait observer que, sur le plan international, les difficultés juridiques seront sans doute liées davantage à l'utilisation transfrontière des méthodes de signature et d'authentification électroniques qui demandent l'intervention de tiers dans le processus de signature ou d'authentification. C'est le cas par exemple des méthodes étayées par des certificats émis par un tiers de confiance prestataire de services de certification, en particulier les signatures numériques dans une infrastructure à clef publique. C'est pour cette raison qu'une attention spéciale est accordée dans la deuxième partie du document à l'utilisation internationale des signatures numériques dans une infrastructure à clef publique. Il ne faudrait pas y voir pour autant l'expression d'une préférence ou d'une prise de position en faveur d'un type particulier de méthode ou technologie d'authentification.

Introduction

1. L'informatique et la technologie de l'information ont mis au point divers moyens pour relier l'information sous forme électronique à des personnes ou à des entités particulières, pour assurer l'intégrité de ces informations ou pour permettre à ces personnes de démontrer qu'elles ont le droit ou l'autorisation d'accéder à un certain service ou à une certaine source d'information. On parle parfois de façon générique, à propos de ces fonctions, de méthodes d'"authentification" électronique ou de "signature" électronique. Parfois, cependant, des distinctions sont faites entre "authentification" électronique et "signature" électronique. L'usage de la terminologie non seulement est incohérent, mais aussi, dans une certaine mesure, source de méprises. Dans un environnement papier, les mots "authentification" et "signature" ainsi que les actions d'"authentifier" et de "signer" n'ont pas exactement la même connotation selon les systèmes juridiques et ont des fonctionnalités qui ne correspondent pas toujours nécessairement à l'objet et à la fonction de ce que l'on appelle les méthodes d'"authentification" et de "signature" électroniques. De plus, le mot "authentification" est parfois utilisé de manière générique en liaison avec l'assurance à la fois de la qualité d'auteur et de l'intégrité de l'information, mais certains systèmes juridiques peuvent faire une distinction entre ces éléments. Il est donc nécessaire de passer brièvement en revue les différences de terminologie et d'interprétation juridique afin d'établir le champ d'application du présent document.

2. Dans les pays de *common law*, pour la preuve civile, un enregistrement ou un document est considéré comme "authentique" s'il y a la preuve "qu'il est ce que son

* Tous les renvois dans le présent document et ses additifs, ainsi que tous les renvois dans leurs notes, seront finalisés lorsque le document final sera publié sous forme consolidée.

auteur prétend”[1]. La notion de “document” en tant que telle est très large et englobe généralement “toute chose dans laquelle des informations de toute nature sont enregistrées”[2]. Elle engloberait, par exemple, des choses telles que des photographies de tombes et de maisons[3], des livres comptables[4] et des dessins et plans[5]. On établit la pertinence d’un document comme élément de preuve en le reliant à une personne, à un endroit ou à une chose, processus qui dans certains pays de *common law* est connu sous le nom d’“authentification”[6]. La signature d’un document est un moyen courant – mais non exclusif – d’“authentification” et, selon le contexte, les mots “signer” et “authentifier” peuvent être synonymes[7].

3. Une “signature, quant à elle, est “tout nom ou symbole utilisé par une partie avec l’intention d’en faire sa signature”[8]. Il est entendu que l’objet de lois qui exigent qu’un document particulier soit signé par une personne particulière est de confirmer la sincérité du document[9]. Le cas paradigmatique de la signature est le nom du signataire, écrit de sa propre main, sur un document papier (signature “manuscrite”)[10]. Toutefois, la signature manuscrite n’est pas le seul type concevable de signature. Du fait que les tribunaux considèrent les signatures comme “une simple marque”, à moins que la loi en question exige qu’elle soit autographe, “le nom imprimé de la partie qui est tenue de signer le document suffit”, ou la signature “peut être imprimée sur le document au moyen d’un cachet où est gravé un fac-similé de la signature ordinaire du signataire”, à condition que la preuve soit fournie dans de tels cas “que le nom imprimé sur le cachet a été apposé par le signataire,” ou que cette signature “a été reconnue et que le signataire a été informé qu’elle avait été faite sous son autorité pour être appropriée à l’instrument particulier”[11].

---

[1] États-Unis d’Amérique, Federal Rules of Evidence, article 901, subdivision a) (“L’exigence d’authentification ou d’identification comme condition préalable à la recevabilité est satisfaite par un témoignage suffisant pour appuyer la constatation que le contenu du document est ce que prétend son auteur.”).

[2] Royaume-Uni de Grande-Bretagne et d’Irlande du Nord, Civil Evidence Act 1995, chapitre 38, section 13.

[3] *Lyell v. Kennedy (n° 3)* (1884) 27 Ch.D.1 (Royaume-Uni, Chancery Division).

[4] *Hayes v. Brown* [1920] 1 K.B. 250 (Royaume-Uni, Law Reports, King’s Bench).

[5] *J. H. Tucker & Co., Ltd. v. Board of Trade* [1955] 2 All ER 522 (Royaume-Uni, All England Law Reports).

[6] *Farm Credit Bank of St. Paul v. William G. Huether*, 12 avril 1990 (454 N.W.2d 710, 713) (États-Unis, Supreme Court of North Dakota, North Western Reporter).

[7] Dans le contexte de l’article 9 révisé du Code de commerce uniforme des États-Unis, par exemple, “authentifier” est défini comme “(A) signer”; ou “(B) exécuter ou adopter d’une autre manière un symbole, ou coder ou traiter de façon similaire un enregistrement en totalité ou en partie, avec l’intention présente de la personne authentifiante d’identifier la personne et d’adopter ou d’accepter un enregistrement”.

