La sécurité des documents électroniques

Hier encore, l'authentification de documents d'importance, comme les plans et devis, se faisait exclusivement en scellant et en signant manuellement les originaux. Aujourd'hui, à l'ère de la signature numérique, de nouveaux systèmes permettent d'assurer la confidentialité des échanges, l'intégrité des documents et l'identification des usagers d'un réseau.

PAR JEAN-MARC PAPINEAU

Avec l'avènement des technologies de l'information, la notion de document original, auparavant si importante pour les ingénieurs, perd de son sens. Il est désormais possible d'obtenir à partir d'un fichier électronique, des copies reproductibles que rien ne permet de distinguer de l'original, voire de modifier ou d'altérer ce même fichier, sans laisser aucune trace. Mais il existe des moyens – relativement efficaces – de garantir non seulement l'authenticité d'une signature ou d'un document technologique (enregistré sur un support faisant appel aux technologies de l'information), mais également l'intégrité lorsque le document technologique est transmis ou manipulé.

La sécurité, en informatique, repose sur plusieurs principes : la disponibilité et l'intégrité des documents, la confidentialité, l'identification des usagers d'un réseau et, dans certaines circonstances, la non-répudiation, c'est-à-dire l'impossibilité de nier la réalisation d'une transaction ou l'émission d'un document. Au-delà de l'arsenal technologique, soulignons que les habitudes des usagers ont un impact déterminant sur la sécurité d'un système.

On fait appel à des algorithmes de chiffrement de documents et à des clés qui permettent de les activer. Le niveau de sécurité dépend des techniques d'identification des usagers, du type et de la complexité des algorithmes utilisés ainsi que de la gestion des clés. Aucun système n'est inviolable. La règle de base en matière de sécurité informatique consiste à s'assurer que le coût du viol d'un système soit plus élevé que les bénéfices qu'escompte un fraudeur éventuel.

Les algorithmes de chiffrement sont basés sur des transformations mathématiques qu'il est très difficile d'inverser. Les principaux types sont les algorithmes symétriques, qui utilisent la même clé pour chiffrer ou déchiffrer un message, et les algorithmes asymétriques, qui utilisent deux clés différentes : l'une pour chiffrer un message, l'autre pour le déchiffrer. Des algorithmes de chiffrement considérés comme sûrs deviennent inutilisables si on réussit à trouver une méthode pour inverser la transformation mathématique sur laquelle ils reposent.

Les algorithmes asymétriques permettent la signature électronique ou technologique, contrepartie informatisée de la signature traditionnelle. Les émetteurs gardent l'une de leurs clés secrètes et communiquent l'autre à leurs correspondants. Les destinataires, qui déchiffrent leurs messages avec la clé publique, peuvent être certains que ces derniers ont été chiffrés avec la clé privée correspondante. Dans la mesure où les destinataires ont l'assurance que la clé privée est unique et qu'elle est en possession d'une seule personne, les principes d'identification, d'intégrité et de non-répudiation sont respectés. En pratique, les utilisateurs de signatures électroniques distribuent leurs clés publiques, accompagnées de certificats d'authenticité émis par des entreprises reconnues, selon différents niveaux de certification et pour une période de temps donnée.

Par contre, les algorithmes asymétriques exigent plus de temps de calcul que les algorithmes symétriques. On peut limiter cet inconvénient en utilisant une variante de la signature électronique. On génère d'abord à l'aide d'un algorithme dit de hachage, une empreinte numérique du document. Cette empreinte est unique et les algorithmes de hachage sont conçus de telle façon qu'un petit changement dans le document original entraîne un changement substantiel de l'empreinte numérique. Celle-ci est chiffrée, à l'aide de la clé privée de l'émetteur, par un algorithme asymétrique, puis est jointe au document. Le tout est chiffré à l'aide d'un algorithme symétrique, ce qui demande beaucoup moins de temps de calcul. La clé symétrique est à son tour chiffrée, mais cette fois à l'aide de la clé publique d'encodage du destinataire par un algorithme asymétrique. La confidentialité et l'identification sont ainsi assurées, puisque le document est chiffré et que seul le destinataire est en mesure de le décoder à l'aide de sa clé privée.

La sécurité, en informatique, repose sur la disponibilité et l'intégrité des documents, la confidentialité, l'identification des usagers et la non-répudiation, c'est-à-dire l'impossibilité de nier la réalisation d'une transaction ou l'émission d'un document.

Un haut niveau de sécurité est-il nécessaire ? L'identification d'un usager peut être certifiée ou complétée par des systèmes particuliers d'authentification, notamment biométriques. Stockés dans des banques de données, ces systèmes biométriques utilisent des caractéristiques physiques propres à chaque individu, basées sur la reconnaissance de la voix, les empreintes digitales, l'iris, la rétine, l'image infrarouge ou, tout simplement, la signature manuscrite.

