Nations Unies A/CN.9/630/Add.1

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 nécessaires à l'élaboration d'un cadre juridique favorable au commerce électronique: chapitre type sur l'utilisation internationale des méthodes d'authentification et de signature électroniques

Note du secrétariat*

Additif

L'annexe de la présente note contient une partie (première partie, chapitre premier, sections B et C) d'un chapitre type d'un document de référence général qui traite des aspects juridiques de l'utilisation internationale des méthodes d'authentification et de signature électroniques.

* Note présentée en retard par le secrétariat de la Commission des Nations Unies pour le droit commercial international pour cause de sous-effectif.

V.07-82781 (F) 070607 080607

Annexe

Table des matières

Première partie

Méthodes d'authentification et de signature électroniques

[...]

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

[...]

B. Principales méthodes d'authentification et de signature électroniques

1. Aux fins du présent document, quatre méthodes principales d'authentification et de signature électroniques seront examinées: les signatures numériques, les méthodes biométriques, les mots de passe et les méthodes hybrides, et les signatures scannées ou saisies au clavier.

1. Signatures numériques fondées sur la cryptographie à clef publique

2. La "signature numérique" désigne des applications technologiques qui utilisent la cryptographie asymétrique, autrement dit un système de chiffrement à clef publique, pour garantir l'authenticité de messages électroniques et l'intégrité de leur contenu. La signature numérique peut prendre de multiples formes, telles que la signature avec arrêt sur défaillance, la signature aveugle et la signature indéniable.

a) Notions et terminologie techniques

i) Cryptographie

3. Les signatures numériques sont créées et vérifiées grâce à la cryptographie, branche des mathématiques appliquées qui s'occupe de la transformation de messages en des formes apparemment inintelligibles et de leur restitution dans leur forme initiale. Les signatures numériques utilisent ce que l'on appelle la "cryptographie à clef publique", qui est souvent basée sur l'utilisation de fonctions algorithmiques pour créer deux "clefs" (c'est-à-dire des nombres de plusieurs chiffres générés à l'aide d'une série de formules mathématiques appliquées aux nombres premiers) différentes mais mathématiquement liées entre elles[1]. L'une de ces clefs est utilisée pour créer une signature numérique ou pour transformer des données en une forme apparemment inintelligible, et l'autre pour vérifier une signature numérique ou restituer le message dans sa forme initiale[2]. Le matériel et le

---

[1] On notera, cependant, que le concept de cryptographie à clef publique, tel qu'il est examiné ici, ne nécessite pas forcément l'utilisation d'algorithmes fondés sur des nombres premiers. On utilise ou l'on met au point actuellement d'autres techniques mathématiques telles que des systèmes de cryptographie fondés sur des courbes elliptiques, souvent décrits comme offrant un niveau élevé de sécurité grâce à l'utilisation de longueurs de clefs considérablement réduites.

[2] Bien que le recours à la cryptographie soit l'une des principales caractéristiques des signatures

logiciel informatiques utilisant deux clefs de ce type sont souvent appelés collectivement “cryptosystèmes” ou, plus précisément, “cryptosystèmes asymétriques” lorsqu’ils utilisent des algorithmes asymétriques.

ii) Clefs publiques et privées

4. Une clef complémentaire utilisée pour les signatures numériques est appelée la “clef privée”, qui n’est utilisée que par le signataire pour créer la signature numérique et qui doit être tenue secrète, tandis que la “clef publique” est d’ordinaire plus largement connue et est utilisée par une partie se fiant à la signature pour vérifier la signature numérique. La clef privée est normalement conservée sur une carte à mémoire, ou est accessible grâce à un numéro d’identification personnel (NIP) ou grâce à un dispositif d’identification biométrique, par exemple un dispositif de reconnaissance d’empreinte de pouce. Si plusieurs personnes ont besoin de vérifier les signatures numériques du signataire, il faut rendre la clef publique accessible ou la distribuer à l’ensemble de ces personnes, en attachant, par exemple, les certificats à la signature ou par d’autres moyens permettant de s’assurer que les parties se fiant aux signatures, et uniquement celles qui doivent vérifier les signatures, aient accès aux certificats correspondants. Bien que les clefs de la paire soient mathématiquement liées, si un système de cryptographie asymétrique a été conçu et mis en œuvre de façon sécurisée, il est pratiquement impossible, connaissant la clef publique, de déduire la clef privée. Les algorithmes les plus courants de chiffrement par utilisation de clefs publiques et privées reposent sur une caractéristique importante des grands nombres premiers: une fois multipliés ensemble pour produire un nouveau nombre, il est particulièrement difficile et long de déterminer les deux nombres premiers qui ont créé ce nouveau nombre plus important[3]. Ainsi, bien que de nombreuses personnes connaissent la clef publique d’un signataire donné et l’utilisent pour vérifier les signatures de ce signataire, elles ne peuvent découvrir la clef privée de ce signataire et l’utiliser pour falsifier des signatures numériques.

---

numériques, le simple fait qu’une signature numérique soit utilisée pour authentifier un message contenant des données sous forme numérique ne doit pas être assimilé à l’utilisation plus générale de la cryptographie à des fins de confidentialité. Le codage pour raison de confidentialité est une méthode utilisée pour coder une communication électronique de manière que seuls l’initiateur et le destinataire du message seront en mesure de le lire. Dans un certain nombre de pays, la loi restreint l’utilisation de la cryptographie à cette fin pour des raisons d’ordre public qui peuvent comporter des considérations de défense nationale. Cependant, l’utilisation de la cryptographie aux fins d’authentification par la création d’une signature numérique n’implique pas nécessairement le recours au codage pour garantir le caractère confidentiel d’une communication, étant donné que la signature numérique codée peut être tout simplement jointe à un message non codé.

[3] Certaines normes existantes contiennent la notion d’“irréalisabilité informatique” pour décrire l’irréversibilité escomptée du processus, c’est-à-dire l’espoir qu’il sera impossible de déduire la clef privée secrète d’un utilisateur à partir de sa clef publique. “Irréalisable par des moyens informatiques” est un concept relatif fondé sur la valeur des données protégées, l’infrastructure informatique requise pour les protéger, le temps nécessaire pour les protéger, ainsi que le coût et le temps nécessaires pour attaquer les données, ces facteurs étant évalués tant en fonction de la situation actuelle que des futurs progrès technologiques.” (American Bar Association, *Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce* (Chicago, Association du barreau américain, 1er août 1996), p. 9, note 23, disponible à http://www.abanet.org/scitech/ec/isc/dsgfree.html, visité le 5 avril 2007).

