Institutional Repository - Research Portal
Dépôt Institutionnel - Portail de la Recherche
researchportal.unamur.be
University of Namur

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

# Pistes de réflexion pour une législation relative à la signature digitale et au régime des autorités de certification

Gobert, Didier; Antoine, Mireille

*Published in:*
Revue Générale de Droit Civil Belge = Tijdschrift voor Belgisch Burgerlijk Recht

*Publication date:*
1998

*Document Version*
le PDF de l'éditeur

Link to publication

*Citation for pulished version (HARVARD):*
Gobert, D & Antoine, M 1998, 'Pistes de réflexion pour une législation relative à la signature digitale et au régime des autorités de certification', *Revue Générale de Droit Civil Belge = Tijdschrift voor Belgisch Burgerlijk Recht*, numéro 4-5, pp. 285-310.

**General rights**
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

**Take down policy**
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 04. May. 2026

# Pistes de réflexion pour une législation relative à la signature digitale et au régime des autorités de certification

**Mireille Antoine et Didier Gobert**

(publié dans la *Revue Générale de Droit Civil*, septembre 1998, n° 4, pp.285 à 310.)

Constatant l'absence néfaste de réglementation juridique en matière de signatures digitales et d'autorité de certification, le Conseil des Ministres a adopté le 30 mai 1997 une note préconisant la création d'un cadre juridique pour l'emploi de telles signatures[1]. Cette décision résulte notamment de la prise de conscience que l'absence de cadre juridique constitue un frein important au développement de services électroniques et une menace pour le consommateur. Une non-intervention mènerait à une prolifération incontrôlée de systèmes de signature ainsi qu'à des incompatibilités découlant d'initiatives divergentes prises tant dans le secteur privé que public en vue de permettre l'emploi d'une signature digitale dans des applications précises. En outre, l'adoption de cette note par le Conseil des Ministres a également été favorisée par les résultats des travaux réalisés au niveau des instances internationales ainsi que par les initiatives prises par d'autres pays en la matière.

Au niveau international, la CNUDCI (Commission des Nations Unies pour le Droit Commercial International) examine actuellement, au sein de son groupe de travail sur le commerce électronique, les questions juridiques relatives à la signature électronique. Celles-ci devraient déboucher sur l'élaboration de règles uniformes relatives aux signatures numériques[2]. De même, la Commission européenne insiste sur l'importance d'un cadre réglementaire favorable au développement du commerce électronique[3] ainsi qu'à la signature numérique et au chiffrement[4].

Au niveau national, certains Etats des Etats-Unis[5] ainsi que l'Allemagne[6] et l'Italie[7] ont adopté une législation relative à la signature digitale et aux autorités de certification. Par

[1] Pour un extrait de cette note, voy. J. DUMORTIER et P. VAN EECKE, « Naar een juridische regeling van de digitale handtekening in België », *Computerrecht*, 1997/4, pp. 154-159.

[2] Voir par exemple Commission des Nations Unies pour le Droit Commercial International, Rapport du groupe de travail sur le commerce électronique sur les travaux de sa trente et unième session (New York, 18-28 février 1997), A/CN.9/437, 12 mars 1997 ; Commission des Nations Unies pour le Droit Commercial International, Rapport du groupe de travail sur le commerce électronique sur les travaux de sa trente et unième session (New York, 1er-12 juin 1998), A/CN.9/446, 10 février 1998.

[3] COM(97)157 : Vers une initiative européenne en matière de commerce électronique, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des Régions, 15 avril 1997, §36.

[4] COM(97)503 : Vers un Cadre Européen pour les Signatures Numériques et le Chiffrement : Assurer la sécurité et la confiance dans la communication électronique, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des Régions, 8 octobre 1997 ; Proposition de directive du Parlement européen et du Conseil sur un cadre commun pour les signatures électroniques, COM (98)297 final, 13 mai 1998.

[5] A titre d'exemple : Utah Digital Signature Act, Utah Code Annotated, titre 46, chapitre 3, 1996, http://www.commerce.state.ut.us/web/commerce/digsig/act.htm ; Floride, Electronis Signature Act of 1996 (General Bill S942), enacted May 25, 1996, http://www.scri.fsu.edu/fla-leg/bills/senate-1996/sb0942.html ; Final draft of California Proposed Digital Signature Regulations , http://www.ss.ca.gov/digsig/finalregs.htm .

[6] Loi allemande sur le multimédia du 13 juin 1997, article 3 (sur la signature digitale), Journal officiel allemand du 22 juillet 1997 (BGBl, IS, 1870), entrée en vigueur le 1er août 1997.

[7] Décret présidentiel italien du 10 novembre 1997, n° 513 on « Regulations establishing criteria and means for implementing Section 15 (2) of Law N° 59 of 15 March 1997 concerning the creation, storage and

ailleurs, des textes sont en préparation dans la plupart des autres Etats membres de l'Union européenne. Face à une telle évolution, la Belgique ne pouvait évidemment rester muette.

Dès lors que la décision d'intervenir sur le plan légal a été prise, on peut s'interroger sur les orientations que pourraient prendre les textes législatifs et sur le contenu de ceux-ci. Cet article tente de présenter quelques pistes d'orientation afin de soutenir le législateur dans sa réflexion. Nous analyserons, dans un premier temps, les problèmes de preuve que pose l'utilisation de la signature digitale ainsi que les solutions envisageables. Dans un second temps, nous tenterons de mettre en exergue un ensemble d'impératifs qui sont relatifs aux activités des autorités de certification et qui mériteraient une attention particulière du législateur.

# 1ère partie : La signature digitale

## Introduction

La signature digitale[8], que l'on pourrait définir comme le résultat d'une transformation cryptographique, basée sur la cryptographie asymétrique, d'un ensemble de données digitales qui permet de vérifier l'identité de l'auteur des données ainsi que l'intégrité de celles-ci, ne constitue qu'un mécanisme particulier de signature électronique. En effet, la notion de signature électronique ne se réfère pas à un mécanisme de signature unique. Celle-ci regroupe différentes technologies (code secret, techniques basées sur la cryptographie symétrique ou asymétrique, signature biométrique,…)[9] qui méritent l'appellation de signature électronique dans la mesure où elles permettent la réalisation par voie électronique des fonctions de la signature classique, à savoir, l'identification du signataire et l'expression de sa volonté d'adhérer au message signé.

Bien que le concept de signature électronique se présente comme un terme générique englobant un ensemble de mécanismes techniques[10], nous nous limiterons à traiter ici de la signature digitale. Et cela, pour deux raisons : d'une part, cette technologie est devenue un standard *de facto* en matière de commerce électronique car elle constitue la technique la plus mûre et qui présente le plus haut degré de sécurité pour les échanges de données en réseau ouvert[11] et, d'autre part, l'intervention d'autorités de certification[12] ne s'effectue actuellement que dans le cadre de l'utilisation de la signature digitale.

## Chapitre 1er. La signature électronique et le droit de la preuve

transmission of documents by means of computer-based or telematic systems », publiée in Gazzetta Ufficiale, 13 mars 1998, n° 60.

[8] La littérature utilise également le terme signature numérique, E.A. CAPRIOLI, « Sécurité et confiance dans le commerce électronique : Signature numérique et autorité de certification », *La Semaine Juridique Edition Générale*, avril 1998, n°14, p.587 ; P. TRUDEL et S. PARISIEN, *L'identification et la certification dans le commerce électronique*, Québec, Les éditions Yvon Blais Inc., 1996, p. 96.

[9] E.A. CAPRIOLI, *op.cit.*, p.587.

[10] Le projet de loi californien adopte par exemple une approche ouverte de la notion de signature, Final draft of California Proposed Digital Signature Regulations, *op.cit.* .

[11] P. TRUDEL et S. PARISIEN, *op.cit.*, p. 96.

[12] Voir *infra* 2ème partie, les autorités de certification.

Le problème de la recevabilité des preuves électroniques en droit a déjà fait couler beaucoup d'encre. Nous renvoyons donc le lecteur aux nombreux articles sur ce sujet[13]. Rappelons simplement que la partie qui veut faire la preuve d'un acte juridique en matière civile [14], dont la somme dépasse 15.000 francs, doit tenir compte de l'article 1341 du Code civil qui exige que la preuve soit apportée par un écrit signé[15]. Notons toutefois que le législateur n'a donné de définition ni de l'écrit ni de la signature[16]. La jurisprudence[17] et une partie de la doctrine[18] ont pallié cette carence en envisageant (malheureusement) l'écrit comme un écrit sur support papier et en définissant la signature comme le signe par lequel une personne se présente habituellement à l'égard des tiers, accompagné d'un certain graphisme, qui est apposé de manière manuscrite sur un écrit papier. Eu égard à ces exigences, on comprend que, sur le plan probatoire, les utilisateurs de nouvelles technologies ne puissent raisonnablement se fier à un document signé électroniquement.

Une telle conception est contestable et incompatible avec l'utilisation sans cesse croissante des nouvelles technologies et le développement de la société de l'information[19]. C'est la raison pour laquelle le Conseil des Ministres[20] a décidé de préparer un projet de loi adaptant les règles du Code civil en matière de preuve aux technologies de l'informatique et des télécommunications.

---

[13] B. AMORY et Y. POULLET, « Le droit de la preuve face à l'informatique et à la télématique : approche de droit comparé », *D.I.T.*, 1985, pp. 11 et s. ; M. ANTOINE, J.-F. BRAKELAND et M. ELOY, *Le droit de la preuve face aux nouvelles technologies de l'information et de la communication*, Cahier du C.R.I.D., n° 7, Bruxelles, Story Scientia,1991, pp. 38 et s. ; G.L. BALLON, « Het bewijs en de moderne technieken », *Computerrecht*, 1990/5, pp.228 à 244 ; E. DAVIO, « Preuve et certification sur Internet », *R.D.C.*, 1997, n°11, pp.660 à 670 ; M. FONTAINE, "La preuve des actes juridiques et les techniques nouvelles", in *La preuve*, Colloque U.C.L., 1987 ; J. LARRIEU, « Les nouveaux moyens de preuve : pour ou contre l'identification des documents informatiques à des écrits sous seing privé », *Cahiers Lamy Droit de l'informatique*, 1988, H/88, p.8 et I/88, p.26 ; Y. POULLET, « Les transactions commerciales et industrielles par voie électronique. De quelques réflexions autour du droit de la preuve », in *Le droit des affaires en évolutions, Le juriste face à l'invasion informatique*, Colloque ABJE, 24 oct. 1996, Bruxelles, Bruylant, Anvers, Kluwer, 1996, pp.39 à 67; D. SYX, « Vers de nouvelles formes de signature ? », *Droit de l'inf.*, 1986/3, pp.133 et s. ; N. VERHEYDEN-JEANMART, *Droit de la preuve*, Précis de la Faculté de Droit de l'Université Catholique de Louvain, Bruxelles, Larcier, 1991, pp. 234 et s. .

