Quelle(s) certification(s) pour la signature électronique ?

Les procédés de signature électronique sont destinés à constituer une brique fondamentale de la confiance dans la société de l'information. La Communauté européenne a publié le 13 décembre 1999 une directive en vue d'instaurer un cadre juridique favorable à leur diffusion, dont la souplesse témoigne du souci de ne pas brider la créativité des marchés. Or les métiers liés à la signature électronique sont complexes, tant du point de vue technique que du point de vue organisationnel, notamment parce que des techniques de sécurité très fiables et certains garde-fous doivent être mis en place. La mise en place d'un schéma de certification sera délicate à organiser.

par Frédéric Tatout
Ingénieur principal de l'Armement, Digitip

En pratique, une signature, quel que soit le procédé utilisé pour la créer (stylo, tampon ou procédé électronique), doit être considérée en regard de plusieurs éléments, en particulier la personne qui la produit (le signataire), la circonstance (lieu, profession, parties d'un contrat signé, le type de relation entre ces parties, etc.) et son objectif (document signé) (1). Compte tenu de la variété de ces éléments et des droits applicables, toute définition de la signature ne peut que rester très générale. De même, en cas de contestation, tous ces éléments sont susceptibles d'entrer en ligne de compte dans l'appréciation du juge. Par exemple, la Cour de New York a émis un jugement pouvant donner à un simple fax, mentionnant le nom de l'émetteur à son entête, une valeur contractuelle (2).

Or, la signature électronique s'appuie sur des techniques nouvelles, puissantes et complètement automatisables (cf. la figure 1, qui explique un procédé fondamental pour la signature électronique), et créera une multitude de nouveaux usages (cf. encadré). Elle vient donc modifier en profondeur le difficile équilibre entre le droit et la pratique, façonné par des siècles de pratique et par la jurisprudence. C'est dire toute la difficulté, pour les professionnels du droit, à créer un cadre juridique pour la signature électronique : un véritable défi !

Défi pourtant incontournable parce que les échanges électroniques sont destinés à devenir prépondérants dans notre vie. Il ne pouvait être question de laisser se développer sur ce sujet une zone de « non droit » nuisible au progrès. *A contrario*, créer un droit spécifique pour les usages électroniques revenait à prendre le risque de créer une société schizophrène, dans laquelle les per-

(1) Par exemple, le Code uniforme du commerce des Etats-Unis dispose que « l'insertion de tout symbole créé ou adopté par une partie avec l'intention d'authentifier un écrit comme provenant de cette partie », constitue une signature.
(2) Parma Tile Mosaic & Marble Co. v. Estate of Fred Short, 590 NYS2d 1019 (N.Y. Sup. Ct. 1992).

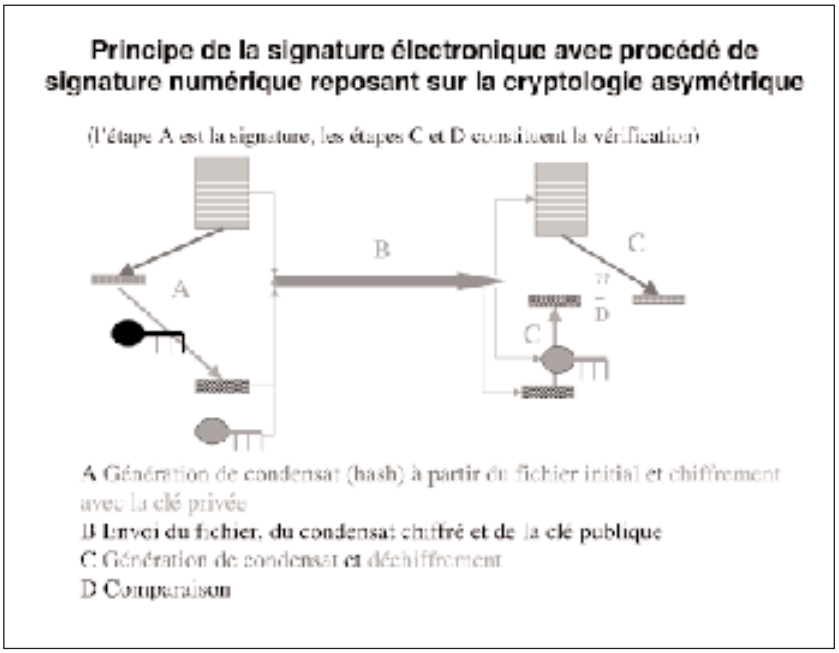

Fig. 1. - Nota : la signature électronique qui accompagne un écrit sous forme électronique peut garantir à la fois l'identité du signataire et l'intégrité de l'écrit tel qu'il a été signé. Il est donc possible en théorie d'avoir une preuve plus « forte » que la signature manuscrite.

sonnes auraient une vie « virtuelle » et une vie réelle.

