Signature numérique: Les enjeux du projet de réglementation

Jean-Maurice Geiser

Lic. en droit, suppléant du chef de la section politique et prospective à l'OFCOM, Bienne

Le commerce électronique est promis à un bel avenir. Les nouvelles technologies de l'information et de la communication offrent des possibilités quasi illimitées de conclure des affaires de manière simple et rapide, au-delà des frontières nationales. Il convient toutefois d'identifier et d'éliminer les obstacles qui risquent de freiner, voire d'empêcher le développement du commerce électronique à grande échelle. Les utilisateurs doivent en effet avoir confiance dans les instruments mis à leur disposition et être assurés que leurs engagements seront suivis d'effets juridiques, indépendamment du lieu où ils se trouvent. Des solutions doivent donc être trouvées tant sur le plan technique qu'au niveau légal, dans un souci d'harmonisation internationale.

Les conditions techniques

Le chiffrement des informations circulant sur les réseaux ouverts de type Internet permet de garantir leur confidentialité. La cryptographie à clé publique (ou cryptographie asymétrique) confère en outre la possibilité de garantir l'intégrité du contenu d'un message ou d'un document électronique ainsi que l'identité de son auteur. Dans ce système, chaque utilisateur possède une paire de clés cryptographiques, dont l'une, la clé privée, reste connue de lui seul, alors que la seconde, la clé publique, est mise à la disposition des autres utilisateurs. La clé privée est utilisée pour chiffrer, c'est-à-dire «signer» le message ou le document, alors que la clé publique sert à déchiffrer, c'est-à-dire à vérifier la signature numérique. Le chiffrement au moyen de la clé privée produisant une valeur différente en fonction du contenu du message ou du document traité, la vérification de la signature numérique permet au destinataire de s'assurer que le texte n'a subi aucune modification depuis le moment où il a été «signé». Elle indique en outre que le message ou le document émane bien de la personne qui est censée avoir la maîtrise exclusive de la clé privée.

Afin de se voir attribuer une identité univoque dans le monde virtuel d'Internet, les utilisateurs ont recours à des tiers de confiance, dont la tâche essentielle consiste à certifier le lien existant entre une personne déterminée et sa clé publique. Ces tiers de confiance, que l'on appelle «autorités de certification» (*certification authorities*) ou encore «fournisseurs de services de certification», émettent à cet effet des certificats électroniques «signés» au moyen de leur propre clé privée et mis à la disposition des autres utilisateurs dans des annuaires. L'ensemble des conditions techniques et administratives nécessaires à la fourniture de services de certification constitue l'infrastructure à clé publique.

Le cadre légal

C'est ici que le législateur est appelé à intervenir. Il s'agit en premier lieu d'assurer la qualité des services de certification, en édictant des exigences essentielles et en donnant aux fournisseurs de services de certification la possibilité de se faire reconnaître selon ces exigences essentielles. C'est le but que vise un projet d'ordonnance préparé par un groupe de travail interne à l'administration fédérale sous la direction de l'Office fédéral de la communication (OFCOM). Selon cette ordonnance, les fournisseurs de services de certification pourraient se faire reconnaître, sur une base volontaire, par des organismes de certification (*certification bodies*) accrédités auprès du Service d'accréditation suisse (SAS). Ils pourraient ainsi se prévaloir d'un label de qualité, et les utilisateurs auraient alors la garantie que leurs services peuvent être considérés

Zusammenfassung:
Unter der Leitung des Bundesamtes für Kommunikation (BAKOM) bereitet eine Arbeitsgruppe eine Verordnung über die Public-Key-Infrastruktur in der Schweiz vor, welche bald vom Bundesrat angenommen werden sollte. Die Verordnung hat insbesondere zum Ziel, einem grossen Benutzerkreis sichere Zertifizierungsdienste anzubieten und die rechtliche Verwendung der digitalen Signatur zu fördern.
Die digitale Signatur ermöglicht den Internet-Benutzern, die Authentizität und Integrität ihrer Mitteilungen oder elektronischen Dokumenten zu garantieren. Der Gesetzgeber ist aufgerufen, nicht nur die technischen und administrativen Bedingungen der digitalen Signatur zu regeln, sondern diese auch rechtlich anzuerkennen und der handschriftlichen Unterschrift gleichzustellen. Auf jeden Fall müssen die Harmonisierungsbestrebungen auf internationaler Ebene mit grosser Aufmerksamkeit verfolgt werden.