[14] En matière commerciale, le principe de la libre admissibilité des modes de preuve autorise l'utilisation des techniques d'authentification en vue d'apporter la preuve de l'existence, du contenu d'un acte juridique, ainsi que de son adhésion par le signataire. Toutefois, quand bien même un document informatique peut être considéré comme recevable en matière commerciale, le juge dispose d'un pouvoir d'appréciation afin d'en apprécier la force de conviction ou "valeur probante".

[15] Si le montant n'excède pas 15.000 francs, la preuve est libre.

[16] La loi comme telle n'exclut donc pas la signature électronique. X. Thunis en conclut même que la « notion d'écrit signé peut s'interpréter assez largement étant donné l'imprécision ou l'ouverture providentielle des concepts fondamentaux, écrit et signature », X. THUNIS, *Responsabilité du banquier et automatisation des paiements*, Travaux de la Faculté de droit de Namur, P.U.N., 1996, p. 228 et les références citées aux notes 67 et 68.

[17] Cass., 24 févr. et 3 nov. 1910, *Pas.*, 1910, I, pp.241 et 475 ; Cass., 1er mars 1917, *Pas.*, 1917, I, p.118 ; Cass., 7 janv. 1955, *Pas.*, 1955, I, p.456 ; Cass., 2 oct. 1964, *Pas.*, 1965, I, p.106.

[18] Voir par exemple E. Dubuisson qui considère que la signature numérique ne constitue pas l'équivalent de la signature manuscrite, E. DUBUISSON, « La personne virtuelle : proposition pour définir l'être juridique de l'individu dans un échange télématique », *D.I.T.*, 1995/3, p.8.

[19] Le problème se pose essentiellement dans les réseaux ouverts. Dans les réseaux fermés, les conventions relatives à la preuve ont ouvert une voie intéressante, s'agissant des nouvelles technologies : la rédaction de conventions permettait aux parties d'aménager leur propre régime probatoire. Toutefois, avec le développement de réseaux ouverts, la conclusion de conventions, préalables aux échanges, devient difficilement envisageable puisqu'elle suppose la rédaction d'un écrit établi selon les règles de l'article 1341 du Code civil.

[20] J. DUMORTIER et P. VAN EECKE, *op.cit.*, pp.154 à 159.

Différentes alternatives s'offrent au législateur pour admettre la signature électronique[21].

**1. Suppression du régime de la preuve réglementée.** En libéralisant le régime de la preuve, la loi n'exigerait plus qu'un acte juridique supérieur à 15.000 francs soit prouvé par un écrit signé. Tout document signé électroniquement deviendrait dès lors recevable.

Adopter une telle alternative est insatisfaisant pour deux raisons essentielles[22]. D'une part, cette solution modifierait profondément le système juridique belge et viendrait ainsi bouleverser l'équilibre des intérêts que le régime de la preuve réglementée entendait assurer. D'autre part, cette solution n'enlèverait rien au pouvoir discrétionnaire du juge dans l'appréciation de la valeur probante du mode de preuve, sachant que la jurisprudence reste attachée à la conception formelle de la signature[23].

**2. Elévation du seuil en deçà duquel la preuve est libre.** Rehausser la limite fixée à l'article 1341 du Code civil permettrait d'augmenter le nombre d'actes juridiques qui peuvent être prouvés librement. En deçà du montant fixé par la loi, un document signé électroniquement serait recevable par le juge.

Une telle solution est inopportune car elle maintient la suprématie de l'écrit papier signé manuscritement et n'apporte aucun élément de réponse quant à la valeur probante qu'il convient d'accorder aux documents signés électroniquement.

**3. Légitimation de la preuve électronique par le biais d'exceptions.** Cette solution consisterait à étendre le champ d'application de l'article 1347 (commencement de preuve par écrit) ou 1348 (impossibilité de se procurer une preuve écrite) du Code civil[24]. Or, le commencement de preuve par écrit[25] présuppose l'existence d'un écrit[26] (article 1347 du Code civil), ce qui, selon la conception actuelle, fait défaut lorsqu'il est fait usage des nouvelles technologies et l'impossibilité de se procurer un écrit ne doit, quant à elle, pas être volontaire[27]. En effet, la jurisprudence exige une véritable impossibilité et non de simples difficultés[28].

---

[21] Voir notamment *Les défis de la société de l'information et les missions de la Justice, Partie II : Le droit de la preuve face aux nouvelles technologies*, K.U.Leuven, ICRI, Janvier 1997.

[22] Voir à ce sujet J. Larrieu, *op.cit.*, p.9 qui critique également cette solution.

[23] Cass., 24 févr. et 3 nov. 1910, *Pas.*, 1910, I, pp.241 et 475 ; Cass., 1er mars 1917, *Pas.*, 1917, I, p.118 ; Cass., 7 janv. 1955, *Pas.*, 1955, I, p.456 ; Cass., 2 oct. 1964, *Pas.*, 1965, I, p.106.

[24] Pour un examen détaillé de la question, M. FONTAINE, *op.cit.*, p.18 et s. ; J.F. LECLERCQ, « Essai de solution d'une adaptation du régime des preuves en droit privé », in *Unité et diversité du droit privé*, Bruxelles, ULB, 1983, p.350 et s. ; D. SYX, *Aspects juridiques du mouvement électronique de fonds*, K.B., 1982, p.79 ; N. VERHEYDEN-JEANMART, *op.cit.*, p.174 et s. .

[25] Voir à ce sujet C. GOUX, note sous Liège, 25 février 1997, *R.R.D.*, 1997, p.204 et s.

[26] L'écrit dont il est question à l'article 1347 du Code civil ne présente pas les conditions requises pour être un acte probatoire complet mais répond à certaines caractéristiques propres quant à :

- sa forme : est considéré comme écrit "tout ce qui émane, sous une forme littérale quelconque, de la partie à qui on l'oppose" (Cass. 21 oct. 1891, *Pas.*, 1892, I, p. 58).
- son origine : un écrit émane d'une personne s'il est écrit ou signé de sa main (Cass. civ., 27 janv. 1971, *Bull. civ.*, 1971, I, n°34) ou si elle se l'est approprié "par une acceptation expresse ou tacite" (Cass. req., 8 août 1860, *D.S.*, 1860, 497.
- son contenu : l'écrit doit rendre vraisemblable le fait allégué. Cette vraisemblance est une question de fait souverainement appréciée par le juge du fond (Cass. 21 oct. 1891, *Pas.*, 1892, I, p. 58 ; Cass. 7 oct. 1895, *Pas.*, 1895, I, p. 284.

[27] L'impossibilité peut être matérielle, morale ou résulter d'un usage bien établi (H. DE PAGE, *Traité élémentaire de droit civil belge*, t. 3, Bruxelles, Bruylant, n° 901).

[28] Voir à ce sujet P. WERY, note sous Liège, 10 mars 1994, *J.M.L.B.*, 1994, p. 894 et s.

Agir par le biais d'exceptions est intellectuellement peu satisfaisant[29] et risquerait d'aboutir à un renversement de la règle (article 1341 : prééminence de l'écrit) et des exceptions (articles 1347 et 1348), avec l'augmentation prévisible du nombre d'actes juridiques passés électroniquement.

**4. Adoption d'une approche ouverte et fonctionnelle des concepts du Code civil.** La doctrine est unanime pour reconnaître à la signature la double fonction d'identification du signataire et de manifestation de volonté de ce dernier de s'approprier[30] le contenu de l'acte auquel la signature se réfère[31]. Par ailleurs, la signature manuscrite combinée à l'écrit papier permet d'assurer l'intégrité du contenu[32].

Au regard des développements techniques récents, il apparaît que les qualités fonctionnelles de la signature peuvent être satisfaites par diverses méthodes d'authentification utilisées dans le cadre d'échanges de données informatisées[33]. Concrètement, il conviendrait donc d'inscrire dans la loi une définition fonctionnelle[34] de la signature en veillant à ce que ne puissent être admises sur cette base que les signatures électroniques issues de procédés qui assurent de façon fiable[35] les fonctions de la signature. La définition adoptée devrait être ouverte afin de

---

[29] Pour une critique du recours aux exceptions, M. FONTAINE, *op.cit.*, p.40.

[30] Parlant de signature, cet élément intentionnel, l'*animus signandi*, est le plus décisif. C'est lui qui permet de distinguer les méthodes d'identification des procédés de signature. D. SYX, "Naar nieuwe vormen van handtekening", *Computerrecht*, 1986/3, p. 155 ; M. VAN QUICKENBORNE, "Quelques réflexions sur la signature des actes sous seing privé", note sous Cass. 28 juin 1982, *R.C.J.B.*, 1985, p. 69.

[31] Voir notamment : H. DE PAGE, *Traité élémentaire de droit civil belge*, Tome III, 3 ° édition, Bruxelles, Bruylant, 1967, n° 744, 777B, 778-787 ; M. FONTAINE, *op.cit.*, p. 11 ; F. LAURENT, *Principes de droit civil*, Tome XIX, 3° édition, 1878, n° 196-206 ; D. SYX, *op.cit.*, p.134 ; M. VAN QUICKENBORNE, *op. cit.*, p. 69 ; N. VERHEYDEN-JEANMART, *op.cit.*, p. 234 ; W. WILMS, "Van handtekening naar elektronische notaris - de validering van electronische communicatie", *R.W.*, 1995-1996, p. 839. Voir également à ce propos l'article 7 de la Loi type de la CNUDCI sur le commerce électronique qui dispose que, lorsque la loi exige une signature, cette exigence est satisfaite dans le cas d'un message de données "a) Si une méthode est utilisée pour identifier la personne en question et pour indiquer qu'elle approuve l'information contenue dans le message de données; et b) Si la fiabilité de cette méthode 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." (Guide pour l'incorporation dans le droit interne de la Loi type de la CNUDCI sur le commerce électronique (1996)).