iii) Fonction de hachage

5. Outre la production de paires de clefs, un autre processus fondamental, généralement appelé “fonction de hachage”, est utilisé à la fois pour créer et pour vérifier une signature numérique. Une fonction de hachage est un processus mathématique fondé sur un algorithme, qui crée une représentation numérique, ou forme comprimée du message, souvent appelée “abrégé” ou “empreinte digitale”, et qui prend la forme d’une “valeur de hachage” ou d’un “résultat de hachage” d’une longueur normalisée généralement bien plus courte que le message lui-même mais qui lui est néanmoins unique. Toute modification apportée au message produit inévitablement un résultat de hachage différent lorsqu’on utilise la même fonction de hachage. Dans le cas d’une fonction de hachage sécurisée, parfois appelée “fonction de hachage unidirectionnelle”, il est pratiquement impossible, connaissant la valeur de hachage, de déduire le message initial. Une autre caractéristique fondamentale des fonctions de hachage est qu’il est également pratiquement impossible de trouver un autre objet binaire (c’est-à-dire différent de celui qui a produit l’abrégé à l’origine) qui produira le même abrégé. Les fonctions de hachage permettent donc au programme de création de signatures numériques d’opérer sur des volumes de données limités et plus prévisibles tout en établissant une solide corrélation avec la teneur du message initial, ce qui lui permet d’assurer qu’aucune modification n’a été apportée au message depuis que ce dernier a été signé sous forme numérique.

iv) Signature numérique

6. Pour signer un document ou toute autre information, le signataire commence par définir précisément les limites de ce qu’il doit signer. Ensuite, une fonction de hachage opérant dans le programme du signataire calcule un résultat de hachage propre (à toutes fins pratiques) à l’information qui doit être signée. Le programme du signataire transforme ensuite le résultat de hachage en une signature numérique à l’aide de la clef privée du signataire. La signature numérique résultante est par conséquent propre à la fois à l’information signée et à la clef privée utilisée pour créer la signature numérique. Généralement, une signature numérique (chiffrement, avec la clef privée du signataire, du résultat de hachage du message) est attachée au message et stockée ou transmise avec ce message. Cependant, elle peut également être envoyée ou stockée comme élément de données distinct, aussi longtemps qu’elle maintient une association fiable avec le message correspondant. Étant donné qu’une signature numérique est propre à son message, elle est inutilisable si on la dissocie de façon permanente dudit message.

v) Vérification de la signature numérique

7. La vérification de la signature numérique consiste à vérifier la signature numérique par rapport au message initial et à une clef publique donnée, et à déterminer de cette façon si la signature numérique a été créée pour ce même message à l’aide de la clef privée correspondant à la clef publique référencée. La vérification d’une signature numérique s’effectue en calculant un nouveau résultat de hachage du message initial au moyen de la fonction de hachage utilisée pour créer la signature numérique. Ensuite, à l’aide de la clef publique et du nouveau résultat de hachage, le contrôleur vérifie si la signature numérique a été créée à l’aide de la clef privée correspondante et si le résultat de hachage nouvellement

calculé correspond au résultat de hachage initial qui a été transformé en signature numérique au cours du processus de signature.

8. Le programme de vérification confirmera la signature numérique comme étant "vérifiée" du point de vue cryptographique: a) si la clef privée du signataire a été utilisée pour signer numériquement le message, ce qui est avéré si la clef publique du signataire a été utilisée pour vérifier la signature étant donné que la clef publique du signataire permettra de vérifier uniquement une signature numérique créée à l'aide de la clef privée du signataire; et b) si le message ne subit aucune modification, ce qui est avéré si le résultat de hachage calculé par la personne chargée de la vérification est identique au résultat de hachage extrait de la signature numérique lors du processus de vérification.

vi) Autres utilisations de la technologie des signatures numériques

9. Comme indiqué plus haut, l'utilisation de la technologie des signatures numériques va bien au-delà de la simple "signature" de communications électroniques à la façon des signatures manuscrites utilisées pour signer des documents (voir par. [...]). Ainsi, des certificats signés numériquement sont souvent utilisés, par exemple, pour "authentifier" des serveurs ou des sites Internet, afin de garantir à leurs utilisateurs que le serveur ou le site en question est bien celui qu'il prétend être, ou est bien relié à la société qui prétend le gérer. Cette technologie peut aussi être utilisée pour "authentifier" des logiciels informatiques, par exemple pour garantir l'authenticité d'un logiciel téléchargé d'un site Internet, ou garantir qu'un serveur donné utilise une technologie largement reconnue comme offrant un certain niveau de sécurité de connexion, ou pour "authentifier" toute autre donnée qui est diffusée ou sauvegardée sous forme numérique.

b) Infrastructure à clef publique et prestataires de services de certification

10. Pour vérifier une signature numérique, le vérificateur doit avoir accès à la clef publique du signataire et s'assurer que celle-ci correspond bien à la clef privée du signataire. Cependant, une paire de clefs publique et privée n'a aucune association intrinsèque avec une personne quelconque; il s'agit simplement d'une paire de nombres. Un mécanisme supplémentaire est nécessaire pour associer de manière fiable une personne ou une entité particulière à la paire de clefs. Cela est très important, car il se peut qu'il n'y ait aucune relation de confiance préexistante entre le signataire et les destinataires de communications signées numériquement. Pour ce faire, les parties concernées doivent avoir confiance dans les clefs publiques et privées émises.

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

régie par un droit particulier. De plus, il faudrait tenir compte du fait que, si des différends doivent être réglés par un tribunal ou par arbitrage, il pourrait être difficile de prouver qu'une certaine clef publique avait, ou n'avait pas, été effectivement donnée au destinataire par son propriétaire.

12. Un signataire éventuel pourrait faire une déclaration publique indiquant que les signatures vérifiables au moyen d'une clef publique donnée devraient être considérées comme provenant de lui. La forme et l'efficacité juridique d'une telle déclaration seraient régies par la loi de l'État adoptant. Par exemple, une présomption d'attribution de signatures électroniques à un signataire particulier pourrait être établie par la publication de la déclaration dans un bulletin officiel ou dans un document reconnu comme "authentique" par les autorités publiques. Cependant, d'autres parties pourraient refuser d'accepter cette déclaration, en particulier lorsqu'il n'existe aucun contrat préalable établissant avec certitude l'effet juridique de ladite déclaration. Une partie se fiant à une telle déclaration non étayée publiée dans un système ouvert courrait alors un risque important de faire confiance, à son insu, à un imposteur ou d'avoir à établir qu'il n'y a pas eu refus de signature numérique (question souvent évoquée à propos de la "non-répudiation" des signatures numériques) dans les cas où une transaction s'avérerait défavorable pour le signataire supposé.