[8] *Alfred E. Weber v. Dante De Cecco*, 14 octobre 1948 (1 N.J. Super. 353, 358) (États-Unis, New Jersey Superior Court Reports).

[9] *Lobb v Stanley* (1844), 5 Q.B. 574, 114 E.R. 1366 (Royaume-Uni, Law Reports, Queen’s Bench).

[10] Lord Denning in *Goodman v. Eban* [1954] Q.B.D. 550 at 56; “Dans l’usage anglais moderne, lorsqu’un document doit être signé par une personne, cela signifie que cette personne doit écrire son nom de sa propre main.” (Royaume-Uni, Queen’s Bench Division).

[11] *R. v. Moore: ex parte Myers* (1884) 10 V.L.R. 322 at 324 (Royaume-Uni, Victorian Law Reports).

4. Dans les pays de *common law*, c'est généralement dans le "British Statute of Frauds" (loi britannique sur les fraudes)[12] et ses versions dans d'autres pays[13] que l'on trouve des prescriptions légales en matière de signature comme condition de la validité de certains actes. Avec le temps, les tribunaux ont eu tendance à interpréter cette loi de façon libérale, en reconnaissant que ses prescriptions rigoureuses concernant la forme avaient été conçues dans des circonstances particulières[14] et que l'observation stricte de ses règles risquait inutilement de priver les contrats d'effets juridiques[15]. Ainsi, au cours des 150 dernières années, les pays de *common law* ont vu évoluer le concept de "signature", avec un déplacement d'accent de la forme à la fonction[16]. Des variations sur ce thème ont été envisagées épisodiquement par les tribunaux anglais, allant de simples modifications telles que des croix[17] ou des initiales[18], l'usage de pseudonymes[19] et de formules d'identification[20], aux noms imprimés[21], à la signature par des tiers[22] et des

---

[12] Le "Statute of Frauds" (loi sur les fraudes) a été adopté initialement en Grande-Bretagne en 1677 "pour prévenir de nombreuses pratiques frauduleuses dont on essaie souvent de défendre la validité par faux témoignage ou incitation au faux témoignage." La plupart de ses dispositions ont été abrogées au Royaume-Uni au XX^{e} siècle.

[13] Par exemple, l'article 2-201, alinéa 1 du Code de commerce uniforme des États-Unis, qui a exprimé le Statute of Frauds comme suit: "Sauf dispositions contraires contenues dans cet article, un contrat de vente de marchandises d'un montant égal ou supérieur à 500 dollars, ne peut être invoqué par voie d'action ou d'exception, à moins qu'il n'existe un écrit suffisant pour prouver qu'un contrat de vente a été conclu entre les parties, signé par la partie contre laquelle l'exécution est demandée, ou par son mandataire ou son courtier."

[14] "Le Statute of Frauds a été adopté en un temps où le corps législatif était enclin à considérer que les affaires devraient être jugées selon des règles fixes, au lieu de laisser le jury examiner l'effet de la preuve dans chaque cas. Cette conception a sans aucun doute son origine, dans une certaine mesure, dans le fait qu'à cette époque le demandeur et le défendeur n'étaient pas des témoins compétents." (J. Roxborough, in *Leeman v. Stocks* (1951) 1 Ch 941 at 947-8) (Royaume-Uni, Law Reports, Chancery Division citing approval for the views of J. Cave in *Evans v. Hoare* [1892] 1 QB 593 at 597) (Royaume-Uni, Law Reports, Queen's Bench).

[15] Comme l'a expliqué Lord Bingham of Cornhill "Il est rapidement devenu évident que si la solution adoptée au dix-septième siècle réglait un problème, elle pouvait en créer un autre, à savoir qu'une partie, concluant ce qu'elle pensait être une convention verbale contraignante et agissant en conséquence, voyait ses attentes commerciales déçues quand, au moment de l'exécution, l'autre partie invoquait avec succès l'absence de note écrite de la convention." (*Actionstrength Limited v. International Glass Engineering*, 3 avril 2003, [2003] UKHL 17) (Royaume-Uni, House of Lords).

[16] Chris Reed, "What is a Signature?", *The Journal of Information, Law and Technology*, vol. 3 (2000), et la référence à la jurisprudence qui y figure (http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/reed/, consulté le 7 février 2007).

[17] *Baker v. Dening* (1838) 8 A. & E. 94 (Royaume-Uni, Adolphus and Ellis' Queen's Bench Reports).

[18] *Hill v. Hill* [1947] Ch 231 (Royaume-Uni, Chancery Division).

[19] *Redding, in re* (1850) 14 Jur. 1052, 2 Rob. Ecc. 339 (Royaume-Uni, Jurist Reports and Robertson's Ecclesiastical Reports).

[20] *Cook, In the Estate of (Deceased) Murison v. Cook and Another* [1960] 1 All ER 689 (Royaume-Uni, All England Law Reports).

[21] *Brydges v. Dicks* (1891) 7 TLR 215 (cité dans *Brennan v. Kinjella Pty Ltd.*, Supreme Court of New South Wales, 24 juin 1993, 1993 NSW LEXIS 7543, 10). Typewriting has also been considered in *Newborne v. Sensolid (Great Britain), Ltd.* [1954] 1 QB 45 (Royaume-Uni, Law Reports, Queen's Bench).

[22] *France v. Dutton*, 24 avril 1891 [1891] 2 QB 208 (Royaume-Uni, Law Reports, Queen's Bench).

tampons en caoutchouc[23]. Dans tous ces cas les tribunaux ont été capables de régler la question de savoir si la signature était valable en faisant une analogie avec une signature manuscrite. On pourrait donc dire que dans un contexte caractérisé par quelques exigences générales de forme rigides, les tribunaux des pays de *common law* ont eu tendance à développer une interprétation assez large des notions d'"authentification" et de "signature", en s'intéressant plus à l'intention des parties qu'à la forme de leurs actes.