[32] En effet, on constate que la fonction d'intégrité est remplie par le support papier, et dans une certaine mesure par la signature manuscrite qui, apposée au bas du document, permet d'éviter toute ajoute non autorisée au texte.

[33] Pour une synthèse du débat, X. THUNIS, « Responsabilité du banquier et automatisation des instruments de paiements », in *Droit de l'informatique : enjeux-nouvelles responsabilités*, Ed. du Jeune Barreau de Bruxelles, 1993, p.348 et s. .

[34] Certains auteurs avaient déjà plaidé en ce sens : M. ANTOINE, J.-F. BRAKELAND et M. ELOY, *op.cit.*, pp. 211 et s. . Pour une interprétation ouverte de la notion de signature, voir aussi E.A. CAPRIOLI, *op.cit.*, p.585 ; J. LARRIEU, *op.cit.* , H/88, p.8 et I/88, p.26 ; Y. POULLET, *op.cit.*, 1996, p. 52. Un arrêt récent de la Cour de cassation française invite également à adopter une conception fonctionnelle de la signature et de l'écrit, Cass. franç., 2 déc. 1997, note de P. CATALA et P-Y. GAUTIER, « L'audace technologique à la Cour de cassation : vers la libération de la preuve contractuelle », *La Semaine Juridique – Edition Générale*, 20 mai 1998, n° 21-22, p. 905.

[35] Pour déterminer la fiabilité de la méthode de signature utilisée, le juge dispose de différents critères d'appréciation, dont : 1) le degré de perfectionnement du matériel utilisé par chacune des parties ; 2) la nature de leur activité commerciale ; 3) la fréquence avec laquelle elles effectuent entre elles des opérations commerciales ; 4) la nature et l'ampleur de l'opération ; 5) le statut et la fonction de la signature dans un régime législatif et réglementaire donné ; 6) la capacité des systèmes de communication ; 8) la série de procédures d'authentification communiquée par un intermédiaire ; 9) l'observation des coutumes et pratiques commerciales ; 10) l'existence de mécanismes d'assurance contre les messages non autorisés ; 11) l'importance et la valeur de l'information contenu dans le message de données ; 12) la disponibilité d'autres méthodes

ne se limiter en aucun cas à une technique particulière de signature électronique[36] et de pouvoir ainsi s'adapter aux évolutions futures. Cette définition légale de la signature, qui se voudrait large et indépendante de la technologie, permettrait de renverser l'interprétation très restrictive de la notion de signature donnée par la Cour de Cassation. Ainsi, nous proposons la définition suivante : Constitue une signature, outre la signature manuscrite, l'ensemble de données issues de la transformation de l'écrit et dont ressort avec certitude l'identité de l'auteur et son adhésion au contenu de ce dernier.

L'adoption d'une définition légale de la notion de signature soulève la question de l'opportunité d'une définition légale de l'écrit. Une définition ouverte et fonctionnelle de la signature devrait suffire sans qu'il soit nécessaire d'inscrire une définition de l'écrit dans la loi. En effet, si le législateur admet que de nouvelles formes de signature puissent constituer une signature au sens du Code civil, a fortiori admettrait-il une évolution du concept d'écrit, la signature électronique ne pouvant être relative qu'à un écrit électronique.

Il convient de souligner que le Code civil reste muet sur cette question. En effet, si l'article 1341 vise formellement la signature, le législateur ne souffle mot du concept d'écrit. Néanmoins si l'écrit en tant que tel n'est pas clairement spécifié dans la loi, il ne fait nul doute qu'il est sous-entendu car la signature n'a de raison d'être que par l'existence de l'écrit auquel elle se rapporte[37].

Si une définition légale de l'écrit n'est pas indispensable, cela ne veut pas dire qu'il ne faille pas repenser la notion d'écrit. L'écrit ne doit plus uniquement être envisagé comme support durable (en l'occurrence, un papier) mais doit plutôt viser la garantie d'un contenu durable. En effet, dans l'environnement papier, il y a une confusion constante entre le contenu et le support, les deux notions ne faisant qu'une car le contenu est matériellement lié au support et l'intégrité n'est assurée que tant que le contenu se trouve sur le premier support. La fonction d'intégrité est donc partiellement[38] remplie grâce au papier.

Il en va différemment dans le contexte électronique. Il est parfaitement concevable de maintenir l'intégrité du contenu d'un message alors même que celui-ci change de support (tel est le cas, par exemple, d'un fichier signé digitalement qui se trouve sur une disquette et qui est ensuite transféré sur un disque dur et enfin sur un réseau). On constate que l'intégrité du contenu du message n'est plus assurée par le support mais par un mécanisme technique (de signature digitale ou autre) qui fige logiquement, et non plus matériellement, le contenu de l'écrit électronique. Ceci mène également à repenser les notions d'original et de copie[39].

## Chapitre 2. Fonctionnement de la signature digitale

Pour les raisons énoncées précédemment, nous réduirons désormais notre propos à un mécanisme particulier de signature électronique : la signature digitale. Celle-ci remplit les

---

d'identification et le coût de leur mise en oeuvre ; 13) le degré d'acceptation ou de non-acceptation de la méthode d'identification dans le secteur ou domaine pertinent, tant au moment où la méthode a été convenue qu'à celui où le message de données a été communiqué ; et tout autre facteur pertinent (Guide pour l'incorporation dans le droit interne de la Loi type de la CNUDCI sur le commerce électronique (1996), pp. 38 et 39).

[36] La définition ne doit donc pas viser uniquement la signature digitale, même si la suite de cet article traite essentiellement de cette technique qui est la plus mûre actuellement.

[37] H. DE PAGE, *Traité élémentaire de droit civil belge*, t. 3, *op. cit.*, n° 777.

[38] Elle est, dans une certaine mesure, également remplie par la signature manuscrite, voir supra note 32.

[39] Voir sur cette question les réflexions intéressantes d'E. DAVIO, *op.cit.*, pp.664 à 666.

différentes fonctions assignées à la signature et répond sans aucun doute à une définition fonctionnelle de la signature[40] car elle présente un niveau de sécurité et de fiabilité inégalé, tant par la signature manuscrite que par tout autre mécanisme de signature[41].

Une brève explication technique s'impose[42].

La signature digitale est fondée sur la cryptographie asymétrique, dite « à clé publique ». Dans un système à clé publique, la réalisation de la fonction d'identification suppose qu'une personne dispose de deux clés mathématiques complémentaires : une clé privée, dont le caractère secret doit effectivement être préservé, et une clé publique, qui peut être librement distribuée. La clé publique est une fonction de la clé privée qui est telle qu'il doit être aisé de calculer la clé publique à partir de la clé privée et matériellement impossible de déduire de la clé publique la clé privée correspondante. La clé publique doit dès lors représenter une fonction irréversible de la clé privée. La clé privée permet de « signer » le message. L'opération de décodage s'effectue, quant à elle, selon le principe de la complémentarité des clés : un message encodé avec une clé privée ne peut être décodé qu'avec sa clé publique complémentaire. L'exemple suivant illustre le fonctionnement de la signature digitale[43].

Alice désire envoyer à Bernard un message informatisé signé de façon électronique. Après avoir écrit son message, Alice réalise un condensé de ce message au moyen d'une opération mathématique. Ce condensé est le résultat d'une fonction appelée fonction de hachage irréversible. Cette fonction permet de générer de façon concise une chaîne de données qui représente le message en question. Cette représentation est sécuritaire, très précise et permet de détecter tout changement apporté au message. En effet il suffit au destinataire d'appliquer la fonction de hachage au message reçu et de comparer le condensé ainsi obtenu avec celui transmis par l'émetteur. Toute différence entre les condensés signifie que le message a été altéré en cours de transmission.

Ce condensé est par la suite encodé (rendu illisible et inaccessible) à l'aide de la clé privée d'Alice. Ce condensé encodé constitue la signature digitale. Alice envoie alors à Bernard son message (en clair) accompagné de la signature digitale.

Lorsque Bernard reçoit le message et la signature digitale, il décode cette dernière en effectuant une opération mathématique impliquant la clé publique complémentaire d'Alice. S'il parvient à décoder la signature, Bernard est assuré que celle-ci a préalablement été réalisée avec la clé privée complémentaire d'Alice : il sait alors de manière certaine qu'elle est l'auteur du message pour autant qu'une partie tierce (une autorité de certification) certifie que cette clé publique est bien celle d'Alice. Grâce à la fonction de hachage[44], l'intégrité du message d'Alice peut être garantie.

---

[40] E.A. CAPRIOLI, *op.cit.*, p.588.

[41] Ce qui ne veut pas dire que d'autres mécanismes de signature électronique ne pourraient pas satisfaire à une définition fonctionnelle de la signature.

[42] Voir pour plus de détails P. TRUDEL et S. PARISIEN, *op.cit*, pp. 91 et s. .

[43] Voir aussi le processus de création d'une signature digitale dans E.A. CAPRIOLI, *op.cit.*, p.588, n°27.

[44] Remarquons toutefois que la réalisation d'un condensé du message à l'aide de la fonction de hachage irréversible n'est pas indispensable. En effet l'émetteur du message pourrait directement encoder le message avec sa clé privée sans nécessairement passer par la production du condensé. Néanmoins la fonction de hachage irréversible sera souvent utilisée dans un souci de gagner du temps : encoder avec la clé privée un condensé (fichier de petite taille) est plus rapide que l'encodage du message en clair (fichier de plus grosse taille).

# 2ième partie. Les autorités de certification

L'utilisation de la signature digitale ne peut être envisagée sans l'intervention au départ d'autorités de certification (ci-après nommées AC). Celles-ci sont appelées à jouer un rôle fondamental dans le cadre de l'identification des différents utilisateurs de réseaux ouverts. Par l'émission de certificats, elles garantissent le lien entre une personne et sa clé publique.

Après quelques précisions terminologiques, nous analyserons les obligations pesant sur les AC et les autorités d'enregistrement, ainsi que sur les utilisateurs de services de certification. Nous présenterons, ensuite, quelques pistes d'orientation concernant le statut des AC.