13. Une solution à certains de ces problèmes consiste à recourir à un ou plusieurs tiers de confiance pour associer un signataire identifié ou le nom de ce signataire à une clef publique spécifique. Ce tiers de confiance est généralement appelé, dans la plupart des normes et directives techniques, "autorité de certification" ou "prestataire de services de certification" (dans la Loi type de la CNUDCI sur les signatures électroniques[4], c'est l'expression "prestataire de services de certification" qui a été retenue). Dans plusieurs pays, ces autorités de certification s'organisent de façon hiérarchique en ce que l'on appelle souvent une infrastructure à clef publique (ICP), dans laquelle certaines autorités de certification ne font qu'en certifier d'autres, qui fournissent directement des services aux utilisateurs. Dans une telle structure, certaines autorités de certification sont donc subordonnées à d'autres, mais on peut aussi concevoir des structures dans lesquelles toutes sont sur un pied d'égalité. Dans une grande ICP, il est probable qu'il y aura à la fois des autorités de certification subordonnées et supérieures. D'autres solutions comprennent, par exemple, les certificats délivrés par les parties se fiant à la signature.

i) Infrastructure à clef publique

14. La création d'une ICP est un moyen d'inspirer confiance dans le fait que: a) la clef publique de l'utilisateur n'a pas été falsifiée et correspond effectivement à sa clef privée; b) les techniques de cryptologie utilisées sont bonnes. Pour inspirer cette confiance, une ICP peut offrir un certain nombre de services, dont les suivants: a) gérer les clefs cryptographiques utilisées pour les signatures numériques; b) certifier qu'une clef publique correspond bien à une clef privée; c) fournir des clefs aux utilisateurs finaux; d) publier des informations relatives à la révocation des clefs publiques ou des certificats; e) gérer des objets personnalisés (par exemple des cartes à puce) capables d'identifier l'utilisateur au moyen d'éléments d'identification qui lui sont spécifiques ou capables de créer et de garder en

[4] Voir note [...] [publication des Nations Unies, numéro de vente: F.02.V.8].

mémoire les clefs privées d'un individu; f) vérifier l'identité des utilisateurs finaux et leur offrir des services; g) offrir des services d'horodatage; et h) gérer les clefs cryptographiques utilisées pour le chiffrement de confidentialité lorsque le recours à cette technique est autorisé.

15. Une ICP peut s'appuyer sur divers niveaux d'autorité. Par exemple, les modèles envisagés dans certains pays pour établir ce type d'infrastructure se réfèrent notamment aux niveaux suivants: a) une autorité principale ("autorité racine") unique, qui certifierait la technologie et les pratiques de toutes les parties autorisées à produire les paires de clefs cryptographiques ou les certificats concernant l'utilisation de ces paires de clefs, et qui enregistrerait les autorités de certification inférieures[5]; b) diverses autorités de certification, situées en dessous de "l'autorité racine", qui certifieraient que la clef publique d'un utilisateur correspond effectivement à sa clef privée (autrement dit, que la clef n'a pas été manipulée); et c) diverses autorités locales d'enregistrement, placées en dessous des autorités de certification, qui recevraient les demandes de paires de clefs cryptographiques ou de certificats relatifs à l'utilisation de ces paires de clefs adressées par des utilisateurs, exigeant une preuve d'identification et vérifiant l'identité des utilisateurs éventuels. Dans certains pays, il est envisagé de confier à des officiers publics la fonction d'autorité locale d'enregistrement, ou tout au moins de leur demander d'apporter leur concours à cette fonction.

16. Les ICP structurées de manière hiérarchique sont modulables, en ce sens qu'elles peuvent incorporer de nouvelles "communautés" ICP entières en chargeant simplement l'"autorité racine" d'établir une relation de confiance avec la "racine" de la nouvelle communauté[6]. L'autorité racine de la nouvelle communauté peut être incorporée directement sous la "racine" de l'ICP réceptrice et devenir un prestataire de services de certification subordonné au sein de cette ICP. Elle peut aussi devenir un prestataire de services de certification subordonné à l'un des prestataires de services de certification dans l'ICP existante. Une autre caractéristique attrayante des ICP hiérarchiques est qu'elles facilitent le développement de chemins de certification, parce qu'elles fonctionnent uniquement dans un sens, du certificat de l'utilisateur au point de confiance. De plus, les chemins de certification au sein d'une ICP hiérarchique sont relativement courts, et les utilisateurs savent implicitement, à partir de la position occupée par le prestataire de services de certification, pour quelles applications un certificat peut être utilisé. Toutefois, les ICP hiérarchiques ont également des inconvénients, du fait surtout qu'elles s'appuient sur un seul point de confiance. Si l'autorité racine est compromise, c'est toute l'ICP qui l'est. En outre, certains pays ont eu des difficultés à choisir une seule entité en tant qu'autorité racine et à imposer cette hiérarchie à tous les autres prestataires de services de certification[7].

---

[5] La question de savoir si un gouvernement devrait avoir la capacité technique de conserver ou de recréer des clefs de confidentialité privées peut être traitée au niveau de l'autorité racine.

[6] William T. Polk et Nelson E. Hastings, *Bridge Certification Authorities: Connecting B2B Public Key Infrastructures*, Institut national américain des normes et de la technologie (septembre 2000), peut être consulté à http://csrc.nist.gov/pki/documents/B2B-article.pdf, visité le 30 mars 2007.

[7] Polk et Hastings (voir note [6]) notent qu'aux États-Unis, il a été très difficile de choisir une agence du gouvernement fédéral pour assumer l'autorité générale de l'ICP fédérale.

17. L'ICP dite "maillée" est une alternative à l'ICP hiérarchique. Dans ce modèle, les prestataires de services de certification sont liés par une relation de pair à pair. Tous peuvent être des points de confiance. En général, les utilisateurs feront confiance à ceux qui ont émis leur certificat. Les prestataires de services de certification s'adressent mutuellement des certificats. La paire de certificats représente leur relation de confiance mutuelle. Du fait de l'absence de hiérarchie dans un tel système, les prestataires de services de certification ne peuvent imposer les conditions régissant les types de certificats émis par d'autres prestataires. Si un prestataire souhaite limiter la confiance accordée à d'autres prestataires, il doit préciser ces limites dans les certificats émis pour ses pairs[8]. Toutefois, il peut être très difficile d'harmoniser les conditions et les limites de la reconnaissance mutuelle.

18. Une troisième structure est l'architecture de l'autorité de certification dite en "pont". Elle peut être particulièrement utile pour permettre à plusieurs communautés ICP existantes de se fier aux certificats les unes des autres. Contrairement à une autorité de certification dans une ICP "maillée", une autorité de certification "pont" n'émet pas directement de certificats aux utilisateurs. Elle n'a pas non plus pour vocation de servir de point de confiance aux utilisateurs de l'ICP, comme c'est le cas d'une autorité "racine". En revanche, une autorité de certification "pont" établit des relations de confiance de pair à pair avec les différentes communautés d'utilisateurs, ce qui permet à ces derniers de conserver leurs points de confiance naturels au sein de leur ICP respective. Si une communauté d'utilisateurs instaure un domaine de confiance sous la forme d'une ICP hiérarchique, l'autorité de certification "pont" établira une relation avec l'autorité racine de cette ICP. Par contre, si elle instaure un domaine de confiance sous la forme d'une ICP "maillée", l'autorité de certification "pont" devra uniquement établir une relation avec l'une des autorités de certification de l'ICP, qui deviendra alors l'autorité "principale" de certification au sein de cette ICP en vue de l'établissement du "pont de confiance" avec l'autre ICP. Le "pont de confiance" qui relie deux ICP ou plus par le biais de leur relation mutuelle avec une autorité de certification "pont" permet aux membres des différentes communautés d'utilisateurs d'interagir les uns avec les autres pour un niveau de confiance donné[9].

ii) Prestataires de services de certification

19. Pour associer une paire de clefs à un signataire éventuel, un prestataire de services de certification (ou autorité de certification) délivre un certificat, enregistrement électronique qui indique la clef publique ainsi que le nom du titulaire du certificat identifié comme "sujet" de ce certificat et qui peut confirmer que le signataire éventuel identifié dans le certificat détient la clef privée correspondante. La fonction essentielle d'un certificat est d'associer une clef publique à un signataire précis. Un "destinataire" du certificat souhaitant se fier à une signature numérique créée par le signataire indiqué dans le certificat peut utiliser la clef publique figurant dans le certificat pour vérifier que la signature numérique a bien été créée avec la clef privée correspondante. Si cette vérification est positive, le

---

[8] Polk et Hastings, *Bridge Certification Authorities* ... (voir note [5]).