De multiples projets d'encadrement juridique, un développement moins rapide que prévu

La création d'un cadre juridique de la signature électronique se généralise, avec notamment :
- en Europe, une directive publiée le 13 décembre 1999,
- aux Etats-Unis, un texte fondateur encensé par le Président Bill Clinton (6), publié en 2000,
- au Japon, une loi publiée en 2000.

Au niveau international la loi-type de la CNUDCI (7) augure d'une généralisation à l'échelle mondiale. Visant à la neutralité, elle repose à la fois sur une analogie fonctionnelle et une association entre des critères techniques et des responsabilités,

Le retard industriel de l'Europe dans le domaine des infrastructures à clés publiques ne l'a pas empêchée de prendre une certaine avance sur les Etats-Unis dans la mise en place d'un cadre juridique. De plus, son rôle dans l'élaboration de la loi-type CNUDCI a été déterminant. Cependant, on constate que la transposition au niveau national de la directive est lente (8), tandis que la Commission tarde à réunir le fameux comité article 9. Le marché de la signature électronique et de la certification électronique n'a toujours pas décollé en Europe.

Sans vouloir recenser les causes de cette baisse de dynamisme, il apparaît que les acteurs ont pris conscience que la signature électronique est difficile à mettre en œuvre : nous assistons à une phase d'intégration au marché des nouvelles technologies que sont les IGCP.

Les obstacles à ce développement

Un premier type de difficulté repose sur l'ambiguïté fondamentale entre ce que permettent les techniques de signature électronique – garantir l'identité de l'émetteur d'un écrit électronique et l'intégrité de cet écrit – et l'autonomie des personnes, à savoir notamment :
- Délégation de signature : faut-il permettre aux personnes de s'échanger des dispositifs de création de signature afin de déléguer leurs pouvoirs, par exemple, en cas d'absence, et si on ne peut pas en faire l'économie, comment gérer cet échange ?
- Non-répudiation : quelle force donner à la non-répudiation, sachant que dans ce cas un malfaiteur qui prendrait le contrôle sur le moyen de signature aurait la possibilité de créer des nuisances bien plus graves qu'en imitant une signature manuscrite ?
- Respect de la vie privée et des libertés fondamentales : quelle limite à l'identification en ligne et quelle place laissée à l'anonymat ? Comment gérer les pseudonymes ?

Un second type de difficulté, qui nous intéresse ici tout particulièrement, est lié à l'utilisation de technologies non matures pour mettre en œuvre certaines techniques de cryptologie réputées inviolables, par exemple :
- l'ordinateur personnel présente de multiples failles de sécurité, donc l'utilisateur n'aura jamais l'assurance absolue de contrôler ce qu'il signe – cette assurance dépendra du prix qu'il est prêt à payer, ainsi que des efforts et de la science d'éventuels fraudeurs ;
- les standards ne sont pas mûrs, y compris en ce qui concerne les dispositifs permettant de créer la signature ;
- la chaîne de confiance a ses limites puisque nul ne devrait être tenu de faire confiance à un certificat vérifié en ligne : l'image qu'un utilisateur voit à l'écran pourrait être contrefaite par une combinaison, certes très sophistiquée, de techniques et de logiciels insérés dans son ordinateur à son insu (ce risque est réduit si l'utilisateur protège bien son ordinateur).

Cryptologie et usages de la signature électronique

Techniquement la cryptologie moderne est un élément central de la signature électronique. De manière plus générale, elle est un acteur clé du développement de la confiance au sein d'un espace virtuel public, le Web, ouvert et de surcroît dominé par des principes de neutralité et de liberté des échanges (3). Comment ? En permettant d'installer une sécurité dans les échanges et les transactions, de créer des frontières et une intimité virtuelle, bref, une vie ressemblant à celle, familière, d'un village avec ses places publiques, ses marchés et ses lieux privés.

La cryptologie asymétrique figure tout en haut de l'affiche pour créer des signatures électroniques. Technique récente, puissante (4) et élégante, elle a suscité un certain engouement (5), à présent très affaibli, pour les infrastructures de gestion de clés publiques – IGCP, en anglais PKI, *Public Key Infrastructures* – et de fortes attentes des utilisateurs, peut-être un peu déçues face aux difficultés de mise en œuvre, mais entièrement justifiées compte tenu de ses applications, par exemple :

organiser des processus de décision et de conception incluant les droits de propriété intellectuelle, sous forme de workflow,

créer des actes notariés électroniques, avec une date elle-même signée,

créer des archives de durée de conservation théoriquement indéfinie,

mettre en œuvre une traçabilité complète et sûre dans le transport, l'alimentaire, etc.