Certains systèmes de sécurité, dont plusieurs sont en cours de développement, permettent d'ajouter à un fichier ou à un document imprimé des marques indétectables, à moins de disposer d'un équipement approprié. D'autres permettent d'ajouter à un document imprimé une copie visible, impossible à copier ou à modifier sur le document technologique correspondant, d'un sceau ou d'une signature.

Tout changement apporté à un document archivé, par exemple pour la mise à jour, doit être soigneusement contrôlé. Or, à l'heure actuelle, l'archivage de documents technologiques, qui consiste à maintenir leur disponibilité et leur intégrité de documents pour une période donnée révèle deux problèmes. Certains supports technologiques, magnétiques notamment, ne peuvent être considérés comme inaltérables pour une trop longue période. De plus, l'équipement et les logiciels évoluent et changent avec une telle rapidité que le simple maintien de la disponibilité des documents, c'est-à-dire la possibilité de les lire et de les reproduire, peut exiger une infrastructure et des ressources importantes.

D'autres professions ont adoptés la signature technologique. Des systèmes de notariat électronique sont ainsi apparus récemment sur le marché. Il s'agit de systèmes d'enregistrement et de conservation de documents sous forme électronique gérés par différentes organisations. Au Québec, la Chambre des notaires a mis sur pied, en avril 1998 et à l'usage exclusif de ses membres, le système Notarius. La solution retenue fait appel à une infrastructure à clés publiques, appuyée par un processus formel de certification qui procure un niveau de sécurité équivalent voire supérieur aux processus basés sur le papier. Reposant sur des normes reconnues mondialement de cryptographie asymétrique, tant sur le plan des algorithmes permettant de générer les clés que des répertoires et des certificats X.500 et X.509, le système Notarius permet d'encoder l'information transmise de façon à ce que seul le destinataire du document puisse en prendre connaissance, de sorte que la moindre altération du document lors de sa transmission est immédiatement détectée et entraîne l'impossibilité de le déchiffrer.

Grâce à un logiciel de signature numérique conçu par la firme Entrust, chaque utilisateur du système Notarius se voit attribuer deux paires de clés : les clés d'encodage, qui servent à assurer la confidentialité des documents transmis, et les clés de

signature, qui servent à signer des documents et à en vérifier l'intégrité. Chacune des paires est composée d'une clé publique déposée dans un répertoire accessible à tous, et d'une clé privée, connue du détenteur seulement. Le procédé est convivial, l'utilisateur n'ayant pas besoin de connaître le fonctionnement technique de la signature numérique, puisse qu'il n'a qu'à cliquer sur quelques icônes : encoder, signer, vérifier, par exemple.

La Chambre des notaires du Québec agit comme autorité de certification puisque, du point de vue juridique, l'identité du signataire d'un document électronique doit être certifiée par une telle autorité. Cette dernière consigne les informations sur les utilisateurs du système dans un certificat rattaché à une signature numérique personnelle. Dans ce but, la Chambre des notaires du Québec a recours à deux entités distinctes : l'autorité de certification locale, par lequel le secrétaire ou le secrétaire adjoint de la Chambre vérifie l'identité des détenteurs de signature numérique au moment de l'émission. Et le centre de certification, géré par le système Notarius qui a le mandat d'émettre, de révoquer et de mettre à jour les certificats d'identité des détenteurs, ainsi que de maintenir l'infrastructure technologique opérationnelle.

Stockés dans des banques de données, les systèmes biométriques utilisent des caractéristiques physiques propres à chaque individu, basées sur la reconnaissance de la voix, les empreintes digitales, l'iris, la rétine, l'image infrarouge ou, tout simplement, la signature manuscrite.

Les ingénieurs comptent parmi les professionnels qui exercent de grandes responsabilités en matière de gestion de documents. Hier encore, l'authentification de documents d'importance, comme les plans et devis, se faisait exclusivement en scellant et en signant manuellement les originaux, qui étaient soigneusement conservés par la suite. Des outils de travail puissants comme l'informatique, la bureautique et les réseaux de communication comme Internet définissent un environnement dans lequel les responsabilités professionnelles s'exercent en fonction de nouvelles règles. Or, les règles définies dans le Code de déontologie des ingénieurs ne peuvent s'appliquer véritablement dans ce nouvel environnement. Conscient de cette réalité, l'Ordre des ingénieurs du Québec a réexaminé l'ensemble de ces règles, les a mises à jour et les présente dans un document intitulé *Directives pour l'authentification des documents d'ingénierie.* ●