[9] L'autorité de certification "pont" est la structure qui a finalement été retenue pour le système ICP du Gouvernement fédéral des États-Unis (Polk et Hastings, voir note [6]). C'est également le modèle suivi pour développer le système ICP du Gouvernement japonais.

destinataire est dans une certaine mesure techniquement assuré que le signataire a créé la signature numérique et que la portion du message utilisé pour la fonction de hachage (et, par conséquent, le message de données correspondant) n'a pas été modifiée depuis qu'on y a apposé la signature numérique.

20. Pour assurer l'authenticité du certificat (pour ce qui est tant de son contenu que de sa source), le prestataire de services de certification y appose une signature numérique. Celle-ci peut être vérifiée au moyen de la clef publique de ce prestataire figurant sur un autre certificat délivré par un autre prestataire (qui peut, mais ne doit pas nécessairement, être une autorité hiérarchiquement supérieure), et cet autre certificat peut à son tour être authentifié par la clef publique figurant sur un autre certificat encore, et ainsi de suite, jusqu'à ce que la personne devant se fier à la signature numérique soit convaincue de son authenticité. Un autre moyen possible de vérifier une signature numérique consiste à enregistrer cette signature numérique sur un certificat délivré par le prestataire de services de certification (parfois appelé "certificat source")[10].

21. Dans chaque cas, le prestataire de services de certification délivrant le certificat doit apposer une signature numérique sur son propre certificat pendant la période de validité de l'autre certificat utilisé pour vérifier sa signature numérique. Selon la législation de certains États, on pourrait inspirer la confiance dans la signature numérique du prestataire de services de certification en publiant dans un bulletin officiel la clef publique de celui-ci ou certaines données se rapportant au certificat source (par exemple une "empreinte digitale numérique").

22. Une signature numérique correspondant à un message, qu'elle soit créée par le signataire pour authentifier un message ou par le prestataire de services de certification pour authentifier son certificat, devrait généralement être horodatée de manière fiable pour permettre au vérificateur de déterminer si elle a bien été créée pendant la "période de validité" indiquée dans le certificat, et avant tout si le certificat était valable (par exemple ne figurait pas sur une liste de révocation) au moment considéré, ce qui est l'une des conditions de la vérifiabilité d'une signature numérique.

23. Pour qu'une clef publique et son association à un signataire spécifique soient aisément vérifiables, le certificat peut être publié dans un répertoire ("repository") ou mis à disposition par d'autres moyens. Généralement, les répertoires sont des bases de données en ligne regroupant des certificats et d'autres informations pouvant être appelés et utilisés pour vérifier les signatures numériques.

24. Une fois délivré, un certificat peut se révéler sujet à caution, par exemple si le signataire a donné une fausse identité au prestataire de services de certification. Dans d'autres cas, un certificat peut être fiable au moment où il est délivré, mais devenir sujet à caution par la suite. Si la clef privée est "compromise", par exemple parce que son signataire en a perdu le contrôle, le certificat peut perdre sa fiabilité. Le prestataire de services de certification (à la demande du signataire ou même sans son consentement, selon les circonstances) peut alors suspendre (interrompre provisoirement la période de validité) ou révoquer (annuler définitivement) le certificat. On peut attendre du prestataire de services de certification que, peu après

[10] *Documents officiels de l'Assemblée générale, cinquante-sixième session, Supplément n° 17* et rectificatif (A/56/17 et Corr.3), par. 279.

cette suspension ou cette révocation, il publie une notification ou en avise les personnes qui l'interrogent ou dont il sait qu'elles ont reçu une signature numérique vérifiable par référence à un certificat qui n'est pas fiable. De même, le cas échéant, on devrait également examiner s'il y a eu révocation du certificat du prestataire de services de certification, ainsi que du certificat émis pour la vérification de la signature de l'autorité d'horodatage et du certificat du prestataire de services de certification qui a émis le certificat de l'autorité d'horodatage.

25. Les autorités de certification pourraient être des organismes relevant de l'État ou des prestataires de services privés. Dans quelques pays, on envisage, pour des raisons d'ordre public, que seuls des organismes publics soient autorisés à assurer la fonction de certification. Toutefois, dans la plupart des pays, ou bien les services de certification sont entièrement laissés au secteur privé, ou bien les organismes gérés par l'État coexistent avec des prestataires de services privés. Il y a aussi des systèmes de certification fermés, dans lesquels de petits groupes établissent leur propre prestataire de services de certification. Dans certains pays, les organismes relevant de l'État émettent uniquement des certificats à l'appui des signatures numériques utilisées par l'administration publique. Quelle que soit l'option retenue, et que les autorités de certification aient ou non besoin d'une licence pour fonctionner, une infrastructure à clef publique comprend généralement plusieurs prestataires de services de certification. Ce qui est particulièrement important est la relation entre les différentes autorités de certification (voir par. [15] à [18] ci-dessus).

26. Il peut incomber au prestataire de services de certification ou à l'autorité racine de veiller à ce que ses prescriptions soient systématiquement respectées. Si la sélection des autorités de certification peut se faire sur la base d'un certain nombre de facteurs, dont la solidité de la clef publique utilisée et l'identité de l'utilisateur, la fiabilité d'un prestataire de services de certification peut également dépendre de la façon dont il applique les normes de délivrance de certificats et de la fiabilité de son évaluation des données communiquées par les utilisateurs qui demandent des certificats. D'une importance toute particulière est le régime de responsabilité qui s'applique concernant le respect des prescriptions en matière de politique générale et de sécurité édictées par l'autorité racine ou par le prestataire de services de certification supérieur, ou de toute autre prescription applicable, et ce, de manière permanente. L'obligation du prestataire de services de certification d'agir en conformité avec les déclarations qu'il a faites en ce qui concerne ses politiques et pratiques, comme prévu à l'alinéa a) du paragraphe 1 de l'article 9 de la Loi type sur les signatures électroniques, est tout aussi importante.

c) Problèmes pratiques dans la mise en œuvre de l'infrastructure à clef publique

27. En dépit des connaissances considérables sur les technologies de signature numérique et leur mode de fonctionnement, la mise en œuvre des systèmes d'infrastructure à clef publique et de signature numérique a, dans la pratique, connu quelques problèmes qui ont modéré l'utilisation des signatures numériques, restée en deçà des attentes.