5. Les pays de droit romano-germanique ont une approche de l'"authentification" et de la "signature" qui diffère à certains égards de celle des pays de *common law*. Ils suivent pour la plupart la règle de la liberté de la forme pour les engagements contractuels dans les matières de droit privé, expressément[24] ou implicitement[25], sous réserve toutefois d'un catalogue plus ou moins long d'exceptions selon les pays. Cela signifie qu'il n'est pas nécessaire en règle générale que les contrats soient "écrits" ou "signés" pour être valides et exécutoires. Certains de ces pays, toutefois, exigent en général un écrit pour prouver le contenu des contrats, sauf en matière commerciale[26]. Contrairement aux pays de *common law*, les pays de droit romano-germanique tendent à interpréter les règles de la preuve de manière assez stricte. Le plus souvent, les règles de preuve civile établissent une hiérarchie des preuves pour prouver le contenu des contrats civils et commerciaux. Occupent le rang le plus élevé les documents délivrés par des autorités publiques, suivis par les actes (originaux) sous seing privé. Souvent, cette hiérarchie est conçue de manière que les notions de "document" et de "signature", bien que formellement distinctes, puissent devenir presque indissociables[27]. D'autres pays de droit romano-

---

23 *Goodman v. J. Eban Ltd.*, [1954] 1 QB 550, cited in *Lazarus Estates, Ltd. v. Beasley*, Court of Appeal, 24 janvier 1956 ([1956] 1 QB 702); *London County Council v. Vitamins, Ltd., London County Council v. Agricultural Food Products, Ltd.*, Court of Appeal, 31 mars 1955 [1955] 2 QB 218 (Royaume-Uni, Law Reports, Queen's Bench).

24 Cela est reconnu, par exemple, à l'article 11, paragraphe 1, du Code suisse des obligations. De même, le § 215 du code civil allemand dispose que les accords ne sont invalidés que lorsqu'ils ne respectent pas une forme *prescrite* par la loi ou convenue par les parties. Sauf dans de tels cas, il est généralement entendu que les contrats de droit privé ne sont pas soumis à des exigences de forme particulières. Lorsque la loi prescrit expressément une forme particulière, cette exigence doit être interprétée de façon stricte.

25 En France, par exemple, la liberté de la forme est une conséquence des règles de base applicables à la formation des contrats en vertu du Code civil. Selon l'article 1108 du Code civil français, la validité d'une convention exige le consentement de la partie qui s'oblige, sa capacité de contracter, un objet certain et une cause licite. Aux termes de l'article 1134, lorsque ces conditions sont remplies, les conventions "tiennent lieu de loi à ceux qui les ont faites". C'est également la règle en Espagne en vertu des articles 1258 et 1278 du Code civil. L'Italie suit elle aussi la même règle, mais de manière moins explicite (voir le Code civil, articles 1326 et 1350).

26 L'article 1341 du Code civil français exige un écrit pour la preuve de contrats excédant une certaine valeur, mais l'article 109 du Code de commerce admet divers types de preuve, sans hiérarchie particulière. Cela a conduit la Cour de Cassation en 1892 à reconnaître le principe général de la liberté de la preuve en matière commerciale (Cass. civ. 17 mai 1892, DP 1892.1.604; cité dans Luc Grynbaum, "Preuve", *Répertoire de droit commercial Dalloz*, juin 2002, sect. 6 et 11)).

27 Ainsi, en droit allemand, par exemple, une signature n'est pas un élément essentiel de la notion de "document" (*Urkunde*) (Gerhard Lüke et Alfred Walchshöfer, *Münchener Kommentar zur Zivilprozessordnung* (Munich, Beck, 1992), § 415, n° 6). Néanmoins, la hiérarchie des preuves documentaires établie par les § 415, 416 et 419 du code de procédure civile allemand lie clairement la signature au document. En fait, le § 416, sur la valeur probante des actes sous seing privé (*Privaturkunden*) dispose que ces derniers constituent une "preuve complète" pour

germanique, en revanche, relient de façon positive la notion de “document” à l’existence d’une “signature”[28]. Cela ne signifie pas qu’un document non signé est nécessairement dépourvu de toute valeur probante, mais il ne bénéficiera pas d’une présomption particulière et n’est généralement pas considéré comme un “commencement de preuve”[29]. La plupart des pays de tradition romano-germanique interprètent le concept d“authentification” de façon assez étroite comme signifiant que l’authenticité d’un document a été vérifiée et certifiée par une autorité publique compétente ou un officier public. En procédure civile il est courant de se référer plutôt à la notion d’“originalité” des documents.

6. Comme dans les pays de *common law*, le paradigme de la signature, dans les pays de droit romano-germanique, est la signature manuscrite. Certains pays tendent à admettre divers équivalents, y compris des reproductions mécaniques, malgré une approche généralement formaliste de la preuve[30]. D’autres pays, cependant, admettent des signatures mécaniques pour les opérations commerciales[31], mais continuaient, jusqu’à l’avènement des technologies informatiques, à exiger une signature manuscrite pour la preuve d’autres types de contrats[32]. On pourrait donc dire, compte tenu de ce principe général de liberté de la forme pour les contrats commerciaux, que les pays de droit romano-germanique tendent à appliquer des normes strictes pour évaluer la valeur probante des actes sous seing privé, et peuvent faire peu de cas des documents dont l’authenticité n’est pas immédiatement reconnaissable sur le fondement d’une signature.