Actuellement la tendance est de mettre en sourdine le discours sur les technologies par rapport aux usages et aux fonctions, ce qui traduit un important processus d'intégration.

(3) Ces principes peuvent bien entendu être modulés localement, mais ils restent dominants compte tenu de la suprématie et de l'activisme des Etats-Unis, qui les prônent.

(4) Sa solidité repose sur des preuves mathématiques, donc inattaquables sauf en cas d'une révolution dans ce domaine, et elle offre une grande flexibilité.

(5) En particulier, les Etats-Unis et le Canada se sont lancés avec enthousiasme dans une politique de grands projets dans ce domaine, ce qui a donné naissance à des géants industriels que sont VeriSign, RSA, Baltimore et Entrust, fervents évangélistes de cette nouvelle technologie.

(6) A cette occasion, Bill Clinton a comparé le rôle de la signature électronique pour le développement de la société de l'information au rail pour la Conquête de l'Ouest.

(7) La loi-type a été finalisée le 17 juillet 2001 à Vienne.

(8) Rappelons que la directive fixait le 19 juillet 2001 comme date limite de la transposition.

Un troisième type de difficulté provient de la complexité du processus de signature électronique certifiée par un certificat électronique. Le processus global de la certification électronique repose sur plusieurs étapes : enregistrement du titulaire puis création, signature, gestion et révocation de certificats électronique. Ces tâches peuvent être partagées entre plusieurs entités : par exemple, une Autorité d'enregistrement (AE) chargée de vérifier l'identité au vu de pièces d'identité et d'un contact face à face, afin de constituer des fichiers informatiques ; un organisme pour la création, la gestion et la révocation des certificats ; et une Autorité de certification (AC), chargée de coordonner ces activités et passer un contrat de service aux utilisateurs (elle endosse donc la responsabilité globale face aux utilisateurs).

En définitive, compte tenu de ces difficultés, il serait déraisonnable à l'heure actuelle d'utiliser sa souris pour signer un contrat d'achat ou de vente d'une maison par exemple (9). En outre, l'articulation complexe entre risque théorique (10) et risque avéré (11) peut brouiller la notion de sécurité et de confiance en l'absence d'un dialogue entre les utilisateurs, les fournisseurs de service et les éventuelles autorités de régulation et de contrôle.

La Directive européenne et sa transposition en France : quelques repères pour la confiance

En instituant des critères de validité et des principes de responsabilité, la directive du 13 décembre 1999 vise, en quelque sorte, à créer un îlot de relative certitude au milieu de cet océan de complexité. Ses grands principes sont les suivants :

- une signature électronique ne peut pas être refusée en justice au motif qu'elle est sous forme électronique (art 5.1) ;
- une signature électronique, sous réserve que soient vérifiés un certain nombre de critères exposés dans les annexes, présente les mêmes garanties formelles que la signature manuscrite sur papier (art 5.2). Dans ce cas, il est établi un principe de responsabilité qui désigne, en particulier, l'AC comme seule responsable vis-à-vis de l'utilisateur, avec toutefois certaines limites, car un régime protégeant l'utilisateur ne doit pas pour autant le décharger de toutes ses responsabilités ;
- un encadrement spécifique est prévu concernant deux composants clés : la ressource cryptographique permettant au prestataire de signer des certificats électroniques (art 3.5) et surtout le dispositif sécurisé de création de signature électronique, dont la conformité « est déterminée par les organismes compétents, publics ou privés, désignés par les États membres » (art 3.4).

Ces principes sont complétés par un régime obligatoire de supervision *a posteriori* (contrôle, art. 3.3), doublé de la possibilité, pour les états membres, de mettre en place un régime *volontaire* d' « accréditation » (12) (art 3.2) des prestataires de services de certification (en abrégé par la suite : PSC). Il ne s'agit pas ici de créer un système d'encadrement strict, mais plutôt de *donner confiance aux marchés* : les pays sont libres dans la manière de l'organiser, moyennant toutefois que les critères soient « transparents, proportionnés et non discriminatoires » (cette nuance limite considérablement cette liberté en pratique).

En France, la loi du 13 mars 2000 (code civil) et le décret du 30 mars 2001 transposent la majeure partie de la directive : seul le régime de responsabilité des prestataires reste en suspens (13) ; transposition relativement fidèle, les seules particularités notables étant les suivantes :

- la signature répondant à l'article 5.1 de la directive est présumée fiable (14) ;
- les prestataires dont la qualification est reconnue dans le cadre prévu par le décret du 30 mars 2001 sont présumés répondre à ses critères.

La transposition nationale institue donc un double niveau de présomption.