28. Les signatures numériques fonctionnent bien lorsqu'il s'agit de vérifier des signatures créées pendant la période de validité d'un certificat. Mais, une fois que le certificat a expiré ou été révoqué, la clef publique correspondante perd sa validité, même si la paire de clefs n'était pas compromise. Par conséquent, il faudrait un

système de gestion des signatures numériques pour les systèmes d'ICP afin de garantir la disponibilité de la signature dans le temps. La principale difficulté provient du risque que le document électronique "original" (c'est-à-dire les chiffres binaires ou "bits" qui constituent le fichier informatique dans lequel l'information est enregistrée), y compris la signature numérique, devienne illisible ou peu fiable avec le temps, en raison principalement de l'obsolescence du logiciel, du matériel ou des deux. En fait, la signature numérique peut devenir peu sûre en raison des progrès scientifiques en matière d'analyse cryptographique, le logiciel de vérification des signatures peut ne pas être disponible sur de longues périodes ou le document peut perdre son intégrité[11]. Il en résulte que la conservation à long terme des signatures électroniques est généralement problématique. Même si on a cru pendant un certain temps que les signatures numériques étaient indispensables à des fins d'archivage, l'expérience a montré qu'elles n'étaient pas à l'abri des risques à long terme. Comme toute altération du document, après la création de la signature, entraînera l'échec de la vérification de cette dernière, les opérations de reformatage destinées à préserver la lisibilité d'un document (comme la "migration" ou la "conversion") peuvent affecter la durabilité de la signature[12]. En fait, les signatures numériques ont été conçues davantage pour assurer la sécurité de la communication d'informations que pour préserver les informations dans le temps[13]. Les initiatives visant à résoudre ce problème n'ont pas encore débouché sur une solution durable[14].

---

[11] Jean-François Blanchette, "Defining electronic authenticity: an interdisciplinary journey", peut être consulté à http://polaris.gseis.ucla.edu/blanchette/papers/dsn.pdf, visité le 5 avril 2007 (document publié dans un volume supplémentaire de la Conférence internationale sur la sûreté de fonctionnement des systèmes et des réseaux (DSN 2004), Florence (Italie), 28 juin-1er juillet 2004), p. 228 à 232.

[12] "En fin de compte, tout ce que nous pouvons préserver dans un contexte électronique sont les bits. Toutefois, nous savons depuis longtemps qu'il est très difficile de conserver une série de bits indéfiniment. Avec le temps, elle devient illisible (pour l'ordinateur et, partant, pour l'homme) en raison de l'obsolescence technologique du logiciel d'application et/ou du matériel (par exemple le lecteur). Jusqu'à présent, le problème de la durabilité des signatures numériques fondées sur une ICP a été mal étudié en raison de sa complexité. ... Bien que les outils d'authentification utilisés dans le passé, comme les signatures manuscrites, les sceaux, les tampons, les empreintes digitales, etc. soient également sujets au reformatage (par exemple le microfilm) en raison de l'obsolescence du support papier, ils ne deviennent jamais complètement inutilisables après une telle opération. Il y a toujours au moins une copie qui peut être comparée avec d'autres outils d'authentification d'origine." (Jos Dumortier et Sofie Van den Eynde, *Electronic Signatures and Trusted Archival Services*, p. 5, peut être consulté à http://www.law.kuleuven.ac.be/icri/publications/172DLM2002.pdf?where=, visité le 5 avril 2007.

[13] En 1999, des archivistes de différents pays ont lancé le projet InterPARES (Recherche Internationale sur les Documents Authentiques Permanents dans les Systèmes Électroniques) pour "accroître les connaissances théoriques et méthodologiques essentielles à la conservation à long terme de documents authentiques créés et/ou conservés sous forme numérique" (voir http://www.interpares.org, visité le 5 avril 2007). Le projet de rapport du groupe de travail sur l'authenticité, qui faisait partie de la première phase du projet (InterPARES 1, achevée en 2001) concluait que "les signatures numériques et les infrastructures à clef publique (ICP) étaient des exemples de technologies développées et mises en œuvre pour authentifier des documents électroniques transmis d'un endroit à un autre. Même si les archivistes et les informaticiens ont confiance dans les technologies d'authentification pour garantir l'authenticité des documents, ces technologies n'ont jamais été destinées, et n'en ont pas l'aptitude à l'heure actuelle, à assurer l'authenticité de documents électroniques dans la durée" (non souligné dans le texte), peut être consulté à http://www.interpares.org/documents/atf_draft_final_report.pdf, visité le

29. Un autre domaine dans lequel les systèmes de signature numérique et d'ICP peuvent poser des problèmes pratiques est celui de la sécurité des données et de la protection de la vie privée. Les prestataires de services de certification doivent garder en sécurité les clefs utilisées pour signer les certificats émis en faveur de leurs clients et risquent d'être exposés à des tentatives de tiers visant à obtenir un accès non autorisé à ces clefs (voir également la deuxième partie, par. [...] à [...] ci-dessous). De plus, ils doivent obtenir une série de données personnelles et d'informations commerciales des personnes qui demandent un certificat. Ces informations doivent être conservées en vue d'une utilisation ultérieure. Les prestataires de services de certification doivent prendre les mesures nécessaires pour que l'accès à ces informations soit conforme aux lois applicables en matière de

---

5 avril 2007. Le rapport final d'InterPARES 1 peut être consulté à http://www.interpares.org/book/index.htm. La suite du projet (InterPARES 2) a pour objectif de développer et d'élaborer des concepts, des principes, des critères et des méthodes pour la création et la préservation de documents exacts et fiables et la conservation à long terme de documents authentiques dans le contexte des activités artistiques, scientifiques et gouvernementales menées entre 1999 et 2001.

[14] L'Initiative européenne de normalisation des signatures électroniques (EESSI), par exemple, a été créée en 1999 par le Conseil de normalisation des TIC, groupe d'organisations s'occupant conjointement de la normalisation et des activités connexes dans les technologies de l'information et de la communication, établi afin de coordonner les activités de normalisation à l'appui de la mise en œuvre de la directive de l'Union européenne sur les signatures électroniques (voir note [...] [Journal officiel des communautés européennes, L 13/12]). Le consortium EESSI (initiative de normalisation qui s'emploie à traduire les exigences de la directive européenne sur les signatures électroniques en normes européennes) a cherché à répondre au besoin de la conservation à long terme de documents à signature cryptographique au moyen de sa norme sur le "format de signature électronique" (norme TS 101 733, ETSI, 2000). Le format distingue des étapes dans la validation de la signature, la validation initiale et une validation ultérieure. Le format de cette dernière réunit toutes les informations qui peuvent être utilisées dans le processus de validation, comme les informations relatives à la révocation, l'horodatage, les politiques de signature, etc. Ces informations sont réunies lors de l'étape de la validation initiale. Les concepteurs de ce format de signature électronique étaient préoccupés par la menace que faisait peser le déclin de la force cryptographique sur la validité de la signature. Pour lutter contre cette menace, les signatures EESSI sont régulièrement horodatées à nouveau, avec des algorithmes de signature et des tailles de clef adaptées aux méthodes d'analyse cryptographique les plus récentes. Le problème de la longévité des logiciels a été traité dans un rapport de l'EESSI datant de 2000, qui introduisait les "opérateurs fiables de services d'archivage", nouveau type de service commercial qui serait proposé par des professions et des organes compétents qui restent à définir, afin de garantir la conservation à long terme de documents à signature cryptographique. Le rapport énumère un certain nombre d'exigences techniques auxquelles ces opérateurs devraient satisfaire, dont la "compatibilité rétroactive" avec les logiciels et le matériel informatiques, par la conservation de l'équipement et/ou par l'émulation (voir Blanchette, "Defining electronic authenticity ..." (voir note [12])). Une étude complémentaire sur la recommandation de l'EESSI relative aux opérateurs fiables de services d'archivage réalisée par le Centre interdisciplinaire pour le droit et les technologies de l'information de l'Université catholique de Louvain, Belgique, intitulée *European Electronic Signature Standardization Initiative: Trusted Archival Services* (phase 3, rapport final, 28 août 2000), peut être consultée à http://www.law.kuleuven.ac.be/icri/publications/91TAS-Report.pdf?where=, visité le 12 avril 2007. L'EESSI a été arrêtée en octobre 2004. Les systèmes permettant d'appliquer ces recommandations ne semblent pas être opérationnels à l'heure actuelle (voir Dumortier et Van den Eynde, *Electronic Signatures and Trusted Archival Services* (voir note [13]).

