

Parlons-en des signatures sécuritaires par Chantal Côté, notaire, Notarius

Les échanges papier font de plus en plus place aux échanges de documents technologiques par différents réseaux menant à la dématérialisation des données ou, plus explicitement, à la mise en œuvre du fameux « bureau sans papier ».

La dématérialisation facilite les échanges et procure des gains de temps et de productivité évidents pour les entreprises. Par contre, les utilisateurs négligent trop souvent la sécurité de leurs opérations.

Une signature à votre niveau pour une dématérialisation réussie

Lien entre l'auteur et le document

L'objectif principal de la dématérialisation est de gérer de façon totalement électronique des données ou des documents dans le cadre d'échanges avec des partenaires ou des clients. Celle-ci doit s'effectuer de façon à restreindre les risques liés au piratage des données ou à leur altération ou à l'usurpation d'identité.

Pour la grande majorité des professionnels, le processus de dématérialisation doit tenir compte des obligations auxquelles ils sont assujettis dans l'exercice de leur profession. À titre d'ingénieur et membre de l'Ordre des ingénieurs du Québec, vous êtes investis d'un droit et d'un devoir : celui de signer les documents d'ingénierie dont vous êtes l'auteur, soit sur support papier ou, soit sur support technologique. Le titre attaché à votre œuvre lui confère alors sa vraie valeur.

Le facteur clé de succès d'une dématérialisation repose sur une solution qui assure une authentification conforme aux énoncés de la Loi concernant le cadre juridique des technologies de l'information (ci-après LCCJTI) et à la législation régissant la profession, c'est-à-dire, notamment, qui confirme l'identité et le statut professionnel d'une personne et son lien avec le document authentifié. Dans un contexte technologique cette obligation ne peut être remplie sans certificat numérique, lequel prouve l'identité de celui qui fait usage d'une signature numérique. Il représente le premier facteur clé de succès d'une dématérialisation réussie.

L'assurance de l'identité du signataire

Le certificat numérique est donc, à l'échelle d'une organisation tel un ordre professionnel, un outil pour témoigner, de façon électroniquement sûre, d'une identité. De ce fait, il est important, au moment de retenir les services d'un prestataire de certificats, de choisir celui qui offre des procédés d'attribution fiables. Il est donc impératif que la délivrance des certificats de signature numérique se fasse après avoir vérifié l'identité des demandeurs. Cet élément s'avère crucial pour une profession, car il servira à créer un sentiment de confiance et de fiabilité auprès de la population et de ses membres.

Le niveau de certification

Il est important de comprendre que les nombreux certificats numériques disponibles sur le marché n'offrent pas le même niveau d'authentification de l'identité. Celui-ci dépend de l'autorité de certification qui les émet et du processus d'authentification. Plus le processus d'authentification est fiable, plus le niveau de confiance du certificat est élevé.

Par exemple, certains certificats sont délivrés sans qu'aucun contrôle de l'identité du détenteur du certificat ne soit effectué. L'utilisateur peut prétendre être quelqu'un d'autre ou faire l'usage d'un pseudonyme. Certaines autorités de certification effectuent un contrôle d'authentification par simple envoi de copies de pièces d'identité. Dans ces deux derniers cas, aucune garantie n'est donnée au destinataire quant à l'identité du signataire. Pour offrir une véritable sécurité aux utilisateurs et aux tiers avec qui ils communiquent, il est prescrit de recourir au déplacement physique de l'utilisateur et d'authentifier en personne ce dernier sur présentation de

plusieurs pièces d'identité originales. Ce niveau d'authentification est sécuritaire et satisfait aux exigences de la LCCJTI visant la certification.

La confiance

La notion d'autorité de certification est rattachée au concept de l'infrastructure à clés publiques (ICP). Cette dernière doit s'assurer, par son autorité de certification, que les clés correspondent bel et bien à l'identité du titulaire. Pour s'acquitter de cette obligation et maintenir la confiance en l'autorité de certification, l'ICP doit offrir un processus d'authentification qui confirme l'identité et, dans certain cas, le statut professionnel de l'utilisateur.

La présence et la continuité

La délivrance d'une signature numérique de confiance s'effectue à la suite d'une vérification de l'identité du demandeur en présence d'une personne dûment accréditée. C'est le processus d'identification privilégié par Notarius. De plus, Notarius confirme le statut professionnel du demandeur lorsqu'il s'agit d'un membre issu d'un ordre professionnel. Un lien permanent est maintenu entre l'Ordre et l'autorité de certification visant à assurer que le professionnel qui utilise la signature numérique possède toujours son permis d'exercice, à défaut de quoi la signature est révoquée. Les contrôles d'authentification réalisés assurent la confiance et la crédibilité des organisations et de leurs membres qui y ont recours.

La confidentialité

De plus, la Loi impose des obligations au prestataire de services de certification relativement à la transmission des éléments secrets liés à la clé privée de signature du titulaire. La transmission de ces données doit se faire de manière à ce que seul le titulaire visé en prenne connaissance. L'activation d'une signature numérique émanant de l'ICP de Notarius s'effectue par le titulaire à l'aide de deux codes secrets. Ces derniers sont acheminés par Notarius séparément l'un de l'autre par des moyens de communication différents, limitant ainsi l'interception des deux codes par une tierce partie. Ces mesures visent, entre autres, à éviter les conséquences d'une usurpation d'identité.

Les garanties

Toute ICP qui agit en conformité à la LCCJTI doit détenir et appliquer une politique de certification qui indique les garanties offertes par les certificats émis. La Loi impose des obligations aux titulaires de signature numérique, entre autres, celle de s'assurer que la signature n'est utilisée que par le détenteur. Dans le cadre du service offert par Notarius, les conditions d'utilisation des certificats sont consignées dans sa politique de certification et font partie de l'engagement du titulaire.

L'intégrité

Outre l'authentification de l'utilisateur, le certificat préserve l'intégrité des documents échangés et permet d'assurer que le document reçu est identique au document initial. Toute modification apportée au document à la suite de l'envoi par son signataire invalidera la signature originalement apposée à celui-ci. Sans cet outil de signature, Internet est un service anonyme permettant de falsifier facilement l'identité et les données de l'auteur d'un document sans laisser de traces. Il en va de l'intérêt de tout professionnel et de celle de ses clients de pallier cette problématique.

Notarius est résolument reconnue pour ses processus rigoureux de certification par plusieurs ordres professionnels et instances gouvernementales. Par conséquent, elle offre la possibilité aux professionnels d'avoir recours à un outil permettant une dématérialisation qui assure la sécurité des données, la conformité aux lois, un potentiel d'économie tout en confirmant les lettres de noblesse du titre professionnel!