## Chapitre 1er. Précisions terminologiques et fonctions des autorités de certification

### Section 1ère. Précisions terminologiques

Il convient de préciser, d'emblée, quelques concepts et de mettre en exergue les différences entre, d'une part, autorité de certification et tiers de confiance (Trusted Third Parties) et, d'autre part, autorité de certification et autorité d'enregistrement.

S'agissant, tout d'abord, de la première distinction, il faut noter que les technologies de cryptographie asymétrique peuvent faire l'objet de deux applications distinctes : d'une part, la signature digitale et d'autre part, le chiffrement en vue d'assurer la confidentialité du message[45]. Ces deux applications peuvent nécessiter l'intervention d'un organisme tiers dont le rôle différera en fonction du type d'application. Pour l'application signature digitale, le rôle principal de cet organisme tiers sera d'émettre des certificats au moyen desquels il confirme formellement le lien entre une personne et sa clé publique : on parlera d'autorité de certification pour désigner cet organisme. Pour l'application « chiffrement », le rôle de l'organisme tiers consistera à conserver une copie de la clé privée[46] utilisée pour déchiffrer le message[47] : on parlera plutôt de tiers de confiance (TTPs). Comme les fonctions de ces deux types d'institutions sont distinctes, il semble que la base légale des AC et des TTPs doive être clairement différenciée d'un point de vue juridique[48].

Il convient ensuite de distinguer la fonction d'enregistrement de celle de certification[49]. L'enregistrement, préalable à la certification, consiste à collecter de manière fiable et sécurisée les informations destinées à figurer sur le certificat (éléments d'identification, fonctions,…). Cette fonction d'enregistrement peut être réalisée par l'AC. Elle peut également être confiée à une autorité d'enregistrement distincte de l'AC (commune, ordre professionnel, chambre de commerce,…). Dans ce cas, il convient de s'interroger sur la répartition de responsabilité entre l'autorité d'enregistrement et l'AC[50].

---

[45] Nous n'approfondirons pas ce point dans le présent article.
[46] Ce qui ne veut pas dire qu'un tiers de confiance ne puisse pas également émettre de certificats.
[47] En effet, certains Etats exigent une telle conservation par des tiers de confiance autorisés afin de donner la possibilité à l'autorité publique de déchiffrer le message lorsqu'il existe des raisons impérieuses (telle que la protection de la sécurité publique par exemple).
[48] COM(97)503, *op.cit.*, p.4, point 2.
[49] P. TRUDEL et S. PARISIEN, *op.cit.*, p. 127.
[50] Cette question est développée *infra*, chapitre 2, section 2.

## Section 2. Fonctions des autorités de certification

La principale fonction d'une autorité de certification est d'assurer un lien formel entre une personne et sa clé publique[51]. Ce lien sera confirmé dans un certificat digital émis par l'AC. Ce certificat contient ainsi différentes informations relatives notamment à l'identité du titulaire du certificat (celui qui veut signer et s'identifier comme tel), sa clé publique et relatives à l'identité de l'AC. Le certificat est réalisé et signé par l'AC à l'aide de sa propre clé privée et est, de ce fait, protégé contre les altérations.

L'exemple suivant illustre l'utilisation possible de certificats. Alice transmet à Bernard un message ainsi que sa signature digitale réalisée à l'aide de sa clé privée. Après avoir reçu ces documents, Bernard commence par vérifier le certificat (qu'il aura soit reçu d'Alice soit été chercher dans un répertoire électronique de certificats) à l'aide de la clé publique de l'AC. Si la vérification s'avère concluante, il est assuré de l'intégrité des informations contenues dans le certificat, soient l'identité d'Alice, de sa clé publique ainsi que de l'identité de l'AC. Il peut ensuite utiliser la clé publique d'Alice pour vérifier la signature du message transmis par celle-ci.

L'AC peut remplir d'autres fonctions qui sont subsidiaires à la certification : l'archivage des informations qui sont relatives aux certificats (surtout pour des questions de preuve) ; le cas échéant, la génération de la paire de clés, sans toutefois conserver copie de la clé privée ; la tenue d'un registre électronique de certificats accessible au public ; l'horodatation de messages signés digitalement ; la vérification de signatures digitales et la confirmation de leur validité[52].

Ainsi qu'on le voit, le rôle de l'AC n'est pas minime. Elle doit mettre en place une infrastructure qui permette de collecter des informations et d'assurer leur intégrité en toute sécurité. L'efficacité du processus d'identification représente un élément déterminant de la responsabilité de l'AC.

Pour ces raisons et dans la droite ligne de la note adoptée par le Conseil des Ministres le 30 mai 1997, il semble que les activités des AC doivent, dans une certaine mesure, être réglementées.

**Pour résumer**, la signature digitale qui est basée sur la technique de cryptographie asymétrique et est combinée à l'utilisation d'un certificat permet de remplir trois fonctions importantes[53] : d'une part, elle garantit l'identité de l'auteur d'un document signé digitalement, d'autre part elle garantit l'intégrité de ce même document, enfin, elle atteste la volonté du signataire de s'approprier le contenu de l'acte signé digitalement[54].

---

[51] Cette clé publique ainsi que la clé privée complémentaire peuvent être générées soit par le titulaire soit par l'AC. Dans ce dernier cas, l'AC ne peut ni enregistrer ni conserver la clé privée générée.

[52] P. TRUDEL et S. PARISIEN, *op.cit.*, pp. 128 à 130 ; E.A. CAPRIOLI, *op.cit.*, p.589.

[53] Outre son utilisation aux fins de signature, la cryptographie peut également être utilisée afin d'assurer la confidentialité des messages. En vertu de l'article 79 de la loi du 19 décembre 1997, l'usage de la cryptographie est libre en Belgique (loi du 19 décembre 1997 modifiant la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques afin d'adapter le cadre réglementaire aux obligations en matière de libre concurrence et d'harmonisation sur le marché des télécommunications découlant des décisions de l'Union européenne, *M.B.*, 30 décembre 1997, p. 34986).

[54] Dans ce sens, E.A. CAPRIOLI, *op.cit.*, p.588, note 66.

Voyons désormais certains points concernant les AC qui mériteraient une attention particulière du législateur.

## Chapitre 2. Les obligations pesant sur les différents intervenants

L'élaboration de dispositions relatives aux obligations, et par voie de conséquence, à la responsabilité des autorités de certification est particulièrement importante car elles conditionnent la confiance[55] des utilisateurs de services de certification et par conséquent la réussite d'une infrastructure de certification en Belgique.

### Section 1ère. Obligations et responsabilité des autorités de certification

De l'analyse des obligations incombant aux AC, il ressort qu'elles peuvent être classées en deux catégories. La première a trait au fonctionnement du mécanisme de certification , plus précisément aux obligations de sécurité qui sont inhérentes à la fonction de certification. La seconde est relative à l'objet de leur activité.

§1er. La sécurité comme fondement de la certification

*1. Obligation de sécurité*

Ainsi qu'il sera souligné[56], une des conditions de base que doivent impérativement remplir les AC consiste à présenter des garanties de sécurité suffisantes pour qu'elles puissent exercer leurs activités. Les AC doivent notamment utiliser un système informatique fiable et faire en sorte de protéger adéquatement la confidentialité de la clé privée qu'elles utilisent pour signer les certificats qu'elles émettent.

*2. Obligation de renseignement et de conseil*

L'objectif d'une intervention législative serait essentiellement de renforcer la confiance des utilisateurs et de promouvoir l'utilisation de la signature digitale. Dans un domaine aussi technique, l'information correcte de l'utilisateur des services proposés par l'AC contribuerait à la réalisation de cet objectif. La loi pourrait donc faire peser sur l'AC une obligation de procurer toute information nécessaire à l'utilisation correcte et sûre de ces services. Elle se justifie d'autant plus que la signature digitale est une matière technique et complexe.

L'AC devrait notamment informer l'utilisateur des obligations qui pèsent sur elle, sur le titulaire de certificat et sur le destinataire du message signé digitalement ainsi que de la procédure à suivre pour produire et vérifier une signature digitale. L'AC devrait également informer l'utilisateur de la nécessité de signer au moyen d'une nouvelle clé privée les messages de données signés digitalement avant que la durée du certificat ne soit écoulée. En effet, la paire de clés et le certificat n'ont qu'une « durée de vie » limitée. Après une certaine période, on considère que cette paire de clés n'a plus un niveau de sécurité suffisant car le risque de découvrir la clé privée au départ de la clé publique augmente. L'utilisateur devra donc recréer une nouvelle paire de clés et un nouveau certificat pour signer les messages antérieurs et les nouveaux messages. Dès lors que l'on signe à nouveau un message antérieurement signé, il est indispensable que celui-ci garde la même valeur juridique que le message initialement signé. Cela ne semble pas poser de problème si ce sont les mêmes

[55] E.A. CAPRIOLI, *op.cit.*, p.589.
[56] voir *infra*, chapitre 3, section 2, §2.

parties qui signent une nouvelle fois. Mais on peut également imaginer que les parties confient à un tiers de confiance (une AC ou une autre entité) la tâche de signer lui-même le document tout en maintenant à celui-ci une valeur identique. C'est le problème de l'archivage électronique, qui dépasse notre propos, mais qui mériterait néanmoins une intervention légale.

*3. Obligation de se conformer aux prescriptions de la loi sur la protection de la vie privée*

L'AC, qui est chargée d'établir un certificat, doit être en mesure d'identifier de manière certaine et non équivoque le candidat titulaire. A cette fin, elle est amenée à collecter diverses informations sur les candidats. Elle ne peut toutefois collecter que les informations strictement nécessaires à la constitution du certificat et ne peut les utiliser que dans le cadre de son activité de certification. Elle ne pourra traiter ces données à d'autres fins que si le candidat titulaire a donné son accord à ce propos ou si elle y est autorisée par ou en vertu de la loi [57].

Le candidat titulaire ne désirant pas, ou n'étant pas légalement obligé de communiquer son identité, peut choisir un pseudonyme qui lui permettra de sauvegarder son anonymat. Toutefois, si les nécessité d'une instruction l'exigent, l'AC ayant délivré le certificat pourrait être tenue de communiquer les données relatives à l'identification du titulaire du certificat dans les circonstances et selon les conditions prévues par les articles 90 ter et suivants du Code d'instruction criminelle.