7. Les considérations ci-dessus montrent non seulement que les notions de signature et d’authentification ne font pas l’objet d’une interprétation uniforme, mais aussi que les fonctions qu’elles remplissent varient selon les systèmes juridiques. Malgré ces divergences, il existe quelques éléments généraux communs. Les notions d’“authentification” et d’“authenticité” sont généralement interprétées en droit comme renvoyant à la sincérité d’un document ou d’un enregistrement, c’est-à-dire que le document est le support “original” des renseignements qu’il contient, sous la forme où il a été enregistré et sans altération. Les signatures, pour leur part, remplissent trois fonctions principales dans l’environnement papier: elles permettent d’identifier le signataire (fonction d’identification); elles apportent une certitude quant à la participation en personne de l’intéressé à l’acte de signature (fonction de preuve); et elles associent cette personne avec la teneur d’un document

---

l’information qu’ils contiennent tant qu’ils sont signés par l’auteur ou par une signature légalisée (ZPO § 416). Du fait que rien n’est prévu pour les actes sans signature, il semble qu’ils partagent le sort des documents défectueux (c’est-à-dire altérés, endommagés), dont la valeur probante est “établie librement” par les tribunaux (ZPO § 419).

[28] Ainsi, en France, la signature est un “élément essentiel” des actes sous seing privé (*“actes sous seing privé”*) (voir *Recueil Dalloz*, “Preuve”, n° 638).

[29] C’est la situation en France, par exemple (voir *Recueil Dalloz*, “Preuve”, n° 657-658).

[30] Les commentateurs du code de procédure civile allemand (*Zivilprozeßordnung – ZPO*) font observer que l’exigence d’une signature manuscrite reviendrait à exclure toutes les formes de signes obtenus mécaniquement, ce qui irait à l’encontre de la pratique ordinaire et du progrès technologique (voir Gerhard Lüke et Alfred Walchshöfer, *Münchener Kommentar zur Zivilprozessordnung* (Munich, Beck, 1992), § 416, n° 5).

[31] Par exemple, la France (voir *Recueil Dalloz*, “Preuve”, n° 662).

[32] En France, par exemple, la signature ne pouvait être remplacée par une croix ou d’autres signes, par un sceau ou des empreintes digitales (voir *Recueil Dalloz*, “Preuve”, n° 665).

(fonction d'attribution)[33]. On peut dire des signatures qu'elles remplissent diverses fonctions également, selon la nature du document qui a été signé. Par exemple, une signature pourrait témoigner de l'intention d'une partie d'être liée par la teneur d'un contrat signé; de l'intention d'une personne de revendiquer la paternité d'un texte (montrant ainsi qu'elle a conscience du fait que l'acte de signature peut avoir éventuellement des conséquences juridiques); de l'intention d'une personne de s'associer à la teneur d'un document rédigé par quelqu'un d'autre; et du fait que, et du moment où, une personne se trouvait en un lieu donné[34].

8. Il convient toutefois de noter que même si l'authenticité est souvent présumée par l'existence d'une signature, une signature à elle seule n'"authentifie" pas un document. Les deux éléments peuvent même être séparables, selon les circonstances. Une signature peut conserver son "authenticité" même si le document sur lequel elle est apposée est altéré par la suite. De la même façon, un document peut encore être "authentique" même si une signature qu'il contient a été contrefaite. Qui plus est, le pouvoir d'intervenir dans une opération et l'identité réelle de la personne en question, éléments pourtant importants pour assurer l'authenticité d'un document ou d'une signature, ne sont pas entièrement démontrés par la signature seule, et ne constituent pas non plus une garantie suffisante de l'authenticité des documents ou de la signature.

9. Cette observation débouche sur un autre aspect de la question examinée ici. Quelle que soit la tradition juridique, une signature, à très peu d'exceptions près, n'est pas autonome. Son effet juridique dépend du lien entre elle et la personne à laquelle elle est attribuable. Dans la pratique, diverses mesures peuvent être prises pour vérifier l'identité du signataire. Lorsque les parties sont toutes présentes au même endroit en même temps, elles peuvent simplement se reconnaître en se voyant; si elles négocient par téléphone, elles peuvent reconnaître leurs voix, etc. Ce sont là des situations courantes qui ne donnent pas lieu à des règles juridiques spécifiques. En revanche, lorsque les parties négocient par correspondance, ou lorsque des documents signés sont expédiés le long d'une chaîne de contrats, il est possible qu'il y ait peu de moyens d'établir que les signes apparaissant sur un document donné y ont bien été apposés par la personne au nom de laquelle ils semblent être liés et de déterminer si seule la personne dûment autorisée a effectivement été celle qui a produit la signature censée lier une personne particulière.

10. Bien qu'une signature manuelle soit une forme familière d'"authentification" et remplisse bien sa fonction pour des documents relatifs à des opérations transmis entre deux parties connues, dans de nombreuses situations commerciales et administratives, une signature est relativement peu sûre. Souvent, la personne qui se fie au document ne connaît pas les noms des personnes autorisées à signer et ne

---

[33] *Loi type de la CNUDCI sur les signatures électroniques et Guide pour son incorporation, 2001*, publication des Nations Unies, numéro de vente: F.02.V.8, deuxième partie, par. 29, disponible à http://www.uncitral.org/pdf/french/texts/electcom/ml-elecsign-f.pdf. Cette analyse avait déjà servi de base pour les critères de l'équivalence fonctionnelle à l'article 7 de la *Loi type de la CNUDCI sur le commerce électronique et Guide pour son incorporation*, *1996* avec article 5 *bis* tel qu'ajouté en 1998 (publication des Nations Unies, numéro de vente: F.99.V.4, disponible à http://www.uncitral.org/pdf/french/texts/electcom/ml-elecsign-f.pdf.

