

Signature numérique

Une protection inégalée

D'évidentes raisons pratiques et économiques poussent les ingénieurs à délaisser de plus en plus les documents de papier pour des documents sous forme de fichiers électroniques. Or, tous ces bouleversements technologiques ont incité les autorités de l'Ordre à adapter les principes et les règles de base qui encadrent ces nouvelles pratiques afin que celles-ci soient conformes à la Loi concernant le cadre juridique des technologies de l'information, et ainsi, assurer la protection du public.

La reconnaissance légale des documents électroniques ouvre la porte à l'utilisation et à l'acceptation des technologies de l'information dans l'exercice des fonctions de l'ingénieur. Les outils technologiques comportent de nombreux avantages sur le plan de l'efficacité, de la rapidité et de l'accessibilité de l'information, mais doivent impérativement répondre aux enjeux sur le plan de la sécurité.

Comment peut-on se protéger contre l'altération et la falsification d'un document électronique ?

L'infrastructure à clés publiques : un système de confiance

Afin de répondre à cet enjeu, un système a été mis au point il y a déjà plusieurs années : l'infrastructure à clés publiques. Ce système, reconnu à travers le monde et relativement standardisé, est basé sur la technologie de signature numérique et d'encodage. Il repose sur un processus de certification de l'identité des détenteurs de signature numérique à travers un réseau de tierces parties impartiales. C'est ce système qui a été retenu par l'Ordre des ingénieurs du Québec par le biais de l'Infrastructure à clés publiques de Notarius. L'obligation d'authentification des documents par l'ingénieur impose un haut niveau de sécurité et la signature numérique délivrée par un tiers de confiance de notoriété publique répond à ce besoin.

En somme, l'ensemble des attributs de l'infrastructure à clés publiques assure la sécurité, l'intégrité et la confidentialité d'un document sur support électronique signé au moyen d'une signature numérique.

L'autorité de certification : l'assurance de l'identité et du statut professionnel

Dans le cas des ingénieurs du Québec, avec l'autorisation de l'Ordre à cet effet, l'autorité de certification, en l'occurrence Notarius, est une personne morale chargée de lier l'utilisateur à sa paire de clés (signature numérique) en délivrant un certificat qui établit avec certitude l'identité de la personne ainsi que son statut professionnel, et par la suite, de garantir un lien formel entre une personne et ses paires de clés numériques. Elle sert à apporter la preuve de l'identité du signataire et à le lier au contenu d'un document électronique.

Délivrance d'une signature numérique et non d'une signature numérisée

La signature numérique n'a rien à voir avec une signature numérisée. La signature numérisée est une signature manuscrite qui a été convertie en fichier électronique par un numériseur. Elle est une image de la signature manuscrite et par conséquent

ne possède aucune valeur juridique contrairement à la signature numérique. La signature numérique est unique au détenteur et lui seul peut l'utiliser. Ainsi, lorsqu'une signature numérique est apposée sur un document, elle en fait partie intégrante et ne peut être déplacée sur un autre document, la signature numérique offre les mêmes avantages que la signature manuscrite, en ce sens qu'elle peut uniquement être créée par le signataire, qu'elle est vérifiable, qu'elle ne peut pas aisément être contrefaite et qu'elle offre une preuve que vous êtes bien l'auteur du document.

Entrust : une technologie éprouvée

La signature numérique délivrée aux ingénieurs utilise la technologie Entrust, laquelle est employée par plusieurs agences gouvernementales et divers professionnels. Cette technologie fait intervenir deux paramètres mathématiquement liés entre eux, la clé privée et la clé publique. La clé privée est propre à l'utilisateur et doit être conservée en secret et être protégée par celui-ci. La clé publique quant à elle, est publiée afin de la rendre accessible à tous. Le couple formé de la clé publique et de la clé privée est souvent désigné par l'expression « paire de clés et de certificats ». La clé privée du détenteur servira à signer un document. Tout lecteur de ce document ayant accès à la clé publique, à l'aide d'un logiciel approprié, peut vérifier cette signature. Plus simplement, on pourrait comparer la

La reconnaissance légale des documents électroniques ouvre la porte à l'utilisation et à l'acceptation des technologies de l'information dans l'exercice des fonctions de l'ingénieur. La signature numérique est unique au détenteur et lui seul peut l'utiliser.

paire de clés à celle formée par une clé et un cadenas. Lorsqu'un individu signe, il scelle le document avec son cadenas privé. Tous ceux ayant accès à la clé permettant d'ouvrir ce cadenas unique à cet individu seront à même de constater que seul le détenteur du cadenas privé est le signataire du document.

Comment fonctionne la signature numérique ?

Avec le logiciel cryptographique Entrust, le détenteur génère ses clés et ses certificats, communément appelés signature numérique, et crée ainsi son mot de passe confidentiel. Ce mot de passe est relié à sa clé privée de signature.

Bien que cette technologie puisse sembler complexe, il suffit au détenteur de faire quelques clics pour lancer tout le processus de signature d'une manière qui permet ensuite à toute partie intéressée de la vérifier.

Pour plus d'information, nous vous invitons à communiquer avec Notarius, le fournisseur autorisé de l'Ordre au (514) 281-1442 ou sans frais au 1 800 567-6703 ou à visiter le site Internet destiné aux ingénieurs à l'adresse www.ingenieur.notarius.com ou en cliquant sur le bouton « signature numérique » à l'adresse www.membres.oiq.qc.ca.