§2. L'exactitude comme essence de la certification

En publiant les certificats qu'elle émet, l'AC met à la disposition des destinataires de messages signés digitalement une banque de données informationnelles. Indépendamment de toute intervention légale, on peut considérer, en se fondant sur la doctrine récente[58], que l'AC se doit d'offrir un produit[59] répondant à l'attente légitime des utilisateurs.

En matière de certification électronique, cette attente légitime consiste à pouvoir disposer d'un produit informationnel dans lequel les informations sont exactes, complètes et mises à jour, étant donné que l'AC connaît les conséquences que pourrait entraîner la publication d'informations inexactes, incomplètes ou obsolètes.

*1. Les informations certifiées doivent être exactes*

Lorsqu'elle émet un certificat, l'autorité de certification garantit, tout d'abord, et, à titre principal, que la personne désignée dans le certificat est titulaire de la clé privée correspondant à la clé publique indiquée dans le certificat. Corrélativement, l'autorité de certification confirme, après avoir testé leur complémentarité, que ces clés sont appariées.

---

[57] Voir à ce propos l'article 5 de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel ainsi que les articles 6 et 7 de la Directive 95/46/CE du 24.1O.95 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

[58] E. MONTERO, *La responsabilité civile du fait des bases de données*, Travaux de la Faculté de Droit de Namur, P.U.N., 1998, à paraître.

[59] Il convient à ce propos de suivre la thèse d'E. MONTERO : puisque les services informationnels peuvent constituer des produits, la responsabilité des fournisseurs de données informationnelles peut être assimilée à la responsabilité des fournisseurs de produits, ceux-ci étant tenus de fournir un produit répondant à l'attente légitime des utilisateurs. E. MONTERO, *id.*

L'autorité de certification confirme ensuite que toutes les mentions figurant sur le certificat sont exactes. Outre les informations minimales que doit contenir tout certificat[60], le titulaire du certificat peut demander l'inscription d'une ou plusieurs informations complémentaires qui dépendront du but dans lequel la signature sera utilisée. Si l'autorité de certification n'est pas tenue de les certifier, elle doit toutefois indiquer le caractère confirmé ou non de ces informations complémentaires. A défaut d'une telle précision, l'AC est présumée avoir vérifié la véracité des informations complémentaires et sa responsabilité pourrait être engagée si une de celles-ci se révélait erronée.

Enfin, l'inscription du certificat dans le registre électronique prévu à cet effet suppose que le titulaire désigné dans le certificat ait marqué son accord quant au contenu du certificat.

*2. Les informations certifiées doivent être complètes*

Le certificat consiste en la confirmation d'une ou plusieurs informations. L'autorité de certification ne pourrait délivrer des certificats qui contiendraient moins que les informations minimales requises par la loi ou stipuler qu'elle n'a pu vérifier une ou plusieurs de ces informations. Toutefois, elle devrait pouvoir refuser l'octroi d'un certificat si elle a de sérieux doutes quant à l'identité ou à l'attribut[61] de la personne physique ou morale, qu'elle ne peut vérifier par des moyens raisonnables. Il pourrait par exemple être difficile pour une AC belge de vérifier l'existence et l'identité d'une société ayant son siège social dans un pays tiers ayant un régime juridique totalement différent de celui qui prévaut en Belgique. Il en ira de même si l'AC estime objectivement que l'attribut n'a pas un caractère durable. Notons néanmoins qu'une AC pourrait difficilement se prévaloir du fait qu'elle ne dispose pas de moyens raisonnables pour vérifier la seule identité d'une personne physique.

Ce tempérament à l'obligation de délivrance se justifie par le fait qu'on ne peut obliger une AC à délivrer un certificat et engager ainsi sa responsabilité si elle n'est pas en mesure de vérifier correctement les informations obligatoires contenues dans le certificat.

*3. Les informations certifiées doivent être mises à jour*

L'essence du certificat étant de refléter la réalité à un moment donné, il est nécessaire que les informations détenues par l'autorité de certification soient maintenues à jour, sans quoi l'activité de certification ne revêtirait plus d'utilité, faute de fiabilité. A cette fin, l'autorité de certification a l'obligation de créer et de gérer un registre électronique accessible en permanence à toute personne par voie électronique. Ce registre énumère les certificats émis par l'autorité qui le tient, le moment de leur émission, celui de leur expiration et, le cas échéant, celui de leur suspension ou de leur révocation. Ce registre doit être protégé contre toute altération ou modification non autorisée.

La **suspension** consiste en l'interruption, jusqu'à nouvel ordre, de l'usage d'un certificat. Il s'agit d'une mesure transitoire qui devrait donner lieu soit à la révocation du certificat soit à la levée de la suspension. Elle peut émaner d'un ordre du titulaire du certificat ou avoir lieu à

[60] La fonction principale du certificat étant de confirmer le lien entre un titulaire et sa clé publique, il est essentiel qu'il contienne au moins les informations suivantes :
- identification du titulaire ;
- clé publique du titulaire correspondant à la clé privée dont le titulaire a le contrôle ;
- dates d'émission et d'échéance du certificat ;
- identification de l'autorité de certification.

[61] Par attribut, on entend toute caractéristique attachée à une personne, autre que son identité.

l'initiative de l'autorité de certification[62]. Dans cette seconde hypothèse, elle ne peut être opérée que si l'autorité de certification a des raisons sérieuses et motivées de croire que la confidentialité de sa clé privée ou de celle du titulaire du certificat a été compromise, que son système informatique ou celui du titulaire du certificat compromet la fiabilité du certificat ou que le certificat émis n'est pas ou plus conforme à la réalité (décès du titulaire s'il s'agit d'une personne physique, dissolution ou faillite lorsqu'il s'agit d'une personne morale, perte d'un attribut, etc).

La **révocation**[63] consiste à mettre fin, sans effet rétroactif, au certificat avant sa date d'expiration. Elle peut avoir lieu à la demande du titulaire du certificat ou à l'initiative de l'autorité de certification. Dans cette seconde hypothèse, en raison de l'importance de cette mesure et de son caractère irréversible, elle devait être précédée d'une décision de suspension afin que l'autorité de certification puisse procéder à un examen plus approfondi des raisons qui ont motivé sa décision de suspension et d'en aviser le cas échéant le titulaire. Les hypothèses d'une révocation à l'initiative de l'autorité de certification seraient essentiellement celles où l'AC arrête ses activités sans qu'il y ait reprise de celles-ci par une autre AC ou lorsqu'une AC est informée du décès de la personne physique ou de la liquidation de la personne morale qui en est titulaire.

S'agissant de l'obligation de l'autorité de certification de procéder à la suspension ou à la révocation de certificats, une distinction est à établir selon que l'obligation de l'AC procède d'un ordre émanant d'un utilisateur ou s'inscrit dans le prolongement de l'acte initial de certification à savoir l'émission du certificat.

Dans la première hypothèse, il convient de considérer que l'obligation d'exécuter les ordres de suspension ou de révocation est de résultat[64] car la part d'aléa est trop réduite pour considérer qu'il y a obligation de moyen.

En outre, lorsque le titulaire demande la suspension ou la révocation du certificat, l'AC est tenue de procéder « immédiatement » à cette suspension ou révocation. Il convient toutefois de noter que le terme « immédiatement » devrait avoir une valeur temporelle différente suivant qu'il s'agit d'une demande de suspension ou de révocation. En effet, avant de procéder à la suspension ou à la révocation, l'AC est tenue d'identifier la personne qui effectue la demande. Cette identification prendra un certain temps. Toutefois ce laps de temps doit nécessairement être extrêmement court en cas de demande de suspension. La suspension suppose que l'on veuille agir vite et bloquer rapidement le certificat afin d'éviter toute utilisation frauduleuse. L'AC pourra donc se contenter de procéder à une identification succincte voire tout à fait superficielle. On estime, dans ce cas, que les inconvénients qui résulteraient de l'absence de suspension immédiate sont supérieurs à ceux qui découleraient d'une suspension demandée par une personne mal intentionnée qui se ferait passer pour le

[62] La procédure de suspension peut être déclenchée d'office par l'AC ou, le cas échéant, sur base d'informations fournies par des tiers. Dans cette seconde hypothèse, préalablement à toute vérification relative à la véracité des renseignements fournis, l'on devrait songer à ce que l'AC ne procède pas à la suspension du certificat, qui pourrait être préjudiciable au titulaire, mais mentionne qu'une information du certificat est affectée d'un indice de doute.

[63] La CNUDCI parle, dans ses travaux, d' annulation. A ce terme, qui pourrait introduire certaines ambiguités, nous préférons celui de révocation ; Commission des Nations Unies pour le Droit Commercial International, *op.cit.*, 12 mars 1997.

[64] Voir, par analogie l'obligation de résultat qui pèse sur la banque lorsqu'il s'agit de bloquer, en cas de perte ou de vol, la carte magnétique permettant l'accès à un guichet automatique de banque. Liège, 22 févr. 1985, *Droit de l'inf.*, 1985/6, p. 28, note B. AMORY.

titulaire du certificat. Par contre, une demande de révocation a des conséquences plus graves qu'une demande de suspension, notamment par le fait qu'une décision de révocation est irréversible. Il est dès lors indispensable que l'AC identifie de manière certaine la personne qui effectue la demande de révocation pour s'assurer qu'elle est le véritable titulaire du certificat, même si cette identification peut prendre du temps. Dans ce cas, il n'existe aucun risque car toute révocation peut être précédée d'office par une suspension. On peut donc dire que le caractère immédiat de l'obligation est plus court s'il s'agit d'une suspension que s'il s'agit d'une révocation.

Dans le second cas, par contre, lorsque la suspension ou la révocation ne procède pas d'un ordre du titulaire du certificat, la nature des obligations incombant à l'autorité de certification doit être appréhendée différemment. Si l'autorité de certification s'engage, par son activité, à mettre en œuvre les moyens appropriés[65] pour garantir la mise à jour des certificats, elle ne pourrait toutefois s'engager à garantir l'absolue véracité des informations figurant sur le certificat postérieurement à son émission. L'obligation de mise à jour des certificats doit dès lors être considérée comme étant de moyen.

L'analyse des obligations de l'autorité de certification relatives au caractère actuel des informations doit donc être circonstanciée.