[34] Ibid.

dispose pas non plus de spécimens de signatures à des fins de comparaison[35]. Cela est particulièrement vrai pour de nombreux documents auxquels se fient des pays étrangers dans les opérations commerciales internationales. Même lorsqu'un spécimen de la signature autorisée est disponible à des fins de comparaison, seul un expert peut être capable de détecter un faux bien imité. Lorsque de très nombreux documents sont traités, les signatures, parfois, ne sont même pas comparées, sauf pour les opérations les plus importantes. La confiance est l'un des principaux piliers des relations d'affaires internationales.

11. La plupart des systèmes juridiques ont des procédures ou des exigences spéciales destinées à accroître la fiabilité des signatures manuscrites. Certaines procédures peuvent être impératives pour que certains documents produisent des effets juridiques. Elles peuvent aussi être facultatives et à la disposition des parties qui souhaitent agir de manière à éviter d'éventuelles controverses concernant l'authenticité de certains documents. On peut citer comme exemples typiques:

a) **La légalisation**. Dans certaines circonstances, l'acte de signature a une importance formelle particulière en raison de la confiance renforcée que l'on associe à une cérémonie spéciale. C'est le cas par exemple avec la légalisation, c'est-à-dire la certification par un notaire afin d'établir l'authenticité d'une signature sur un acte juridique;

b) **L'attestation** est l'acte qui consiste à assister à la signature d'un acte juridique puis à signer son propre nom comme témoin. Le but de l'attestation est de conserver la preuve de la signature. En attestant, le témoin déclare et confirme que la personne qu'il a regardée signer l'acte l'a effectivement signé. Attester ne signifie pas se porter garant de l'exactitude ou de la sincérité du document. Le témoin peut être appelé à déposer sur les circonstances entourant la signature[36];

c) **Les sceaux**. L'utilisation de sceaux, en plus ou à la place de signatures, n'est pas rare, en particulier dans certaines régions du monde[37]. La signature ou l'apposition d'un sceau peuvent par exemple prouver l'identité du signataire; que le signataire a accepté d'être lié par l'accord et qu'il l'a fait volontairement; que l'acte est définitif et complet; ou que les renseignements n'ont pas été modifiés après la signature[38]. Elle peut aussi mettre en garde le signataire et indiquer l'intention d'agir d'une manière juridiquement contraignante.

---

[35] Certains domaines du droit reconnaissent à la fois l'insécurité inhérente aux signatures manuscrites et l'impossibilité pratique d'insister sur des conditions de forme strictes pour la validité des actes juridiques, et admettent que dans certains cas même la falsification d'une signature ne priverait pas un document de son effet juridique. Ainsi, par exemple, l'article 7 de la loi uniforme sur les lettres de change et billets à ordre annexée à la Convention portant loi uniforme sur les lettres de change et billets à ordre, conclue à Genève le 7 juin 1930, dispose que "si la lettre de change porte des signatures de personnes incapables de s'obliger par lettre de change, des signatures fausses ou des signatures de personnes imaginaires, ou des signatures qui, pour toute autre raison, ne sauraient obliger les personnes qui ont signé la lettre de change, ou au nom desquelles elle a été signée, les obligations des autres signataires n'en sont pas moins valables." (*Recueil de traités de la Société des Nations,* vol. CXLIII, n° 3313).

[36] Adrian McCullagh, Peter Little et William Caelli, "Electronic signatures: understand the past to develop the future", *University of New South Wales Law Journal*, vol. 21, n° 2 (1998), voir en particulier la section III.D sur le concept de témoin.

[37] On utilise des sceaux dans plusieurs pays d'Asie orientale, comme la Chine et le Japon.

[38] Mark Sneddon, "Legislating to facilitate electronic signatures and records: exceptions, standards

12. En dehors de ces situations spéciales, les signatures manuscrites sont utilisées dans les opérations commerciales, nationales et internationales, depuis des siècles sans cadre législatif ou opérationnel particulier. Les destinataires ou les détenteurs des documents signés ont évalué la fiabilité des signatures au cas par cas en fonction du niveau de confiance dont jouit le signataire. En fait, dans leur grande majorité, les contrats internationaux écrits – si tant est qu'il y ait un "écrit"– ne donnent pas nécessairement lieu à des formalités ou à une procédure d'authentification spéciales.

13. L'utilisation transfrontalière de documents signés devient plus compliquée lorsque des autorités publiques interviennent, car les autorités destinataires dans un pays étranger ont généralement besoin de preuves de l'identité et du pouvoir du signataire. Ces exigences sont traditionnellement satisfaites par les procédures dites de "légalisation", où les signatures figurent dans des documents nationaux, authentifiés par les autorités diplomatiques pour être utilisés à l'étranger. Inversement, les représentants consulaires ou diplomatiques du pays dans lequel il est prévu d'utiliser les documents peuvent eux aussi authentifier les signatures d'autorités publiques étrangères dans le pays d'origine. Souvent, les autorités consulaires et diplomatiques n'authentifient que les signatures de certaines autorités de haut rang dans les pays émetteurs, ce qui demande par conséquent plusieurs niveaux de reconnaissance des signatures, lorsque le document a été délivré au départ par un agent de rang inférieur, ou bien la légalisation préalable des signatures par un notaire dans le pays émetteur. Dans la plupart des cas la légalisation est une procédure lourde, longue et coûteuse. C'est pourquoi a été négociée la Convention supprimant l'exigence de la légalisation des actes publics étrangers[39], conclue à La Haye le 5 octobre 1961, pour remplacer les exigences existantes par un formulaire simplifié et normalisé (l'"apostille"), qui est utilisé pour fournir une certification de certains actes publics dans les États Parties à la convention[40]. Seule une autorité compétente désignée par l'État dont émane l'acte public peut délivrer une apostille. Les apostilles attestent la véracité de la signature, la qualité en laquelle le signataire de l'acte a agi et, le cas échéant, l'identité du sceau ou timbre dont cet acte est revêtu, mais ne concernent pas la teneur de l'acte lui-même.