Eu égard à la mise en place d'un régime volontaire de certification, certains États comme le Danemark, la Norvège et la Finlande, l'estiment inutile vu la taille de leur marché intérieur (15). Les régimes mis en place ou en construction s'appuient généralement sur une architecture à deux étages : accréditation par une entité de type COFRAC, certification des prestataires de services liés à la signature électronique par les organismes accrédités, avec un encadrement administratif plus ou moins strict (16). Ils se fonderont tous – mais pas forcément de manière exclusive – sur des documents en cours d'élaboration au CEN et à l'ETSI, destinés à être publiés au Journal officiel de la Communauté européenne (JOCE).

Quel peut être le rôle d'une certification ?

Une certification des PSC peut viser notamment à donner aux utilisateurs l'assurance d'un niveau de fiabilité et de sécurité des prestataires de certification et du système global, à créer une meilleure transparence, et à promouvoir le libre échange des services en Europe et au-delà.

Notons que le dernier de ces trois objectifs, rappelé avec insistance par le texte de la directive, repose effectivement sur la constitution de jalons de confiance pour les utilisateurs en ce qui concerne l'équivalence des certificats. Or, le droit peut difficilement se substituer, du point de vue de la confiance des utilisateurs, à des accords de reconnaissance que les prestataires passeront entre eux. A cette fin les éléments à prendre en compte ne doivent pas se limiter à l'interopérabilité technique mais s'étendre à la gestion des services et voir la finalité de ces services (comment est utilisée la signature électro-

(9 Mais rassurons-nous : un acheteur potentiel pourra y songer seulement après que le second décret d'application de la loi du 13 mars 2000, relatif aux actes notariés, aura été publié avec d'autres textes ministériels.

(10) C'est-à-dire tel que l'on peut le percevoir par une analyse *a priori* (étude de failles et de vulnérabilités).

(11) C'est-à-dire connu à travers l'expérience des sinistres survenus et des menaces actives.

(12) C'est le terme de la directive, qu'il faut entendre en réalité comme une certification.

(13) C'était prématuré dans la loi et cela ne peut pas être fait par décret.

(14) Dans la logique du code civil, c'était logique parce que d'un point de vue technique elle atteste non seulement de l'identité du signataire mais aussi de l'intégrité de l'écrit.

(15) Mais la Finlande par exemple collecte une taxe sur les certificats pour financer des activités de supervision.

(16) Le régime est complètement privé en Grande-Bretagne et en Irlande ; un encadrement plus ou moins souple existe ou existera en Italie, Belgique, France et Allemagne, par exemple.

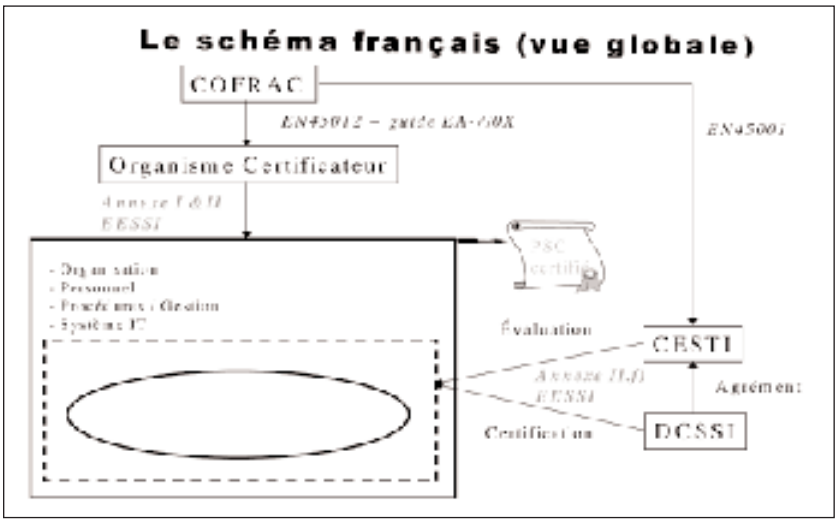

Figure 2.

nique), afin de pouvoir estimer les risques qui en découlent. D'où un intérêt, sur un plan théorique, à ce que la certification aille au-delà de la technique, sans pour autant empiéter sur la créativité commerciale des prestataires. En France, le double niveau de présomption de la transposition renforce les effets juridiques de la signature qualifiée avec un certificat garanti par un PSC. De ce fait, le schéma national de certification qui sera mis en place apportera peut-être une contribution significative au développement de la confiance dans l'usage de la signature électronique, mais ce sera au prix d'une attention soutenue de tous les acteurs en ce qui concerne leur part de responsabilité.

Le schéma national de certification en vue de la reconnaissance de la qualification

Ce schéma est conforme au principe de la directive selon lequel la constitution d'une chaîne de confiance, présentant un bon niveau de sécurité pour l'utilisateur, repose sur la mise en œuvre, au sein d'un système organisé et géré de manière adéquate, de certains équipements clés de confiance visés à son article 3.4. Ce principe, s'il reflète l'état de l'art au moment de l'élaboration de la directive, n'est peut-être pas absolu et n'exclut pas que d'autres procédés de très bonne qualité, bien que n'y répondant pas, voient le jour (la valeur de tels procédés s'exprimera à travers l'expérience que l'on en aura).