§3. Régime de responsabilité

Le régime de responsabilité institué doit établir un équilibre entre les intérêts des autorités de certification et celui des utilisateurs des certificats émis (titulaire de la clé et destinataire d'un message signé digitalement) afin que le régime de certification présente un haut degré de fiabilité et, par là même, de crédibilité, sans qu'il entrave pour autant le développement de la certification électronique et, par conséquent, des applications qui en découlent.

Il conviendrait de concevoir un régime de responsabilité qui allège la charge de la preuve qui pèse sur l'utilisateur d'un certificat erroné. Ainsi pourrait-on prévoir un régime de présomption de responsabilité à charge de l'AC. En cas d'identification erronée du titulaire du certificat, d'attribution par erreur d'une clé publique à une personne, ou de certification d'une information incorrecte, l'autorité de certification serait présumée responsable du préjudice subi, sauf si elle parvient à démontrer, soit qu'elle s'est conformée aux obligations qui lui incombent, soit l'existence d'autres causes étrangères libératoires[66].

**Section 2. Obligations des autorités d'enregistrement**

Certaines des fonctions dévolues à l'autorité de certification peuvent être confiées par celle-ci à une autorité d'enregistrement (ordre professionnel, chambre de commerce, …) dont la mission sera d'assurer la collecte d'informations destinées à figurer sur le certificat pour ensuite les communiquer[67] à l'AC. C'est toutefois à celle-ci que reviendra la fonction ultime

[65] Ainsi, lorsque la certification a lieu sur base d'informations fournies par une autorité d'enregistrement, il convient de considérer que l'AC a l'obligation de mettre en place des procédures sécurisées pour la mise à jour régulière des informations. Cette obligation incombant aux AC sous-tend l'obligation, pour les autorités d'enregistrement, de communiquer toute information pouvant avoir une incidence sur le caractère exact ou complet des certificats émis sur base d'informations communiquées par l'autorité d'enregistrement.

[66] Commission des Nations Unies pour le Droit Commercial International, *op.cit.*, 12 mars 1997, p.16.

[67] S. PARISIEN, P. TRUDEL, *op. cit.*, p. 159.

de confirmer, sur base des documents produits, la correspondance personne-clé publique par l'émission de certificats.

Des législations ou projets de législation[68] faisant référence à la notion de certificat, il ressort clairement que la volonté des divers législateurs a été de désigner une autorité responsable en la soumettant, d'une part, à des conditions d'agréation très strictes et, d'autre part, en faisant de la signature de l'autorité agréée une condition de validité du certificat. De ces éléments, il résulte que, quand bien même les informations seraient-elles rassemblées par l'autorité d'enregistrement, c'est l'autorité de certification qui engage sa responsabilité. Elle ne pourrait donc s'exonérer de sa responsabilité en arguant qu'elle ne pouvait connaître le caractère erroné des informations en raison de la collecte de celles-ci par une autorité d'enregistrement. En sa qualité d'autorité de certification, une obligation de contrôle de vraisemblance pèse sur elle.

**Section 3. Obligations des utilisateurs**

§1. Obligations des titulaires de certificats

Lors de l'introduction de sa demande, le candidat-titulaire a l'obligation de fournir à l'autorité de certification toute information pertinente qui est nécessaire à l'élaboration du certificat. Sa responsabilité pourrait dès lors être engagée en cas de dommage causé par l'utilisation d'un certificat dont il est titulaire si celui-ci contient, par sa faute, des informations inexactes ou incomplètes à son sujet[69].

En raison des conséquences juridiques qui sont liées à l'utilisation de la signature digitale, il est impératif que le titulaire de la clé secrète, liée à la clé publique certifiée au moyen du certificat, prenne les mesures nécessaires afin d'en préserver la confidentialité. S'il craint toutefois que la confidentialité de la clé secrète ait été compromise, il a l'obligation d'en avertir immédiatement l'autorité de certification et de lui faire procéder soit à la suspension, soit à la révocation du certificat. Il en va de même si l'une des mentions du certificat n'est plus conforme à la réalité (suite à un changement d'identité ou la perte d'un attribut par exemple).

Que ce soit à l'expiration du certificat ou en cas de suspension ou de révocation de celui-ci, le titulaire du certificat a l'obligation de s'abstenir d'utiliser la clé privée liée à la clé publique certifiée par le certificat suspendu ou révoqué. La responsabilité de l'autorité de certification ne pourrait être engagée si le titulaire contrevenait à cette obligation.

§2. Obligations des destinataires de messages signés digitalement

Une obligation de vérification pèse sur le destinataire d'un message signé digitalement. Il est tenu, tout d'abord, de vérifier la signature au moyen du certificat correspondant (afin de s'assurer de l'adéquation titulaire-clé publique). Il doit ensuite s'assurer que le certificat en question a été émis par une autorité de certification agréée ( puisque seules les signatures réalisées sur cette base seraient automatiquement considérées comme répondant à la définition fonctionnelle de la signature qui serait insérée dans le Code civil et bénéficieraient ainsi des conséquences juridiques qui y seraient attachées). Le destinataire du message doit enfin contrôler que le certificat n'est ni expiré, ni suspendu ni révoqué.

[68] Voir *supra* notes 5 à 7.
[69] S. PARISIEN, P. TRUDEL, *op. cit.*, p. 135.

## Chapitre 3. Quelques pistes d'orientation pour un statut des AC

L'activité de certification est relativement nouvelle[70]. Dès lors, peu de règles peuvent actuellement se dégager de la pratique. On peut imaginer une grande variété de systèmes et de solutions, et le législateur demeure très libre dans les orientations qu'il peut prendre. Toutefois, il conviendrait qu'il adopte une série de principes fondamentaux qui assurent la cohérence et la faisabilité du système dans l'environnement actuel ainsi qu'une grande souplesse qui lui permettent de s'adapter aisément à l'évolution du marché et de la technologie.

### Section 1ère. Libertés et variabilité de l'agréation

§1. Liberté d'agréation

*1. Diversité des systèmes*

Lorsqu'on analyse les initiatives prises en Europe ou ailleurs[71], on constate qu'il existe une grande variété de projets prenant des orientations différentes. Certains pays mettent en place une infrastructure de certification hiérarchisée[72]. Cette structure pyramidale à plusieurs niveaux comprend des autorités de certification qui exercent leurs activités sous la gouverne d'une AC suprême. Le rôle de cette dernière est d'émettre des certificats destinés à l'identification des AC régionales ou sectorielles hiérarchiquement inférieures et non à l'identification des signataires. Un tel système n'est pas sans inconvénient. Il est lourd et difficile à organiser. De plus se pose la question de savoir quelle entité peut jouer le rôle d'autorité suprême. Parallèlement, d'autres pays comme l'Allemagne[73] ou l'Italie[74] adoptent un système beaucoup plus souple et non hiérarchique où peuvent coexister une multitude d'AC. Ce système peut être subdivisé en deux sous-systèmes : d'une part, un système obligatoire dans lequel toute entité sur le marché désirant exercer une activité de certification serait nécessairement soumise à une réglementation après avoir obtenu obligatoirement une agréation ou une licence et, d'autre part, un système libre où peuvent coexister sur le marché des AC agréées et non agréées, soumises ou non à la réglementation, la demande d'agréation n'étant que facultative. Parmi ces différentes possibilités, le système libre d'agréation semble offrir un maximum de souplesse tout en assurant un niveau de sécurité satisfaisant.

*2. Vers un système libre d'agréation*

Dans un système libre d'agréation , une AC n'aurait pas l'obligation de demander une agréation pour exercer ses activités de certification. Toutefois si une AC désirerait obtenir une agréation, elle devrait répondre à des conditions prévues par la loi, qui auraient pour objectifs de garantir un ensemble d'impératifs de nature à accroître la confiance dans les AC qui répondent à celles-ci (AC agréées) et d'établir un régime clair de responsabilité.

---

[70] Des sociétés telles que Verisign aux Etats-Unis ainsi que Belsign et Isabel en Belgique se sont déjà engagées sur le marché de la certification.

[71] Voir à ce propos P. TRUDEL et S. PARISIEN, *op.cit.*, pp. 117 et s. .

[72] Voir notamment le projet d'infrastructure de clé publique du gouvernement fédéral canadien ou le projet européen FAST (First Attempt to Secure Trade) dans P. TRUDEL et S. PARISIEN, *op.cit.*, pp. 120 et 147 .

[73] Loi allemande du 13 juin 1997, *op.cit.*, note 6.

[74] Décret présidentiel italien du 10 novembre 1997, *op.cit.*, note 7.

Le choix entre un système d'agréation libre et un système obligatoire n'est pas aisé. Le système obligatoire permettrait d'assurer que toute entité qui effectue de la certification sur le marché belge a obtenu une agréation et qu'elle présente ainsi un niveau de sécurité élevé. Cependant il existe plusieurs éléments qui plaident en faveur de l'adoption d'un système libre d'agréation[75].

Le système obligatoire porte atteinte au principe de la liberté probatoire en matière commerciale. De ce principe, il résulte que deux commerçants peuvent faire la preuve de leur acte juridique l'un envers l'autre par toute voie de droit, y compris un document signé digitalement, peu importe qu'il soit combiné à un certificat émis par une AC agréée ou non. Or dans un système obligatoire, on imposerait aux commerçants de recourir à une AC agréée pour faire la preuve de leurs transactions, sans qu'ils puissent se prévaloir d'un document dont la signature digitale est combinée à un certificat émis par une AC non agréée[76].

De plus, la coexistence d'AC agréées et non agréées permettrait de répondre adéquatement aux différentes demandes de ce marché en pleine évolution. En effet, tout type de transaction électronique n'exige pas nécessairement un niveau de sécurité élevé. Les utilisateurs doivent donc garder le choix, suivant l'utilisation qu'ils veulent faire de la signature digitale, de recourir à une AC agréée ou non, sachant que la tarification, les services, l'accessibilité,… seront probablement différents dans l'un et l'autre cas.

Notons que l'adoption d'un système libre est encouragée par la Commission européenne qui indique dans sa communication du 8 octobre 1997[77] que « en tout état de cause, il faut assurer la coexistence de systèmes de signatures numériques réglementées et non réglementées ». Elle ajoute que « un cadre réglementaire (communautaire) devrait permettre la coexistence d'AC licenciées et non licenciées ».