Résumé: *Sous la direction de l'OFCOM, un groupe de travail prépare une ordonnance sur l'infrastructure à clé publique suisse qui devrait prochainement être adoptée par le Conseil fédéral. L'ordonnance a notamment pour but de promouvoir la fourniture de services de certification électronique sûrs à un large public et d'encourager l'utilisation et la reconnaissance juridique de la signature numérique. Grâce à la signature numérique, les utilisateurs d'Internet disposent d'un moyen technique leur permettant de s'assurer de l'authenticité et de l'intégrité d'un message ou d'un document électronique. Le législateur est appelé à régler non seulement les conditions techniques et administratives des services liés à la signature numérique, mais également la valeur juridique de cette dernière par rapport à la signature manuscrite. Dans tous les cas, les travaux d'harmonisation menés au niveau international doivent être suivis avec la plus grande attention.*

comme sûrs. L'ordonnance s'attache en particulier à assurer que l'identification des titulaires de clés publiques soit faite de manière sérieuse et que les certificats électroniques émis soient publiés, conservés et, au besoin, annulés. Elle comprend également des dispositions sur la génération et l'utilisation des clés cryptographiques ainsi que sur le contenu des certificats électroniques.

L'entrée en vigueur de l'ordonnance est prévue pour le début de l'année prochaine. Restera alors encore à régler le problème de la valeur juridique de la signature numérique par rapport à la signature manuscrite. Certes, aujourd'hui déjà, la plupart des contrats, selon le droit suisse, peuvent être conclus librement, sans respecter de forme particulière. Il n'est toutefois pas sûr que le juge, en cas de litige, considère comme valable un contrat passé par voie électronique. La plupart du temps, il n'a d'ailleurs pas les moyens techniques suffisants pour procéder lui-même à la vérification d'une signature numérique. L'adoption de l'ordonnance devrait cependant *de facto* améliorer les choses. Mais là où le droit positif impose la forme écrite, l'existence d'une signature manuscrite au sens de l'article 14 du code des obligations est nécessaire. C'est entre autres le cas en ce qui concerne la mainlevée provisoire de l'opposition selon l'article 82 de la loi fédérale sur la poursuite pour dettes et la faillite. C'est pourquoi les milieux intéressés consultés dans le cadre de l'élaboration de l'ordonnance considèrent comme urgent le règlement de la question de la valeur juridique de la signature numérique au niveau du droit privé. Le Conseil des Etats vient par ailleurs de transmettre au Conseil fédéral, comme postulat, la motion Leumann visant à adapter la législation suisse de manière que la signature électronique soit reconnue au même titre que la signature manuscrite.

L'harmonisation internationale

Par définition, le commerce électronique ne connaît pas de frontières. Il importe donc que les solutions adoptées au niveau national ne créent pas de nouveaux problèmes dans les échanges internationaux. Dès 1996, la Commission des Nations Unies pour le droit commercial international (CNUDCI) a élaboré une loi type sur le commerce électronique et travaille actuellement à la préparation de règles uniformes sur les signatures électroniques. Dans le cadre de l'OCDE, la déclaration ministérielle d'Ottawa sur l'authentification pour le commerce électronique (octobre 1998) a notamment relevé l'impact potentiel que des solutions nationales diverses pourraient avoir sur le développement du commerce électronique mondial. Quant à l'Union européenne, elle est sur le point d'adopter une directive sur un cadre communautaire pour les signatures électroniques, qui confère un effet juridique à toute signature électronique et rend les signatures électroniques qualifiées équivalentes à la signature manuscrite. Au niveau de la normalisation enfin, l'EESSI (European Electronic Signature Standardization Initiative) s'attache à définir les standards nécessaires à la mise en œuvre de la directive.

La Suisse se doit de suivre de près ces efforts d'harmonisation internationale. En particulier, les travaux de l'EESSI s'avèrent être d'un grand intérêt pour les prescriptions techniques liées à la reconnaissance des fournisseurs de services de certification qui devront être spécifiées en exécution de l'ordonnance. En adoptant des solutions compatibles avec les Etats européens, notre pays préserve ses chances de participer pleinement, à l'aube de l'an 2000, à l'avènement de la société de l'information. ■

Références et liens:
- Avant-projet d'ordonnance sur l'infrastructure à clé publique suisse : http://www.bakom.ch/fre/subpage/?category_61.html
- Motion Leumann du 16 juin 1999 (99.3288) : http://www.pd.admin.ch/afs/toc/f/gesch/f_mainFrameSet.htm
- Travaux de la CNUDCI : http://www.uncitral.org/
- Travaux de l'OCDE : http://www.oecd.org/subject/e_commerce/
- Travaux de l'Union européenne : http://www.ispo. cec.be/
  Voir aussi la position commune arrêtée par le Conseil le 28 juin 1999 en vue de l'adoption de la directive du Parlement européen et du Conseil sur un cadre communautaire pour les signatures électroniques au JO C 243 du 27 août 1999, p. 33
- Travaux de l'EESSI: http://www.cenorm.be/isss/Workshop/EESSI/Default.htm.