L'art 3.4 de la directive dispose que la conformité des équipements clés procède d'une certification délivrée par des organismes compétents. Dans les pays possédant une tradition forte en cryptologie, notamment la Grande-Bretagne, l'Allemagne, la Hollande, l'Italie et la France, la certification de la sécurité des produits et systèmes, qui constitue un enjeu de souveraineté et reste organisée par l'Etat. L'article 3.4 de la directive prévoit en conséquence que les États membres désigneront le(s) organisme(s) compétents. Dans le cas de la France, cette certification repose à la fois sur un schéma d'accréditation par le COFRAC et un agrément des organismes d'évaluation par la DCSSI, seule habilitée à délivrer un certificat (cf. partie droite du schéma global, graphique 2).

A ce propos il faut noter que, suite à des années d'efforts d'harmonisation, des accords de reconnaissance importants ont pu être passés entre plusieurs pays européens, dont la France, en ce qui concerne l'évaluation Critères Communs selon la norme ISO 15 408. Mais le droit reste muet par rapport à ce patrimoine européen, la directive renvoyant à des documents publiés au JOCE. Or, ces documents, élaborés par EESSI (17) font référence essentiellement aux critères fédéraux américains, du fait que les produits actuellement disponibles sur le marché sont évalués aux Etats-Unis ; et il se trouve qu'aucun laboratoire européen n'est habilité à certifier des produits de sécurité selon ces critères. Il y a là un risque de dépendance pour l'Europe, qui disparaîtra avec la mise sur le marché de produits de signature électronique certifiés selon la norme ISO 15 408.

La certification de la manière dont sont mis en œuvre des équipements de confiance reposera sur une procédure de type audit exercée par des organismes eux-mêmes accrédités par le COFRAC (cf. la partie centrale du schéma global). Cette procédure est donc « classique », l'accréditation s'appuyant sur la norme NF EN 45012 de mai 1998 (18), qui sera complétée par le document EA – 07/01 (19). Cependant il faut noter que l'évaluation de la sécurité d'un système d'information complexe comme celui d'un PSC requiert une analyse différente, plus poussée que l'audit d'un système qualité. Le COFRAC devra donc sans doute lancer un programme spécifique afin que ses auditeurs puissent mieux prendre en compte les spécificités liées à la sécurité des systèmes d'information. Ils s'appuieront notamment sur les spécification ISMS (sécurité des systèmes d'information) (20).

Normes et documents applicables pour la certification

Aucune norme ou document normatif ne paraît pouvoir être appliqué tel quel :

- par rapport aux PSC, des guides existent, notamment X9-79, le référentiel du programme *WebTrust for CA*, un guide de l'*American Bar Association*. Ils sont insuffisants compte tenu de l'objectif recherché et du double niveau de présomption du droit français. Des schémas nationaux ont été mis en place

(17) EESSI : European Electronic Signature Standardisation initiative (cf. infra).

(18) C'est la version française du guide ISO/CEI 62, qui vise la certification ISO 90xx (assurance qualité).

(19) Ces documents sont en cours de refonte, consulter le site d'EA : www.european –accreditation.doc.

(20) Consulter le site d'EA : www.european –accreditation.doc.

en Hollande (TTP.NL), en Grande-Bretagne (T Scheme) et en Irlande (référentiel pour l'instant non public). Ils pourront être utiles pour l'élaboration des référentiels des organismes de certification.

- Par rapport à la sécurité des systèmes d'information, on peut nommer la norme ISO 17799, inventaire cependant trop générique, ou les GMITS du DIN Allemand, qui propose une méthode de rigoureuse mais coûteuse à mettre en œuvre.

Fort heureusement, une initiative européenne, EESSI (21) (*European Electronic Signature Standardisation Initiative*), soutenue par la Commission européenne, produira des référentiels (s'inspirant notamment des documents mentionnés ci-dessus) suffisamment spécifiques pour être applicables moyennant des précisions et peut-être quelques modifications mineures.

Que peut-on en attendre ?

Les offreurs de services liés à la signature électronique sont en attente de la mise en place de ce schéma. Cette attente semble liée en premier lieu à la sécurité juridique qu'il créera, qui pourrait contribuer au décollage du marché (le nombre de certificats distribués en France est très loin de un par personne !).