§2. Liberté de signature et de recours à une AC

Même si de nouvelles formes de signature se développent, il ne faut pas en arriver à exclure la signature classique et il serait inconcevable de contraindre une personne de recourir à une signature digitale. Dès lors toute personne doit garder le libre choix d'utiliser sa signature manuscrite ou de recourir à une signature digitale, même dans ses rapports avec l'administration.

Dans le même sens, le choix de recourir à une autorité de certification agréée ou non agréée doit être libre. La personne qui décide de recourir à une signature digitale doit rester libre de se faire délivrer un certificat par une AC agréée ou non. Toutefois il peut arriver que certaines relations ou transactions exigent un certain niveau de sécurité et de fiabilité, tel que cela pourrait être le cas, par exemple, dans le cadre du transfert de données entre le citoyen et l'administration ou dans le cadre de transactions ayant des implications financières importantes. Dans de telles hypothèses, il devrait être possible d'obliger, par la loi, que lorsqu'une personne souhaite signer digitalement, la signature digitale soit combinée à un certificat émis par une AC **agréée**.

---

[75] Pour une opinion en sens contraire, voir E.A. CAPRIOLI, *op.cit.*, p.590.

[76] Puisque dans un système obligatoire, aucune AC ne peut exercer l'activité de certification sans avoir préalablement obtenu une agréation. On constate également qu'un tel système réduit fortement l'utilité des conventions par lesquelles les parties règlent, essentiellement dans les systèmes fermés tels qu'Isabel, les questions relatives à la preuve et aux activités de l'AC.

[77] COM(97)503, *op. cit.*, point 4.

§3. Système d'agréations variables

En vue de garantir au système un maximum de souplesse, la loi devrait donner la possibilité pour une AC de demander une agréation plus ou moins étendue en fonction des personnes auxquelles elle souhaite délivrer des certificats. L'agréation pourrait donc avoir un contenu variable qui dépendra au départ de la demande effectuée par l'AC. En effet, la loi devrait permettre qu'une AC puisse demander une agréation large qui couvre la délivrance de certificats à la fois à des personnes physiques et morales de droit privé ou de droit public (ci-après personne morale). Inversement, l'AC pourrait restreindre l'étendue de son agréation à la délivrance de certificats à l'une ou l'autre de ces personnes. Elle pourrait même limiter son agréation à la délivrance de certificats à des personnes physiques ayant un attribut particulier. Par exemple, une AC pourrait se spécialiser dans la certification de la profession d'avocat ou de médecin : l'AC serait donc agréée pour certifier une personne physique ayant l'attribut avocat ou médecin mais ne pourrait pas se prévaloir de son statut d'AC agréée pour les autres catégories de personnes physiques (notaire, architecte,…) ni pour les personnes morales. Toutefois, son agréation couvrirait la certification de toute personne physique n'ayant aucun attribut à certifier (l'AC se limite à certifier l'identité d'un citoyen).

**Section 2. Garanties fondamentales de fonctionnement des AC**

Certaines garanties de base doivent impérativement être fournies par une AC afin de créer et de renforcer la confiance que les utilisateurs peuvent avoir en elle[78].

§1er. Garantie d'indépendance

L'AC doit disposer d'une indépendance minimale. Celle-ci se manifeste dans la possibilité pour l'AC d'agir indépendamment de toute pression d'un acteur qui est partie aux transactions. Elle doit notamment être exempte de tout intérêt financier ou autre, direct ou indirect, dans les opérations. Elle doit également être reconnue pour ses qualités d'intégrité et d'impartialité.

§2. Garanties de sécurité et de fiabilité

L'AC doit aussi présenter des garanties de sécurité suffisantes afin d'exercer ses activités. A ce titre, elle utilise un système informatique fiable et fait en sorte de protéger adéquatement la confidentialité de la clé privée qu'elle utilise pour signer les certificats qu'elle émet. Elle possède l'expertise nécessaire pour exercer ses activités de certification. Elle assure sa sécurité interne en mettant en place un dispositif d'urgence (par exemple, un logiciel de récupération catastrophe ou un mécanisme de blocage de la clé privée) et en utilisant du matériel et des logiciels accrédités. Elle met sur pied un processus de sélection et de gestion du personnel afin d'engager des employés compétents, ayant une bonne maîtrise de la technologie à clé publique et des procédures de sécurité, et intègres (absence de condamnation pour fraude, faux en écriture, …).

[78] Cette section est essentiellement inspirée des documents suivants : Commission des Nations Unies pour le Droit Commercial International, *op.cit.*, A/CN.9/WG.IV/WP.73, 12 décembre 1997, pp. 17 et 18 ; COM(97)503, *op.cit*, pp.7 et 21 ; Utah Digital Signature Act, Utah Code Annotated, *op. cit.*, art. 201,202 et 301 ; Loi allemande sur la signature digitale du 13 juin 1997, *op.cit.*, §4 et 14 ; Décret présidentiel italien, *op.cit.*, art. 3 et 8 ; P. TRUDEL et S. PARISIEN, *op.cit.*, pp. 131 et 132 ; E.A. CAPRIOLI, *op.cit.*, p. 589 ; Electronic Commerce Promotion Council of Japon (ECOM), Certification Authority Working Group, « Certification Authority Guidelines », April 1997, ECOM-WG08/SWG1.

§3. Garanties d'information

L'AC devrait également faire une déclaration relative aux pratiques de certification [79]. Il s'agit d'une déclaration dans laquelle l'AC expose la politique qu'elle suit ou donne des détails sur les pratiques, procédures et systèmes qu'elle applique dans son activité, venant à l'appui de l'émission, de la gestion et de la révocation d'un certificat. Ces éléments sont importants, à la fois pour le titulaire qui reçoit le certificat, et pour les parties qui s'y fieront pour effectuer des transactions avec ce dernier. Pour cette raison, la déclaration devrait être publique ou à tout le moins accessible au public.

§4. Garanties financières

L'AC doit également posséder des garanties financières suffisantes pour exercer ses activités et, le cas échéant, indemniser les utilisateurs ayant subi un dommage suite à l'inexécution des obligations qui lui sont imposées par la loi. A cet effet, elle souscrira utilement une assurance en vue de couvrir sa responsabilité professionnelle.

§5. Garanties tarifaires

Les tarifs appliqués par l'AC doivent être exprimés de manière claire et ne peuvent en aucun cas être discriminatoires. Par ailleurs, dans la société de l'information, l'accès à la signature digitale devrait constituer un droit. La reconnaissance de ce droit, c'est-à-dire la reconnaissance de l'accès à la signature digitale à des prix abordables, pourrait être atteint par la fixation de conditions tarifaires, voire la fixation de tarifs réduits pour certaines couches de la population.

§6. Garanties d'interopérabilité

Enfin, comme l'indique la Commission européenne dans sa communication du 8 octobre 1997[80], l'interopérabilité des différents systèmes et applications de signatures digitales est absolument nécessaire afin d'assurer que celles-ci puissent être mises en œuvre en Europe et en dehors de l'Europe.

**Section 3. Délivrance de certificats aux personnes physique et morale de droit privé ou de droit public.**

La délivrance de certificats par une AC agréée ne devrait pas se limiter aux personnes physiques mais s'étendre aux personnes morales[81]. Ainsi, toute personne ayant la personnalité juridique devrait avoir le droit de demander et d'obtenir un certificat. Il en résulte qu'un citoyen, une société commerciale, une ASBL, un GIE, l'Etat, un parastatal, une EPA,… pourraient devenir titulaire d'un certificat. Par ailleurs, une personne physique ou morale doit pouvoir faire certifier plusieurs clés et devenir ainsi titulaire de plusieurs certificats.

A l'inverse, les entités qui n'ont pas la personnalité juridique ne pourraient pas obtenir de certificat d'une AC agréée. La raison de ce choix réside dans la difficulté pour une AC de

[79] Commission des Nations Unies pour le Droit Commercial International, *op.cit.*, A/CN.9/WG.IV/WP.73, 12 décembre 1997, § 59.
[80] COM(97)503, *op. cit.*, p. 21.
[81] Dans le même sens, voy. E.A. CAPRIOLI, *op.cit.*, p.588, n°29.

vérifier et de confirmer l'identité d'une entité qui n'existe pas juridiquement alors que cette tâche s'avère plus aisée pour les personnes ayant une personnalité juridique (une personne physique peut être identifiée au moyen d'un document officiel, les données d'identification d'une personne morale sont publiées au Moniteur Belge et un Registre national des personnes morales existe). De plus, si on admet la signature des personnes morales, il est difficile de reconnaître à une entité qu'elle puisse être titulaire d'une clé privée et d'un certificat, susceptible a priori de l'engager, si cette entité n'a pas la personnalité juridique.

La possibilité pour une personne morale de demander un certificat est nécessaire dans la mesure où la communication électronique ne se limite pas à une communication entre personnes physiques. Bien au contraire, il est révélateur par exemple de voir la croissance du nombre de sites sur Internet appartenant à une personne morale. La plupart de ces sites ne contiennent aucune référence à des personnes physiques et la communication est directement établie avec la personne morale. Cette évolution démontre bien la volonté de ces dernières de s'identifier en tant que telles, sans passer par l'intermédiaire d'une personne physique. De plus, on peut très probablement s'attendre à ce que le développement du commerce électronique soit essentiellement le fait de personnes morales. Enfin il est primordial que le consommateur qui effectue des transactions électroniques puisse s'assurer de l'identité exacte de la personne morale avec laquelle il traite, puisqu'en définitive, celle-ci sera engagée financièrement. Il eût, dès lors, été déraisonnable de réserver la délivrance de certificats uniquement à des personnes physiques.