14. Comme il a été indiqué ci-dessus, dans de nombreux systèmes juridiques, il n'est pas toujours nécessaire que les contrats commerciaux figurent dans un document ou soient attestés par un écrit pour être valables. Même lorsqu'un écrit existe, une signature n'est pas nécessairement impérative pour que le contrat soit contraignant pour les parties. Naturellement, lorsque la loi exige qu'un contrat soit écrit et signé, le non-respect de ces conditions l'invaliderait. Les conditions de forme à des fins de preuve sont peut-être plus importantes que les conditions de forme à des fins de validité des contrats. La difficulté de prouver les conventions

---

and the impact of the statute book", *University of New South Wales Law Journal*, vol. 21, n° 2 (1998), voir en particulier la deuxième partie, chapitre II sur les objectifs de l'écrit et les prescriptions relatives à la signature.

[39] Nations Unies, *Recueil des* Traités, vol. 527, n° 7625. Voir l'espace apostille sur le site Web de la Conférence de La Haye de droit international privé (http://hcch.e-vision.nl/index_en.php?act=text.display&tid=37, 7 février 2007).

[40] Ces actes comprennent: les documents qui émanent d'une autorité ou d'un fonctionnaire relevant d'une juridiction de l'État (y compris ceux qui émanent d'un tribunal administratif, constitutionnel ou ecclésiastique, du ministère public, d'un greffier ou d'un huissier de justice); les documents administratifs; les actes notariés; et les déclarations officielles apposées sur un acte sous seing privé.

verbales est une des principales raisons pour lesquelles les contrats commerciaux sont reproduits dans des documents écrits ou documentés par correspondance, même si une convention verbale serait autrement valable. Les parties dont les obligations sont documentées dans des écrits signés ont peu de chances de réussir dans les tentatives de contester la teneur de leurs obligations. Des règles strictes sur les preuves documentaires visent généralement à accorder un degré élevé de fiabilité aux documents qui y satisfont, ce qui, estime-t-on généralement, accroît la sécurité juridique. En même temps, cependant, plus les conditions en matière de preuve sont élaborées, plus grande est la possibilité pour une partie d'invoquer des vices de forme pour invalider ou refuser la force exécutoire d'obligations qu'elle n'a plus l'intention d'exécuter, par exemple parce que le contrat est devenu commercialement désavantageux. Il faut donc trouver un équilibre entre l'intérêt de promouvoir la sécurité dans l'échange de communications électroniques et le risque de donner un moyen facile aux négociants de mauvaise foi de refuser d'honorer leurs obligations juridiques librement assumées. Y parvenir par des règles et des normes internationalement reconnues et applicables dans différents pays est une tâche importante pour les décideurs dans le domaine du commerce électronique. L'objet du présent rapport est d'aider les législateurs et les décideurs à identifier les principales questions juridiques en cause dans l'utilisation internationale de méthodes d'authentification et de signature électroniques et d'envisager des solutions possibles.

Première partie

Méthodes de signature et d'authentification électroniques

I. Définition et méthodes de signature et d'authentification électroniques

A. Remarques générales sur la terminologie

15. Les termes "authentification électronique" ou "signature électronique" désignent diverses techniques actuellement disponibles sur le marché ou encore en développement pour reproduire dans un environnement électronique certaines ou la totalité des fonctions identifiées comme caractéristiques des signatures manuscrites ou d'autres méthodes traditionnelles d'authentification.

16. Diverses méthodes de signature électronique ont été mises au point au fil des années. Chacune vise à satisfaire des besoins différents et à conférer des niveaux de sécurité différents, et donne lieu à des exigences techniques différentes. Les méthodes d'authentification et de signature électroniques peuvent être classées en trois catégories: celles qui sont fondées sur la connaissance de l'utilisateur ou du destinataire (par exemple mot de passe, numéro d'identification personnel), celles qui sont fondées sur les caractéristiques physiques de l'utilisateur (par exemple la biométrie) et celles qui sont fondées sur la possession d'un objet par l'utilisateur (par exemple codes ou autres renseignements stockés sur une carte magnétique)[41]. On pourrait envisager une quatrième catégorie, comprenant divers types de méthodes qui, sans ressortir à l'une quelconque des catégories précédentes, pourrait aussi être utilisée pour indiquer l'auteur d'une communication électronique (comme le fac-similé d'une signature manuscrite, ou un nom dactylographié au bas d'un message électronique). Les technologies actuellement utilisées comprennent: les signatures numériques dans le cadre d'une infrastructure à clef publique (PKI), les dispositifs biométriques, les numéros d'identification personnels (PIN), les mots de passe définis par l'utilisateur ou attribués, les signatures manuscrites scannées, la signature au moyen d'un stylo numérique, et le fait de cliquer sur une case "valider"[42]. Des solutions hybrides, fondées sur la combinaison de différentes technologies, se répandent de plus en plus, comme c'est le cas par exemple de l'utilisation combinée de mots de passe et des protocoles TLS/SSL (transport layer security/secure socket layer), qui est une technologie mêlant chiffrement à clef publique et à clef symétrique. Les caractéristiques des principales techniques actuellement en usage sont décrites ci-dessous (voir par. [...] à [...]).

---

[41] Voir le Rapport du Groupe de travail sur le commerce électronique sur les travaux de sa trente-deuxième session, tenue à Vienne du 19 au 30 janvier 1998 (A/CN.9/446), par. 91 sq, disponible à http://www.uncitral.org/uncitral/fr/commission/working_groups/4Electronic_Commerce.html.