D'autre part, le schéma de certification national ouvre des perspectives intéressantes en créant des jalons de confiance, non seulement de la signature électronique « selon les conditions de l'article 5.1 de la directive », mais aussi toutes ses applications :

- des systèmes permettant de créer et générer des signatures de « haut de gamme » (par exemple pour la notarisation, comprenant, donc, la certification par un horodatage signé) ;
- des systèmes d'archivage très sûr ;
- les gestions de procédures pour autrui (par exemple, collecte des réponses à appel d'offre) ;
- la collecte à la volée d'éléments de preuve tels que des transactions, de manière automatique (cas de la billettique notamment) ;
- courrier électronique recommandé avec accusé de réception, le tout ayant force probante,

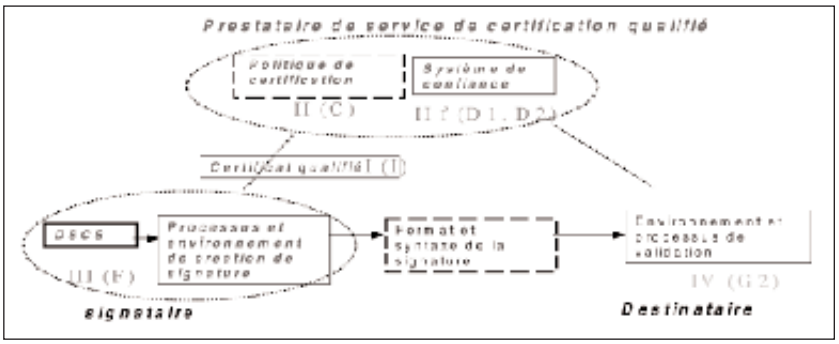

Fig. 3. - Les travaux en cours au niveau européen

- etc.

Par ailleurs la certification prévue pour les composants de confiance devrait également accentuer la dynamique née des Critères communs (ISO 15408), dont l'application a longtemps été cantonnée au secteur de la carte à puce. Peut-être même que dans quelques années on pourra envisager une certification des prestataires liés à la signature électronique selon cette norme.

Ces jalons de confiance pourront par la suite être complétés, sur la base de l'expérience acquise dans le domaine spécifique de la signature électronique, tout d'abord par l'extension du schéma à d'autres applications (cf. ci-dessus), voire à la création d'autres schémas de certification (par exemple spécifiques à certaines types d'entreprises).

En définitive, l'effet d'entraînement du schéma en cours de préparation sur l'ensemble du marché est donc potentiellement important, bien que difficile à évaluer *a priori*. D'autre part son efficacité ne sera pas connue avant une longue période, et seule la jurisprudence le validera définitivement.

Des difficultés cependant…

Les quatre difficultés suivantes nous paraissent fondamentales.

- L'obligation des prestataires sera au minimum une obligation de moyens dans un premier temps puis, lorsque toutes les dispositions de la directive auront été transposées, une obligation de moyens renforcée (présomption de responsabilité en cas de litige, moyennant quelques exceptions). Or, compte tenu de la force juridique du procédé de signature électronique présumé fiable, et de la confiance qu'elle génère, l'utilisation d'une faille par un fraudeur pourrait avoir un impact très élevé ; d'où une responsabilité très lourde pesant sur les organismes chargés d'évaluer les PSC. La procédure d'accréditation devra donc être très rigoureuse.
- Le type de contrôle effectué par les auditeurs reste à définir. Compte tenu du point précédent, il est probable qu'un simple audit ne suffira pas. Mais, pour rendre son coût et sa durée acceptables, il serait préférable que les vérifications et les tests éventuels soient aussi limités que possible.
- Les premiers travaux d'EESSI, dont certains sont destinés à être publiés au JOCE, se concentrent sur la création de la signature et les certificats électroniques (cf. graphique 3), ce qui est logique puisqu'il s'agit des aspects les moins difficiles à cerner du point de vue des technologies. Mais, à supposer qu'ils puissent démontrer leur conformité aux documents en question, les opérateurs devront en plus gérer de manière suffisamment fiable, au minimum, les aspects supplémentaires suivants :
- enregistrement du titulaire d'un certificat,
- gestion du risque de proximité de l'utilisateur afin de limiter l'impact d'une fraude (limitation du nombre de signature, marche à suivre en cas de doute, etc.),
- procédure et moyens de vérification de la signature et du document signé,
- vérification de ce que l'on signe.

(21) Site www.ict.etsi.fr/eessi.

Ces éléments sont difficiles à normaliser : sur le premier aspect, une harmonisation européenne est impossible à trouver à l'heure actuelle (et pas avant longtemps) ; le second aspect est laissé essentiellement à l'initiative des prestataires (c'est un facteur de différenciation commerciale). Enfin, les deux derniers aspects ne peuvent pas être normalisés compte tenu des technologies disponibles à l'heure actuelle (cf. le cas de l'ordinateur personnel, réputé peu sûr). Certains de ces aspects pourront, voire devront, être définis par l'Etat, en particulier en ce qui concerne l'enregistrement. En effet, l'Etat est seul garant et responsable de la confiance que l'on peut avoir dans les titres officiels vérifiés lors de l'enregistrement (art 6.m du décret du 30 mars 2001).