protection des données[15]. Malgré tout, la menace d'un accès non autorisé reste bien réelle.

2. Biométrie

30. Un identificateur biométrique est une mesure utilisée pour identifier une personne par ses caractéristiques physiques ou comportementales. Les caractéristiques susceptibles d'être utilisées pour la reconnaissance biométrique sont l'ADN, les empreintes digitales, l'iris, la rétine, la forme de la main ou du visage, la thermographie faciale, la forme de l'oreille, la voix, l'odeur corporelle, le dessin des vaisseaux sanguins, l'écriture, la démarche et la dynamique de frappe.

31. Le recours à des dispositifs biométriques implique en général de prélever un échantillon biométrique d'une caractéristique biologique d'une personne. Cet échantillon est numérisé, puis des données biométriques en sont extraites pour créer un modèle de référence. Par la suite, les données enregistrées dans ce modèle sont comparées avec celles qui proviennent de l'utilisateur final à des fins de vérification, ce qui permet d'indiquer si une identification ou une vérification d'identité a été possible[16].

32. Les dispositifs biométriques ont par nature des propriétés uniques qui doivent être prises en considération. L'existence de ces propriétés qui peuvent, dans une certaine mesure, différer de la caractéristique choisie comme référence, a des incidences importantes sur l'adéquation de la technologie à l'utilisation envisagée.

33. La conservation des données biométriques comporte un certain nombre de risques, car, en général, les caractéristiques biométriques ne peuvent être contestées. Lorsque des systèmes biométriques ont été compromis, l'utilisateur légitime n'a pas d'autre choix que d'abandonner les données d'identification et d'en adopter un autre ensemble, non compromis. Des règles spéciales sont donc nécessaires pour empêcher l'utilisation abusive des bases de données biométriques.

---

[15] Voir les Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel (Paris, 1980), disponibles à http://www.oecd.org/document/0,2340,fr_2649_34255_1815225_1_1_1_1,00.html, visité le 7 février 2007; la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Conseil de l'Europe, *Série des traités européens* n° 108), disponible à http://conventions.coe.int/treaty/FR/Treaties/Html/108.htm, visité le 7 février 2007; les Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel (résolution 45/95 de l'Assemblée générale), disponibles à http://www.unhchr.ch/french/html/menu3/b/71_fr.htm, visité le 7 février 2007; et la Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 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 (*Journal officiel des communautés européennes*, L 281, 23 novembre 1995), disponible à http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:FR:HTML, visité le 7 février 2007.

[16] *Glossaire de termes biométriques* (1999) de l'International Association for Biometrics (Association internationale de biométrie) et de l'International Computer Security Association (Association internationale de sécurité informatique), peut être consulté à http://www.afb.org.uk/docs/glossary.htm, visité le 7 février 2007.

34. L'exactitude des techniques biométriques ne peut être absolue, car les caractéristiques biologiques tendent par essence à être variables, et toute mesure peut comporter un écart. À cet égard, les données biométriques ne sont pas considérées comme des identificateurs uniques, mais plutôt semi-uniques. Pour tenir compte de ces variations, on peut jouer sur l'exactitude des données en fixant le seuil de correspondance entre le modèle de référence et l'échantillon prélevé. Toutefois, un seuil bas risque d'introduire une distorsion dans le sens de fausses acceptations et un seuil élevé de favoriser les faux rejets. Cela dit, l'exactitude de l'authentification fournie par la biométrie peut être suffisante dans la majorité des applications commerciales.

35. D'autre part, la conservation et la divulgation des données biométriques suscitent des questions concernant la protection des données et les droits de l'homme. Bien qu'elles ne se réfèrent peut-être pas expressément à la biométrie, les lois sur la protection des données[17] ont pour objectif de protéger les données des personnes physiques dont le traitement, qu'il s'agisse des données brutes ou de modèles, est au cœur de la technologie biométrique[18]. De plus, des mesures peuvent être requises pour protéger les consommateurs contre les risques découlant de l'utilisation privée des données biométriques, ainsi qu'en cas de vol d'identité. D'autres domaines juridiques, notamment le droit du travail et de la santé, peuvent également entrer en ligne de compte[19].

36. Des solutions techniques pourraient aider à répondre à certaines préoccupations. Par exemple, la conservation de données biométriques sur des cartes à puce ou des jetons peut prévenir un accès non autorisé, qui pourrait se produire si les données sont stockées dans un système informatique centralisé. De plus, des pratiques optimales ont été mises au point pour réduire les risques dans différents domaines tels que le champ d'application et les capacités, la protection des données, le contrôle de l'utilisation des données personnelles, et la divulgation, la vérification, la responsabilité et la surveillance[20].

37. On considère généralement que les dispositifs biométriques offrent un niveau élevé de sécurité. Bien qu'ils soient compatibles avec de nombreuses applications, ils sont surtout utilisés actuellement par les gouvernements, en particulier dans le domaine de la sécurité, notamment pour les vérifications en matière d'immigration et les contrôles d'accès.

---

17 Voir note [15].

18 Paul de Hert, *Biométrie: questions et incidences juridiques* – document d'information pour l'Institute for Prospective Technological Studies de la Commission européenne (Communautés européennes, Direction générale du Centre commun de recherche, 2005), p. 13, peut être consulté à http://cybersecurity.jrc.es/docs/LIBE%20Biometrics%20March%2005/LegalImplications_Paul_de_Hert.pdf.

19 Au Canada, par exemple, l'utilisation de la biométrie a été examinée en relation avec la mise en œuvre de la Loi sur la protection des renseignements personnels et les documents électroniques (2000, ch. 5) sur le lieu de travail (voir *Turner c. TELUS Communications Inc.*, 2005 CF 1601, 29 novembre 2005 (Cour fédérale du Canada)).

20 Pour un exemple de pratiques optimales, voir l'initiative de l'International Biometric Group sur la biométrie et la vie privée, "Best practices for privacy-sympathetic biometric deployment", disponible à http://www.bioprivacy.org.