[42] *Loi type de la CNUDCI sur les signatures électroniques et Guide pour son incorporation*, *2001*, (voir note [33]), deuxième partie, par. 33.

17. Comme c'est souvent le cas, la technologie s'est développée bien avant que la loi s'intéresse au sujet. Il en résulte un écart, qui entraîne non seulement des niveaux variables de connaissance des experts, mais aussi des incohérences sur le plan de la terminologie. Des expressions qui étaient traditionnellement employées avec une connotation particulière dans les droits nationaux ont commencé à être utilisées pour décrire des techniques électroniques dont la fonctionnalité ne coïncidait pas nécessairement avec les fonctions ou caractéristiques du concept correspondant dans l'usage juridique. Comme on l'a vu ci-dessus (voir par. [...] à [...]), les notions d'"authentification", d'"authenticité", de "signature" et d'"identité", bien qu'elles soient étroitement liées dans certains contextes, ne sont pas identiques ou interchangeables. L'usage dans le secteur de la technologie de l'information, qui s'est constitué pour l'essentiel autour des considérations de sécurité des réseaux, n'applique cependant pas nécessairement les mêmes catégories que les écrits juridiques.

18. Dans certains cas, l'expression "authentification électronique" désigne des techniques qui, selon le contexte dans lequel elles sont utilisées, peuvent comporter divers éléments, tels que l'identification d'individus, la confirmation du pouvoir d'une personne (généralement d'agir au nom d'une autre personne ou entité) ou des prérogatives (par exemple, l'appartenance à une institution, l'abonnement à un service) ou l'assurance de l'intégrité de l'information. Dans d'autres cas, l'accent est mis sur la seule identité[43], mais il s'étend parfois au pouvoir[44], ou à une combinaison de plusieurs de ces éléments[45].

19. Ni la Loi type de la CNUDCI sur le commerce électronique[46], ni la Loi type de la CNUDCI sur les signatures électroniques[47] n'emploie le terme

---

[43] L'Administration de la technologie du Département du commerce des États-Unis, par exemple, définit l'authentification électronique comme "le processus consistant à établir la confiance dans les identités des utilisateurs présentées dans un système d'information" (Département du commerce des États-Unis, *Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology,* NIST Special Publication 800-63, version 1.0.2 (Gaithersburg, Maryland, avril 2006)), disponible à http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf, visité le 4 avril 2007).

[44] Par exemple, le gouvernement australien a mis au point un cadre d'authentification électronique qui définit celle-ci comme "le processus consistant à établir un niveau de confiance sur le point de savoir si une déclaration est sincère ou valide lors d'une transaction s'effectuant en ligne ou par téléphone. Il aide à renforcer la confiance dans une transaction en ligne en donnant aux parties concernées une certaine assurance que leurs rapports sont légitimes. Ces déclarations peuvent comprendre: des détails sur l'identité; les qualifications professionnelles, ou le pouvoir délégué de mener la transaction" (Australie, Department of Finance and Administration, *Australian Government e-Authentication Framework: An Overview* (Commonwealth of Australia, 2005), disponible à (http://www.agimo.gov.au/infrastructure/authentication/agaf_b/overview/introduction#e-authentication, visité le 4 avril 2007).

[45] Les Principes d'authentification électroniques élaborés par le gouvernement du Canada, par exemple, définissent l'"authentification" comme un "processus qui atteste des attributs des parties prenantes à une communication électronique ou de l'intégrité de la communication". Le terme "attributs" à son tour est défini comme une "information concernant l'identité, les privilèges ou les droits d'une partie prenante ou d'une autre entité identifiée." (Canada, Industrie Canada, *Principes d'authentification électronique – Cadre canadien*, mai 2004, http://strategis.ic.gc.ca/epic/site/ecic-ceac.nsf/fr/gv00242f.html, consulté le 4 avril 2007).

[46] *Loi type de la CNUDCI sur le commerce électronique et Guide pour son incorporation* (voir note [33]).

[47] *Loi type de la CNUDCI sur les signatures électroniques* (voir note [33]).

d'"authentification électronique", en raison du sens différent du mot "authentification" dans divers systèmes juridiques et de la confusion possible avec des procédures ou des exigences de forme particulières (voir par. [...] à [...] ci-dessus). La Loi type sur le commerce électronique utilise à la place la notion de "forme originale" comme critère de l'équivalence fonctionnelle de l'information électronique "authentique". D'après son article 8, lorsque la loi exige qu'une information soit présentée ou conservée sous sa forme originale, un message de données satisfait à cette exigence:

a) S'il existe "une garantie fiable quant à l'intégrité de l'information à compter du moment où elle a été créée pour la première fois sous sa forme définitive en tant que message de données ou autre"; et

b) Si, lorsqu'il est exigé qu'une information soit présentée, cette information "peut être montrée à la personne à laquelle elle doit être présentée".

20. En conformité avec la distinction faite dans la plupart des systèmes juridiques entre signature (ou sceaux, lorsqu'ils sont utilisés à la place) comme moyen d'"authentification", d'une part, et "authenticité" en tant que qualité d'un document ou enregistrement, d'autre part, les deux lois types complètent la notion d'"originalité" par celle de "signature". L'alinéa a) de l'article 2 de la Loi type de la CNUDCI sur les signatures électroniques définit la signature électronique comme: des données sous forme électronique contenues dans un message de données ou jointes ou logiquement associées audit message, pouvant être utilisées pour "identifier le signataire" dans le cadre du message de données et "indiquer qu'il approuve l'information qui y est contenue".