- Un tel schéma devra être compatible avec le souci légitime des prestataires de ne pas devoir passer de multiples qualifications selon les partenaires avec lesquels ils s'associent (cas, par exemple, d'un opérateur de certification qui peut souhaiter s'associer avec plusieurs autorités d'enregistrement). Il s'agit d'une forme de modularité qui reste à inventer.

Pour toutes ces raisons, tout référentiel d'évaluation utilisé par les organismes d'évaluation, et notamment le guide de l'auditeur, devra probablement être soumis à une homologation (en l'occurrence celle du ministre en charge de l'Industrie), qui constituerait un compromis possible entre le souhait de ne pas forcer une harmonisation susceptible de « brimer » les forces de la concurrence et la possibilité pour l'Etat de prendre sa part de responsabilité dans la reconnaissance de la qualification des PSC.

Il s'agira en particulier de limiter, par des critères appropriés, certains comportements « déviants » générateurs de « gisements d'insécurité ». Considérons, par exemple, le cas des « vrais-faux » passeports (volés puis falsifiés). L'Etat devra peut-être créer des « garde-fous » pour que toute la sécurité ne soit pas reportée exclusivement sur ces documents, à l'exception de toute autre mesure par ailleurs (recoupements, etc), afin de faciliter un niveau de risque global acceptable dans le long terme.

… et il ne fera pas tout

On peut noter certaines difficultés concernant plus particulièrement la responsabilité des organismes d'évaluation face aux prestataires qu'ils évaluent, donc potentiellement l'organisation du schéma de certification ; d'autres liées à la nature particulière de l'analyse de la sécurité des systèmes d'informations ; d'autres auxquelles les prestataires de certification électronique devront apporter des réponses ; d'autres enfin, pour l'instant plus théoriques. Nous ne citons ici que quelques limitations majeures.

Sans s'étendre sur les questions de la confidentialité et de l'indépendance des évaluations, qui sont classiques, il faut noter qu'elles revêtent une importance toute particulière puisque c'est en quelque sorte du commerce de la confiance qu'il s'agit ! Quelques dispositions spécifiques figureront probablement à l'arrêté devant paraître ce sujet.

D'autre part, la sécurité de systèmes d'information complexes n'est jamais absolue : elle n'a de sens que face à un ensemble de menaces qui évoluent avec le temps. Si la majorité des incidents peuvent être gérés, quant à leurs conséquences, par les organisations, d'autres restent inconnus ou difficiles à anticiper. La qualité des évaluateurs, leur science et leur jugement, sont donc primordiaux. En particulier ils doivent être capables d'analyser les risques, d'anticiper leurs conséquences, et de préconiser le cas échéant des mesures pour limiter l'impact de ces risques. Il y a là, en cas d'accident postérieur à la reconnaissance de la qualification, matière à litiges en ce qui concerne la responsabilité de l'auditeur. Dans quelle mesure le rapport d'expertise peut-il lui être opposé ?

Cette difficulté intrinsèque à l'analyse de la sécurité des systèmes d'information, a également des retombées dans le rapport entre les prestataires et les utilisateurs. En effet, certaines attaques sur les systèmes d'informations peuvent être assorties d'une responsabilité pénale (par exemple le vol, la destruction ou l'altération de données), tandis d'autres ne seront jamais punies parce qu'il sera impossible de remonter à la source (cas des virus), de sorte que l'analyse en cas de contestation pourra dans certains cas, certes improbables, se révéler délicate, même avec un droit protecteur pour les utilisateurs. Cette facette de la responsabilité des prestataires de certification soulève de nombreuses questions, notamment eu égard aux informations présentées aux utilisateurs : ces informations sont-elles suffisamment claires, sont-elles « efficaces », autrement dit, ne risquent-elles pas à cause de force de détails de dissuader les utilisateurs d'une consultation pourtant indispensable ? Les travaux d'EESSI n'abordent pratiquement pas ces aspects. Un référentiel de qualification, *a fortiori* s'il était homologué, pourrait apporter quelques principes utiles, mais il ne pourra certainement pas épuiser la question, et ce n'est sans doute pas souhaitable. En revanche, il y a là un axe de progrès très important pour les codes de déontologie.

