

INFORMATIQUE • La question de la transmission électronique de contrats ou de pièces comptables est juridiquement réglée. L'émission de certificats de signature n'est cependant pas encore monnaie courante

# Le marché de la signature électronique est légalement ouvert, mais encore peu utilisé

Willy Boder

Le Conseil fédéral a fixé au 1er janvier 2005 l'entrée en vigueur de la loi sur la signature électronique. Ce texte permet de placer sur le même plan juridique une signature électronique et une signature manuscrite au bas d'une facture, d'un contrat, ou de tout document important. Mais de la théorie à la pratique il reste un fossé à franchir car passer du simple stylo directorial à la multiplication des cartes à puce ou des clés «USB» enfichables dans un ordinateur paraît, pour de nombreuses entreprises, encore trop complexe.

D'autre part, aucune entreprise de certification n'a encore demandé d'être reconnue par la Confédération, via l'entreprise KPMG, comme la loi l'exige pour obtenir une équivalence juridique indiscutable des signatures devant un tribunal. «Cette procédure peut atteindre plusieurs centaines de milliers de francs. Si une telle somme est admissible pour des pays comme l'Allemagne ou la France, nous nous demandons si cela vaut vraiment la peine d'entamer ces démarches compte tenu de la petite taille du marché suisse», explique un spécialiste de la branche.

En juin 2003, Carlos Moreira, président de l'entreprise genevoise WISEkey, évaluait entre 100 et 130 millions de francs le potentiel de ce marché en visant l'ensemble

de l'identification électronique, de la pièce d'identité, au contrôle d'accès en passant par les certificats de signature électronique à usage commercial.

Pour l'instant, il n'existe pas de projet de véritable carte d'identité électronique identifiable par ordinateur que l'Etat délivrerait à chaque individu, ce qui simplifierait évidemment la généralisation de la signature individuelle électronique. En l'an 2000, le Conseil fédéral n'excluait pas une telle initiative, mais il fait désormais preuve de scepticisme. «La cyber-euphorie a fait place au réalisme. Une fois seulement que les conceptions techniques seront arrivées à maturité et auront été harmonisées au niveau

international, il sera possible de juger comment il conviendra de s'adapter à l'évolution technologique», expliquait-il en mai dernier, en réponse à une motion parlementaire sur le sujet.

L'authentification de la signature est donc confiée à des organismes privés via une procédure de certification comparable aux normes ISO 9001. La vérification de signature se fait de manière électronique par cryptage sur la base d'un système fourni par une entreprise privée de certification qui émet des cartes à puce ou des clés USB générant des cryptages à double clé. Une entreprise est ainsi confrontée à des procédures différentes et complexes si elle entend sécuriser la transmission

électronique de ses factures, de ses pièces comptables, ou de ses contrats.

«Le système était perçu comme trop compliqué et trop cher, mais c'est en train de changer. On peut aujourd'hui émettre des cartes à puce vendues entre 30 et 150 francs. Il y aura une profonde évolution de ce marché en 2005 et 2006 déjà», assure Juan Avellan, vice-président de WISEkey, société genevoise qui s'étend aux Etats-Unis et a déjà délivré plusieurs milliers de certificats de signature électronique.

## Un gain de place pour archiver

Albin Delavy, membre de la direction de GIT, société genevoise spécialisée dans la fourniture de logiciels comptables sécurisés, est également persuadé du potentiel de la signature électronique. «J'ai déjà remis une centaine de clés USB, notamment à des fiduciaires et à des PME», explique-t-il. L'avantage du système permet d'empêcher toute falsification de pièces en associant directement l'écriture comptable à la facture ad hoc, puis en sécurisant le transfert de données à une fiduciaire via le cryptage des documents par la signature électronique. «Le gain de place pour conserver, comme l'exige la loi, dix ans d'exercices comptables, associé à l'inviolabilité du système de sécurité séduit nos clients».

## Un système de double clé comparatif

Rien de plus facile que de copier un document informatique, voire découvrir ou falsifier un mot de passe. Comment, dès lors, garantir l'authenticité d'un document transmis par voie électronique? La technique de vérification repose sur un système de cryptage par chiffrement asymétrique utilisant deux clés, l'une publique, accessible à celui qui reçoit le document, l'autre privée connue du seul auteur. Une entreprise de certification possède la racine de cryptage et délivre des certificats d'authenticité de signature sous forme, par exemple, de cartes à puce. L'utilisateur final, chef de la comptabilité ou directeur, reçoit en mains propres une carte à puce ou une clé USB qui crypte tous les documents qu'il désire signer électroniquement. A chaque texte est attaché de manière indissoluble un double codage, privé et public. Le destinataire du document possède la clé publique qui, associée à la clé privée, permet d'authentifier l'auteur. L'utilisation de la carte à puce ou de la clé USB est elle-même protégée par un système de code connu de son seul utilisateur.

W. B.