21. La définition de "signature électronique" dans les textes de la CNUDCI est délibérément large, de manière à englober toutes les méthodes de "signature électronique" existantes et futures. Tant que la fiabilité des méthodes utilisées est "suffisante au regard de l'objet pour lequel le message de données a été créé ou communiqué, compte tenu de toutes les circonstances, y compris de tout accord en la matière"[48], elles devraient être considérées comme satisfaisant aux prescriptions légales en matière de signature. Les textes de la CNUDCI relatifs au commerce électronique, ainsi que beaucoup d'autres textes législatifs, reposent sur le principe de la neutralité technologique et visent par conséquent à prendre en compte toutes les formes de signature électronique. Ainsi, la définition de signature électronique de la CNUDCI couvrirait l'ensemble des techniques de "signature électronique", de la sécurité de haut niveau, telle que les systèmes de garantie de la signature fondés sur la cryptographie associés à une infrastructure à clef publique (forme courante de "signature numérique"(voir par. [...] à [...]) aux niveaux inférieurs, tels que les codes ou mots de passe non chiffrés. La simple dactylographie du nom de l'auteur à la fin d'un message électronique, qui est la forme la plus courante de "signature" électronique, par exemple, remplirait la fonction consistant à identifier correctement l'auteur du message toutes les fois qu'il n'est pas déraisonnable d'appliquer un niveau de sécurité aussi bas.

22. Les lois types de la CNUDCI n'abordent pas autrement les questions liées au contrôle de l'accès ou à la vérification de l'identité. Cela tient aussi au fait que, dans

---

[48] *Loi type de la CNUDCI sur le commerce électronique et Guide pour son incorporation* (voir note [33]), art. 7, par. 1 b).

un environnement papier, si les signatures peuvent être des signes de l'identité, elles sont nécessairement attributives de l'identité (voir par. [...] à [...]). La Loi type de la CNUDCI sur le commerce électronique traite toutefois des conditions dans lesquelles le destinataire d'un message de données est fondé à supposer que le message émanait effectivement de son expéditeur présumé. De fait, son article 13 indique qu'en ce qui concerne la relation entre l'expéditeur et le destinataire, un message de données est réputé émaner de l'expéditeur s'il a été envoyé: par une personne "autorisée à agir à cet effet au nom de l'expéditeur"; ou par un "système d'information programmé par l'expéditeur ou en son nom pour fonctionner automatiquement". S'agissant du destinataire, il est fondé à considérer qu'un message de données émane de l'expéditeur et à agir en conséquence a) si, pour s'assurer que le message de données émanait de l'expéditeur, il a "correctement appliqué une procédure que l'expéditeur avait précédemment acceptée à cette fin"; ou b) si le message de données tel qu'il l'a reçu résulte des actes d'une personne qui, de par ses relations avec l'expéditeur ou un agent de celui-ci, a eu accès à une méthode que l'expéditeur utilise pour identifier comme étant de lui les messages de données. Dans l'ensemble, ces règles permettent à une partie de déduire l'identité de quelqu'un d'autre, que le message ait été ou non "signé" électroniquement et que la méthode utilisée pour l'attribuer à l'expéditeur ait été ou non utilisée valablement à des fins de "signature". Cela est conforme à la pratique actuelle dans l'environnement papier. Vérifier la voix, l'apparence physique ou les papiers d'identité (par exemple un passeport national) d'une personne peut suffire pour conclure que cette personne est celle qu'elle prétend être aux fins de communication, mais ne tiendrait pas lieu de "signature" de cette personne dans la plupart des systèmes juridiques.

23. Outre la confusion due au fait que l'usage technique et juridique des termes dans l'environnement papier et dans l'environnement électronique ne coïncident pas, les diverses techniques mentionnées précédemment (voir ci-dessus, par. 16 et l'analyse plus détaillée dans les par. [...] à [...] ci-dessous) peuvent être utilisées à des fins différentes et fournir une fonctionnalité différente, selon le contexte. Des mots de passe ou des codes, par exemple, peuvent être utilisés pour "signer" un document électronique, mais aussi pour accéder à un réseau, à une base de données ou à un autre service électronique, de la même façon qu'une clef peut servir à déverrouiller un coffre ou à ouvrir une porte. Toutefois, alors que dans le premier cas le mot de passe est une preuve d'*identité*, dans le second c'est un *pouvoir*, qui, bien que lié d'ordinaire à une personne particulière, peut également être transféré à une autre. Dans le cas des signatures numériques, l'inadéquation de la terminologie actuelle est encore plus patente. La signature numérique est largement considérée comme une technologie particulière pour "signer" des documents électroniques. Il n'est toutefois pas du tout certain que l'on puisse, d'un point de vue juridique, dire de l'application de la cryptographie asymétrique à des fins d'authentification qu'elle est une "signature" numérique, car ses fonctions vont au-delà des fonctions typiques d'une signature manuscrite. La signature numérique offre le moyen à la fois de "vérifier l'authenticité de messages électroniques" et de "garantir l'intégrité du contenu"[49]. En outre, la technologie de la signature numérique "n'établit pas

[49] Babette Aalberts et Simone van der Hof, *Digital Signature Blindness: Analysis of Legislative Approaches to Electronic Authentication*, novembre 1999 (http://rechten.uvt.nl/simone/Digsigbl.pdf, consulté le 4 avril 2007), p. 8.

simplement l'origine ou l'intégrité pour ce qui est des individus, comme cela est exigé à des fins de signature, mais elle peut aussi authentifier, par exemple, des serveurs, des sites Web, des logiciels informatiques, ou toutes autres données distribuées ou stockées numériquement", ce qui confère aux signatures numériques "une utilisation beaucoup plus vaste qu'un substitut électronique à des signatures manuscrites[50].

---

[50] Ibid.