D'autre part, tout ne peut pas être formalisé dans un référentiel d'évaluation, en particulier l'organisation technique et les contrats privés passés entre les différentes parties d'une AC. Ceci n'est pas surprenant puisque le droit exprime clairement que, face aux utilisateurs ou à des tiers, seule l'AC est responsable : charge aux professionnels de la certification électronique de régler ensuite leurs différends entre eux. Cependant il faut noter que, par exemple, il ne peut pas être totalement exclu que des parties soient en charge de certaines tâches sans prendre leur part de responsabilité. Or, dans la mesure où le métier d'opérateur de certification nécessite des investissements très importants, si un tel opérateur est associé avec de nombreuses autorités d'enregistrement, sa disparition peut avoir des répercussions lourdes.

En outre, même lorsque le schéma de certification sera organisé, même si la directive et le décret du 30 mars 2001 prévoient que les certificats qualifiés par un prestataire établi dans un pays membre seront reconnus qualifiés dans toute l'Europe, cela ne suffit pas pour créer un marché européen dans ce secteur : encore faut-il peut-être que les PSC formalisent cette reconnaissance

par des contrats privés (22). Certes, la certification leur permettra de gagner du temps dans la négociation de ces accords ; mais il est probable que des analyses plus poussées seront nécessaires. Au niveau européen, compte tenu des disparités entre les différentes transpositions nationales (cf. encadré), cela demandera un travail important. La conclusion d'accords de reconnaissance avec des prestataires extérieurs à l'Europe ne devrait pas demander beaucoup d'efforts supplémentaires, mais il se pourrait en revanche qu'elle fasse l'objet d'une attention soutenue de la part des pouvoirs publics.

Pour progresser parmi ces difficultés, les assureurs auront certainement un rôle à jouer. En effet, seule une analyse très approfondie des risques leur permet de créer un contrat d'assurance d'un PSC – sauf peut-être si un tel contrat se double d'une association solidaire de l'assureur et du PSC aux bénéfices et aux risques de la prestation de service. L'apparition contrats d'assurance sans une telle association pourrait donc constituer le signe d'une certaine maturité de l'offre. Cependant, la directive comme le projet de loi de Société de l'information qui transposera cet aspect, laisse ouverte la possibilité pour le PSC de disposer de ressources financières suffisantes.

Enfin, comme nous l'avons déjà remarqué, de nombreux aspects de la certification et de la signature électronique restent en suspens dans les sources documentaires disponibles. En particulier, la précision des travaux de l'EESSI est limitée par la nécessité de trouver un compromis parmi les différents participants – autant de points de vue nationaux quant au droit résultant de la transposition de la directive, à la charge de la preuve ou aux procédures en cas de contentieux, à l'enregistrement et la notion d'identité des personnes, et bien entendu, quant aux technologies utilisées, sans parler de l'influence des grands fournisseurs de solutions clé en main -.

Enfin, le moment venu, comment l'auditeur considérera-t-il des PSC recourant à des systèmes organisés selon des principes éloignés de ceux, exposés plus haut, de la directive, et donc aux documents destinés à être publiés au JOCE ? Que se passerait-il si de tels opérateurs, sans pour autant être certifiés, recevaient les faveurs des marchés. La communauté des utilisateurs gagnerait-elle à un rééquilibrage du schéma de certification en conséquence ? La réponse n'est pas simple dans la mesure où seule la pratique permet de connaître en fin de compte la fiabilité d'un opérateur de confiance : du point de vue technique les contrôles organisés par la DCSSI permettront de se faire une idée de la valeur des systèmes ; du point de vue plus global, c'est la jurisprudence qui statuera.

Pour ne pas conclure trop vite…

En définitive, un schéma en vue de reconnaître la qualification des prestataires de services de certification, surtout s'il est proposé par l'Etat et encadré par le droit, constituera un jalon de confiance favorable au décollage des usages liés à la signature. Il permettra aussi aux professionnels du secteur de développer une expérience collective utile pour étendre cette confiance à l'ensemble des services de confiance sur les réseaux ouverts.

Mais la profession n'en devra pas moins proposer des chartes ou des codes de déontologie insistant sur les nombreux points que ce schéma laissera en suspens. C'est un peu déjà le cas avec, par exemple, la rédaction d'une charte par le groupe « juridique et garantie » de la Fédération nationale des tiers de confiance.

D'autre part, une harmonisation des schémas nationaux devra être envisagée à l'échelle européenne. Elle contribuera certainement, dans la foulée de la directive du 13 mars 1999, à créer un marché européen des prestations liées à la signature électronique. ●

(22) C'est un sens que l'on peut donner à l'article 8.b du décret du 30 mars 2001, qui dispose qu'« un certificat électronique délivré par un prestataire de services de certification électronique établi dans un Etat n'appartenant pas à la Communauté européenne a la même valeur juridique que celui délivré par un prestataire établi dans la Communauté, dès lors que le certificat électronique délivré par le prestataire a été garanti par un prestataire établi dans la Communauté et satisfaisant aux exigences fixées au II de l'article 6 ».