38. Des applications commerciales ont aussi vu le jour, où la biométrie est souvent utilisée dans le contexte d'un processus d'authentification à double facteur, qui exige la fourniture d'un élément en possession de la personne (identificateur biométrique) et d'un élément en sa connaissance (généralement un mot de passe ou un PIN). En outre, des applications ont été mises au point pour enregistrer et comparer les caractéristiques d'une signature manuscrite. Des tablettes graphiques basées sur la technologie numérique enregistrent la pression du stylet et la durée du processus de signature. Ces données sont ensuite conservées sous la forme d'un algorithme utilisé pour comparer les signatures futures. Toutefois, en raison des caractéristiques inhérentes à la biométrie, la prudence est de mise face aux dangers d'un renforcement progressif et non contrôlé de son utilisation dans les opérations commerciales courantes.

39. Le remplacement des signatures manuscrites par des signatures biométriques risque de poser un problème de preuve. Comme il a été indiqué plus haut, la fiabilité des preuves biométriques varie en fonction de la technologie utilisée et du taux de fausses acceptations choisi. De plus, il est possible de manipuler ou de falsifier les données biométriques enregistrées sous forme numérique.

40. Les critères généraux de fiabilité prévus dans les Lois types de la CNUDCI sur les signatures électroniques[21] et sur le commerce électronique[22], de même que dans la Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux[23], plus récente, peuvent s'appliquer à l'utilisation des signatures biométriques. Dans un souci d'uniformité, il pourrait également être utile d'élaborer des lignes directrices internationales relatives à l'utilisation et à la gestion des méthodes biométriques[24]. Il faut toutefois examiner avec soin si de telles normes seraient ou non prématurées, compte tenu de l'état d'avancement actuel des technologies biométriques, et si elles risqueraient ou non d'en compromettre le développement continu.

3. Mots de passe et méthodes hybrides

41. Mots de passe et codes sont utilisés à la fois pour contrôler l'accès à des informations ou à des services et pour "signer" des communications électroniques. Dans la pratique, cette deuxième utilisation est moins fréquente que la première, en raison du risque de compromettre le code s'il est transmis dans un message non codé. Toutefois, les mots de passe et les codes sont la méthode d'authentification la plus utilisée pour les contrôles d'accès et la vérification de l'identité dans de nombreuses opérations, y compris pour la plupart des opérations bancaires en ligne,

---

21 Voir note [...] [publication des Nations Unies, numéro de vente F.02.V.8].

22 Voir note [...] [publication des Nations Unies, numéro de vente F.99.V.4].

23 La version finale de la Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux a été établie par la CNUDCI à sa trente-huitième session (Vienne, 4-15 juillet 2005) et officiellement adoptée par l'Assemblée générale le 23 novembre 2005 (résolution 60/21 de l'Assemblée générale, annexe). Elle peut être consultée à l'adresse http://www.uncitral.org/uncitral/fr/uncitral_texts/electronic_commerce/2005Convention.html.

24 Celles-ci pourraient être comparées aux critères de fiabilité présentés dans le Guide pour l'incorporation de la Loi type de la CNUDCI sur les signatures électroniques (voir note [...] publication des Nations Unies, numéro de vente: F.02.V.8), par. 75).

les retraits d'espèces aux guichets automatiques et les transactions par carte de crédit.

42. Il faut savoir que de multiples technologies peuvent être utilisées pour "authentifier" une transaction électronique. On peut recourir à plusieurs technologies ou à plusieurs utilisations d'une même technologie pour une seule transaction. Par exemple, la dynamique de la signature à des fins d'authentification peut être combinée avec la cryptographie pour garantir l'intégrité du message. Une autre possibilité consiste à communiquer des mots de passe sur Internet au moyen de la cryptographie (par exemple SSL dans les navigateurs) pour les protéger, et à utiliser en même temps la biométrie pour déclencher une signature numérique (cryptographie asymétrique) qui, à réception, génère un ticket Kerberos (cryptographie symétrique). L'élaboration de cadres généraux et juridiques pour traiter ces technologies devrait tenir compte du rôle des technologies multiples. Pour ce qui est de l'authentification électronique, de tels cadres devront être assez souples pour couvrir les solutions fondées sur des technologies hybrides, car des cadres axés sur des technologies spécifiques pourraient entraver l'utilisation de technologies multiples[25]. Des dispositions technologiquement neutres faciliteraient l'acceptation de telles solutions.

4. Signatures scannées et noms saisis au clavier

43. Le droit privé s'est surtout intéressé au commerce électronique en raison de l'influence que pourraient avoir les nouvelles technologies sur l'application de règles de droit conçues pour d'autres moyens de communication. Cet intérêt pour la technologie a souvent conduit, délibérément ou non, à mettre l'accent sur des technologies perfectionnées offrant un niveau élevé de sécurité pour les méthodes d'authentification et de signature électroniques. Dans ce contexte, on oublie souvent qu'une grande partie, sinon la majorité, des communications commerciales échangées dans le monde ne font appel à aucune technologie particulière d'authentification ou de signature.

44. Dans la pratique quotidienne, les entreprises du monde entier se contentent souvent, par exemple, d'échanges de courriers électroniques sans autre forme d'authentification ou de signature que le nom saisi au clavier, le titre et l'adresse des parties figurant à la fin du message. Parfois, elles recourent à une présentation plus formelle au moyen de fac-similés ou d'images scannées de signatures manuscrites qui, cela va de soi, ne sont qu'une copie numérisée d'un original manuscrit. Ni des noms saisis dans un courrier électronique non chiffré ni des signatures scannées n'offrent un niveau élevé de sécurité ou ne peuvent prouver avec certitude l'identité de l'auteur des communications électroniques dans lesquelles ils apparaissent. Néanmoins, les entités commerciales choisissent librement d'utiliser ces formes d'authentification pour des raisons de facilité, de rapidité et d'économie des communications. Il est important que les législateurs et les responsables politiques aient à l'esprit ces pratiques commerciales répandues lorsqu'ils envisagent de

---

[25] Foundation for Information Policy Research, *Signature Directive Consultation Compilation*, 28 octobre 1998, document qui fournit une compilation des réponses apportées au cours des consultations sur le projet de directive de l'Union européenne sur les signatures électroniques, établi à la demande de la Commission européenne. Peut être consulté à www.fipr.org/publications/sigdirecon.html, visité le 12 avril 2007.

réglementer les méthodes d'authentification et de signature électroniques. Des exigences strictes en la matière, notamment l'imposition d'une méthode ou technologie particulière, pourraient par inadvertance jeter des doutes sur la validité et la force obligatoire d'un nombre important de transactions réalisées tous les jours sans l'utilisation d'une méthode particulière d'authentification ou de signature. Cela risque, par conséquent, d'inciter les parties de mauvaise foi à éviter les conséquences d'obligations qu'elles ont librement contractées en remettant en cause l'authenticité de leurs propres communications électroniques. Il n'est pas réaliste de penser que l'imposition d'un niveau élevé d'exigences en matière d'authentification et de signature, conduirait, à terme, toutes les parties à les utiliser au quotidien. Des expériences menées récemment avec des méthodes sophistiquées, telles que les signatures numériques, ont montré que les préoccupations de coût et de complexité mettaient souvent un frein à l'utilisation, dans la pratique, de techniques d'authentification et de signature.