Cette solution est préconisée par la Commission Européenne qui, dans sa communication du 8 octobre 1997[82], indique dans le point 2.3., (i) que « Les clés *(et par conséquent les certificats)* peuvent être allouées à des personnes privées ou juridiques (par exemple une société à responsabilité limitée)… ». Les travaux de la CNUDCI des Nations Unies se dirigent également dans ce sens. En effet, dans son rapport du groupe de travail sur le commerce électronique[83], la CNUDCI analyse le projet d'article D qui reconnaît expressément la possibilité pour une personne morale d'obtenir la certification de clés publiques. Le texte ajoute qu'il « était inopportun d'établir une distinction entre personne morale et personne physique aux fins des signatures numériques ». Cette prise de position se fonde notamment sur la Loi type de la CNUDCI sur le commerce électronique « où la notion de personne recouvrait aussi bien les personnes physiques que les personnes morales ».
De même, la loi de l'état de l'Utah des Etats-Unis[84], qui constitue la première législation consacrée exclusivement à la signature digitale et aux autorités de certification, ainsi que la version finale de la proposition californienne de réglementation de la signature digitale[85], adoptent une position identique. Enfin le décret présidentiel italien[86] semble aller dans le même sens puisque dans la section 8 relative à la certification, le texte traite de « toute personne ou entité ».

On constate que la pratique actuelle des autorités de certification va clairement dans ce sens : Belsign, Isabel et Verisign, par exemple, délivrent des certificats aussi bien à des personnes physiques qu'à des personnes morales. Ces autorités de certification ne font finalement que répondre à la demande du marché.

---

[82] COM(97) 503, *op. cit.*
[83] Commission des Nations Unies pour le Droit Commercial International, *op. cit.*, A/CN.9/437, 12 mars 1997.
[84] Utah Digital Signature Act, Utah Code Annotated, *op. cit.*, note 5.
[85] Final Draft of California Digital Signature Regulations, *op. cit.*, note 5.
[86] Décret présidentiel italien du 10 novembre 1997, *op. cit.*, note 7.

## Section 4. Lien avec une définition fonctionnelle de la signature

Le message signé électroniquement à l'aide d'une signature digitale réalisée sur base d'un certificat émis par une autorité de certification agréée devrait constituer une signature au sens d'une définition fonctionnelle de la signature qui serait insérée dans le Code civil. Le régime sécuritaire qui entourerait l'infrastructure de certification agréée serait tel qu'il conférerait à la signature digitale un niveau de sécurité équivalent, voire supérieur à la signature manuscrite. Dès lors, les conséquences juridiques liées à l'utilisation de la signature digitale devraient être les mêmes que celles qui sont actuellement attachées à l'usage de la signature manuscrite[87].

Cette solution est encouragée tant par la CNUDCI que par la Commission européenne. En effet, dans ses travaux relatifs à l'élaboration de Règles uniformes sur les signatures électroniques[88], la CNUDCI propose trois définitions : une de la « signature », une deuxième de la « signature électronique » et enfin une définition de la « signature électronique sûre ». Elle précise dans ses observations que ces définitions permettent de délimiter dans ses grandes lignes le champ d'application des Règles uniformes, qui couvrent aussi toutes les techniques applicables pour fournir un équivalent fonctionnel à une signature manuscrite. Toutefois, elle ajoute que « la principale définition à retenir pour délimiter le champ d'application des Règles uniformes est celle de « signature électronique sûre », le but recherché étant de qualifier un niveau supérieur de fiabilité d'une signature électronique par référence à un ensemble de critères qui, une fois satisfaits, produiraient certains effets juridiques » (équivalents à la signature manuscrite). La CNUDCI considère que constitue d'emblée une « signature électronique sûre » la signature numérique qui est utilisée dans le cadre d'une infrastructure à clé publique réglementée c'est-à-dire la signature numérique combinée à un certificat émis par une AC agréée par l'Etat. Dans le même sens, la Commission européenne indique dans sa communication du 8 octobre 1997 que, tout en relevant les différences entre la signature manuscrite et la signature numérique, « ces différences n'empêchent pas les signatures numériques d'avoir une valeur juridique équivalente pour certaines fins légales »[89] (notamment sur le plan de la preuve).

[87] Selon E.A. Caprioli « Avec l'usage d'une signature numérique, le consentement à l'acte ne semble faire aucun doute, …, l'adjonction de l'abrégé du message chiffré avec la clé privée au message correspond en quelque sorte à la signature au bas d'un acte. Ainsi, la signature numérique est intimement liée au contenu de l'acte établi sous la forme d'un message », *op.cit.*, p.588 et la note 66.

[88] Commission des Nations Unies pour le Droit Commercial International, Note du secrétariat du groupe de travail sur le commerce électronique sur les travaux de sa trente-deuxième session concernant le projet de règles uniformes sur les signatures électroniques (Vienne, 19-30 janvier 1998), A/CN.9/WG.IV/WP.73, 12 décembre 1997.

[89] COM(97)503, *op.cit.*, p. 10.

# CONCLUSIONS

La mise en place d'une procédure de certification n'a de sens en Belgique que si l'admissibilité de documents signés digitalement peut être envisagée sur une base légale adéquate. Il s'agirait donc, dans un premier temps, de définir la signature afin que ne soit pas écartée la signature digitale pour le seul motif qu'elle ne répond pas à l'interprétation qui a été donnée de la notion d'écrit signé. La tâche consisterait ensuite à jeter les bases juridiques d'un mécanisme de certification afin que la fonction d'identification puisse être assurée en réseau ouvert.

**Vers une –nouvelle- définition de la signature**

La signature digitale, fondée sur la cryptographie asymétrique ou à clé publique, remplit adéquatement les deux fonctions attribuées à la signature :
1. identification du signataire
2. expression de la volonté du signataire de s'approprier le contenu de l'acte auquel la signature se réfère.

Si le Code civil belge ne donne aucune indication quant aux formes que doit revêtir la signature, l'interprétation qu'en a donnée la jurisprudence semble constituer aujourd'hui un obstacle à l'admissibilité de documents signés électroniquement sur base de l'article 1341 du Code civil. Eu égard au développement de nouvelles méthodes de signature qui présentent un niveau de sécurité équivalent, voire supérieur à la signature manuscrite et qui, de surcroît, sont susceptibles de remplir des fonctions supplémentaires (telles que l'authentification de contenu), la nécessité de s'orienter vers une définition de la signature, écartant toute ambiguïté, est aujourd'hui ressentie. Celle-ci doit impérativement se fonder sur les fonctions reconnues à la signature afin de laisser la voie ouverte au développement de nouvelles techniques de signature[90].

**Elaboration d'une réglementation relative à la certification électronique**

Les autorités de certification sont appelées à jouer un rôle essentiel dans l'accomplissement de la première fonction de la signature, à savoir l'identification du signataire.

Une réglementation de la certification doit, en vue d'offrir un maximum de souplesse tout en maintenant un niveau de sécurité et de confiance élevé, mettre en place un système libre d'agréation et donner la possibilité aux AC de demander une agréation qui varie en fonction des personnes et attributs qu'elles désirent certifier. En outre, elle doit consacrer certains principes de base tels que le droit pour tout citoyen de continuer à utiliser sa signature manuscrite et de choisir l'AC à laquelle il compte s'adresser.

Une réglementation de la certification doit également, à l'instar de celle qui est relative à la signature, demeurer ouverte aux développements technologiques. Elle devrait essentiellement fixer le statut des autorités de certification ainsi que les droits et obligations des différents acteurs.

Concernant tout d'abord le statut des autorités de certification, les principes suivants devraient être respectés :

[90] Y. POULLET, *op.cit.*, 1996, p. 52.

- garanties : toute AC doit disposer des moyens nécessaires pour assurer sa fonction de certification (indépendance, sécurité, garanties financières, interopérabilité, transparence des tarifs) sans qu'interfèrent des intérêts politiques, commerciaux, industriels ou financiers particuliers[91] ;
- agréation libre : afin de répondre aux besoins existants et de n'asphyxier ni l'activité de certification ni le commerce électronique, des AC agréées et non agréées doivent pouvoir coexister sur le marché ;
- agréation variable : toute AC peut demander une agréation plus ou moins étendue en fonction des personnes ou des attributs qu'elle entend certifier.

En ce qui concerne les obligations incombant aux autorités de certification, elles sont surtout conditionnées par la nature particulière des activités exercées. Dans le cadre de réseaux ouverts, la signature est appelée à jouer seule la fonction d'identification alors que dans le cadre contractuel traditionnel, la signature n'était "guère l'élément le plus important, ni même l'élément déterminant dans l'identification du cocontractant"[92]. Les autorités de certification se voient donc reconnaître une mission spécifique qui transcende l'activité de renseignement pour s'apparenter à celle exercée par les officiers publics. Il apparaît, dès lors, indispensable que l'étendue de leurs obligations soit clairement définie par la loi. A ce propos, différents éléments devraient être pris en considération :

- l'AC doit présenter des garanties de sécurité suffisantes pour exercer ses activités (elle doit notamment adopter les mesures nécessaires pour assurer la confidentialité de sa clé privée) ;
- l'AC est tenue de procurer toute information nécessaire à l'utilisation correcte et sûre de ses services ;
- l'AC doit s'engager à ce que les informations véhiculées par le certificat soient exactes, actuelles et complètes
- enfin, l'AC doit demeurer le seul interlocuteur en cas de litige relatif à un certificat émis sous son autorité.

Diverses obligations pèsent également sur les utilisateurs de services. En effet, le titulaire de certificat est tenu de fournir des informations exactes à l'AC, de préserver la confidentialité de sa clé privée et, le cas échéant, de faire procéder à la suspension ou à la révocation du certificat. Le destinataire d'un message signé digitalement doit, quant à lui, vérifier la signature au moyen du certificat correspondant et s'assurer que celui-ci n'est pas expiré, suspendu ou révoqué.

Enfin, si l'on désire que la réglementation sur la certification revête un intérêt pratique, il est indispensable de permettre non seulement la certification des personnes physiques mais également la certification des personnes morales afin de s'orienter vers la reconnaissance de la signature des personnes morales[93].

**Mireille Antoine et Didier Gobert**
**Chercheurs au CRID**
**Assistant à la Faculté de droit de Namur**

[91] Voir à ce sujet ce qui est dit à propos de l'implantion d'une infrastructure de certification au Québec, S. PARISIEN, P. TRUDEL, *op.cit.*, p. 187.

[92] D. G. MASSE, "L'autoroute de l'information : convergence du droit et de la technologie", F*aire des affaires en toute sécurité sur les autoroutes de l'information,* Actes du colloque du 10 novembre 1995, http://www.droit.umontreal;ca/A...loque_10_11_95/Masse/aqd95.html,p.7.

[93] Commission des Nations Unies pour le Droit Commercial International, *op. cit.*, 12 mars 1997, p.29.