C. Gestion de l'identité électronique*

45. À l'ère de l'électronique, les personnes physiques ou morales peuvent accéder aux services d'un certain nombre de fournisseurs. Chaque fois qu'une personne s'inscrit à cette fin auprès de l'un d'entre eux, une "identité" électronique est créée. Par ailleurs, une identité unique peut être reliée à un certain nombre de comptes pour chaque application ou plate-forme. La multiplication des identités et de leurs comptes peut en compliquer la gestion, pour l'utilisateur comme pour le prestataire de services. Ces difficultés pourraient être évitées si chaque personne avait une seule identité électronique.

46. L'inscription d'une personne auprès d'un prestataire de services et la création d'une identité électronique entraînent l'établissement d'une relation de confiance mutuelle entre cette personne et le prestataire. La création d'une identité électronique unique suppose que l'on regroupe toutes ces relations bilatérales dans un cadre plus large où elles pourraient être gérées globalement, dans ce que l'on appelle un système de gestion de l'identité. Les avantages de la gestion de l'identité peuvent être, pour le fournisseur, une sécurité accrue, une plus grande facilité de respecter les règlements et une plus grande souplesse commerciale et, pour l'utilisateur, un accès facilité à l'information.

47. La gestion de l'identité peut donner lieu à deux approches: le paradigme traditionnel de l'accès utilisateur (connexion), qui repose sur une carte à puce avec des données que le client utilise pour se connecter à un service, et le paradigme de services, plus novateur, qui fournit des services personnalisés aux utilisateurs et à leurs dispositifs.

48. La première approche se concentre sur l'administration de l'authentification de l'utilisateur, les droits et restrictions d'accès, les profils des comptes, les mots de passe et autres attributs dans un ou plusieurs systèmes ou applications. Elle vise à faciliter et contrôler l'accès aux applications et aux ressources tout en protégeant les données personnelles et commerciales confidentielles vis-à-vis d'utilisateurs non autorisés.

* Cette section serait développée dans une version finale du document de référence général.

49. Avec la seconde, la gestion de l'identité a une portée plus vaste et comprend toutes les ressources de l'entreprise servant à fournir des services en ligne, comme l'équipement réseau, les serveurs, les portails, le contenu, les applications et les produits, de même que le justificatif d'identité, les carnets d'adresses, les préférences et les droits d'un utilisateur. Dans la pratique, elle pourrait inclure par exemple des informations sur les paramètres du contrôle parental et la participation à des programmes de fidélité.

50. On s'emploie actuellement à développer la gestion de l'identité à la fois dans le monde des affaires et au niveau gouvernemental. Il faut toutefois noter que les grands choix, dans les deux scénarios, peuvent différer considérablement. L'approche gouvernementale visera peut-être plutôt à mieux répondre aux besoins des citoyens et penchera davantage vers l'interaction avec des personnes physiques, alors que les applications commerciales doivent tenir compte de l'utilisation croissante de machines automatisées dans les transactions commerciales et choisiront peut-être des caractéristiques destinées à répondre aux besoins spécifiques de ces machines.

51. Parmi les difficultés liées aux systèmes de gestion de l'identité figurent les questions de confidentialité, en raison des risques associés à l'utilisation abusive d'identificateurs uniques. En outre, des questions peuvent également se poser du fait des différences entre les règlements juridiques applicables, notamment pour ce qui est de la possibilité de déléguer le pouvoir d'agir pour le compte d'autrui. On a suggéré des solutions reposant sur une coopération commerciale volontaire fondée sur ce que l'on appelle le cercle de confiance, où les participants doivent se fier à l'exactitude et à la précision des informations qui leur sont fournies par d'autres membres du cercle. Cette approche ne suffira toutefois peut-être pas pour réglementer toutes les questions connexes et l'adoption d'un cadre juridique pourra rester nécessaire[26]. Des lignes directrices ont également été élaborées, qui prévoient des prescriptions juridiques pour les cercles d'infrastructures de confiance[27].

52. S'agissant de l'interopérabilité technique, l'Union internationale des télécommunications a établi un groupe spécialisé sur la gestion de l'identité, pour faciliter et promouvoir l'établissement d'un cadre générique pour la gestion de l'identité et les moyens d'identifier des identités distribuées de façon autonome et des fédérations d'identités[28].

---

[26] Voir *Modinis Study on Identity Management in eGovernment: Identity Management Issue Report* (Commission européenne, Direction générale société de l'information et médias, juin 2006), p. 9 à 12, disponible à https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/pub/Main/ProjectDocs/modinis.D3.9_Identity_Management_Issue_Interim_Report_II1.pdf.

[27] Le Liberty Alliance Project (voir www.projectliberty.org) est une alliance mondiale qui regroupe plus de 150 entreprises, organisations à but non lucratif et agences gouvernementales. Le consortium tente de développer une norme ouverte d'identité de réseau fédéré prenant en charge tous les périphériques de réseau actuels et futurs. L'identité fédérée offre aux entreprises, aux gouvernements, aux employés et aux consommateurs un moyen plus pratique et plus sécurisé de contrôler les paramètres d'identité dans l'économie numérique d'aujourd'hui, ce qui en fait un élément essentiel dans la mise en œuvre du cybercommerce, de services de données personnalisés et de services Web. L'adhésion est ouverte à toutes les organisations commerciales et non commerciales.

[28] Voir http://www.itu.int/ITU-T/studygroups/com17/fgidm/index.html.

53. Des solutions de gestion de l'identité sont également apportées dans le contexte de l'administration en ligne. Ainsi, dans le cadre de la stratégie de l'Union européenne "i2010: une société de l'information pour la croissance et l'emploi", une étude sur la gestion de l'identité dans l'administration en ligne a été lancée pour encourager les progrès vers l'adoption d'une approche cohérente en la matière dans l'Union européenne, sur la base des connaissances et des initiatives existantes dans les États membres de l'Union européenne[29].

54. La distribution de dispositifs de signature électronique, qui prennent souvent la forme de cartes à puce, se répand de plus en plus dans le contexte du gouvernement en ligne. Des opérations de distribution à l'échelle nationale de cartes à puce ont été lancées, entre autres, en Belgique[30] et en Estonie. Avec ces initiatives, un très grand nombre de citoyens reçoivent des dispositifs permettant notamment de sécuriser des signatures électroniques à un coût faible. Bien que l'objectif premier de ces initiatives ne soit peut-être pas commercial, de tels dispositifs peuvent également être utilisés dans un environnement commercial. On reconnaît de plus en plus la convergence de ces deux domaines d'application[31].

---

[29] Voir https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi.

[30] Voir http://eid.belgium.be/en/navigation/12000/index.html.

[31] Voir, par exemple, le *Livre blanc coréen sur Internet* (Séoul, Agence nationale coréenne de développement d'Internet, 2006), p. 81, qui se réfère à la double utilisation, dans le gouvernement en ligne et dans le commerce électronique, de la loi sur les signatures électroniques de la République de Corée, disponible à http://www.ecommerce.or.kr/activities/documents_view.asp?bNo=642&Page=1.