Questions courantes à propos des signatures numériques

notarius

Notarius est un fournisseur de services de signature numérique de qualité gouvernementale qui totalise plus de 20 ans d'expérience et sert plus de 35 associations professionnelles de divers secteurs, y compris des secteurs juridique, de l'ingénierie, de l'architecture et de l'arpentage. De nombreuses organisations qui envisagent une transformation numérique s'interrogent sur les implications que cela représente en matière de technologie, de fiabilité juridique, de conformité, de sécurité et de fonctionnalités pour les utilisateurs finaux. Ce document vise à répondre aux questions les plus fréquentes lorsque vient le temps d'évaluer les solutions de Notarius.

AU PLAN JURIDIQUE

Q **Pourquoi les associations professionnelles choisissent-elles d'émettre des signatures numériques pour leurs membres?**

R Le contrôle de l'utilisation des sceaux ainsi que la protection du public font partie intégrante des responsabilités des associations professionnelles. Au format papier, cela se fait en apposant un sceau qui contient le nom, le numéro et la désignation du membre et qui est officialisé en datant et signant le document à la main. Comment les associations peuvent-elles sceller de façon sécurisée des documents officiels dans un monde numérique où un sceau peut facilement être reproduit et copié d'un document à l'autre? Les associations qui offrent des signatures numériques choisissent de contrôler l'utilisation des sceaux dans un monde numérique afin de s'assurer que seuls les membres en règle peuvent signer des documents officiels. Cela permet également aux clients et aux organismes gouvernementaux de vérifier instantanément qu'un document a été signé par un professionnel habilité à le faire.

Q **Est-ce qu'une personne peut continuer d'utiliser une signature numérique si cette dernière est révoquée?**

R Chaque signature numérique appartient à son titulaire et ne peut être utilisée que par celui-ci. Toutefois, dans la plupart des cas, la signature est émise par une association ou un employeur et non directement à une personne. Par conséquent, la signature numérique peut être révoquée par l'association si un membre n'est plus en règle ou par l'employeur si l'employé quitte l'entreprise. Lorsqu'un signataire n'est plus habilité à utiliser sa signature, la révocation est instantanée, et la signature numérique ne fonctionne plus.

NOTE : La révocation d'une signature n'invalide pas les signatures apposées précédemment (puisque le signataire était en règle à ce moment), mais elle empêche le signataire qui n'est plus en règle de signer de nouveaux documents.

Q **Pourquoi les signatures numériques de Notarius sont-elles reconnues comme des signatures de confiance par les organismes gouvernementaux?**

R Les signatures numériques ne sont pas toutes émises et contrôlées de la même façon. Les gouvernements ont tendance à limiter le nombre d'autorités de certification qu'ils reconnaissent et autorisent. Des directives strictes sont établies et font l'objet de contrôles afin de s'assurer que l'autorité de certification approuvée a les technologies, les mesures de sécurité, les politiques et les processus permettant de garantir l'identité des signataires. Notarius a été fondée dans les années 1990 par la Chambre des notaires du Québec dans le but d'établir une autorité de certification de qualité gouvernementale reconnue par le Registre foncier du Québec. Encore aujourd'hui, très peu d'autorités de certification tierces sont autorisées à émettre des signatures numériques de confiance dans le cadre d'interactions avec des organismes gouvernementaux. Notarius est la seule autorité de certification tierce reconnue par plusieurs gouvernements provinciaux au Canada.

AU PLAN JURIDIQUE (suite)

Q **Les signatures numériques de Notarius sont-elles reconnues partout dans le monde?**

R Les signatures numériques de Notarius sont utilisées pour signer des documents officiels et répondre aux standards de nombreux pays. Toutefois, chaque juridiction peut avoir des exigences particulières à remplir afin qu'une signature soit reconnue. Par exemple, en France, de nombreux organismes ne reconnaissent que les autorités de certification françaises. Aux États-Unis, les exigences relatives aux documents techniques se limitent principalement à l'aspect technologique et non à un fournisseur ou à une norme. À ce titre, les signatures numériques de Notarius satisfont ou surpassent les exigences minimales pour l'ensemble des États-Unis. Il est important de vérifier les exigences locales liées aux signatures numériques auprès des destinataires avant de soumettre des documents signés qui utilisent des signatures numériques de Notarius.

Bien sûr, d'autres considérations doivent être prises en compte avant d'entreprendre un virage numérique. N'hésitez pas à nous contacter pour planifier une séance de travail afin d'en discuter plus en détail.

SÉCURITÉ

Q **Les signatures numériques sont-elles sûres? Peuvent-elles être piratées?**

R Les signatures numériques sont basées sur la cryptographie, qui a vu le jour dans les années 1970 et qui est encore aujourd'hui considérée comme la norme pour assurer la sécurité de différents types de données. Les signatures numériques et leurs dérivés cryptographiques sont utilisés dans nos vies quotidiennes afin de protéger sites web, communications, documents et transactions financières. Si des signatures numériques devaient être « piratées », le premier cas d'attaque serait probablement lié au secteur financier, militaire ou gouvernemental. Un simple document PDF signé serait le dernier souci d'un pirate informatique.

Q **Quels protocoles de sécurité l'autorité de certification Notarius a-t-elle mis en place?**

R Au cours de la dernière décennie, Notarius a énormément investi dans les certifications ayant de hauts standards de sécurité pour l'ensemble de ses solutions. À ce titre, Notarius est certifiée ISO 27001 et ISO 9001. Elle figure également sur la Adobe Approved Trust List (AATL) et est certifiée eIDAS en Europe. Seules quelques autorités de certification dans le monde peuvent rivaliser avec les certifications de Notarius.

Q **Quels sont les plans de contingence si l'autorité de certification Notarius se retrouvait hors ligne ou était piratée?**

R Le temps de disponibilité actuel est de 99,99 avec une redondance complète et de multiples sites de données. Depuis le lancement de la première autorité de certification Notarius en 1998, aucune violation de données n'est survenue. Les signatures numériques de Notarius sont utilisées pour assurer la sécurité de millions de documents officiels qui, dans certains cas, doivent être conservés pendant des décennies. La sécurité est au cœur de tous les services de Notarius, et l'entreprise est certifiée ISO 27001 pour ses protocoles de sécurité.

TECHNOLOGIE

Q **Qui a accès aux images des sceaux et des signatures numériques?**

R Notarius n'a pas accès à la signature numérique, au mot de passe utilisé pour signer, à l'image des signatures ni aux informations d'utilisation (ni à la fréquence d'utilisation ni au contenu des documents signés). Notarius ne stocke pas d'informations liées aux documents signés, et les documents ne sont d'aucune façon visibles pour Notarius.

Q **Qui contrôle les signatures numériques?**

R Les signatures numériques de Notarius sont comparables à un passeport numérique. Les signatures numériques sont émises par l'entremise d'une autorité de certification de confiance, telle que Notarius. Bien que Notarius fournisse l'infrastructure et l'expertise pour générer des signatures numériques, ses partenaires (p. ex. associations professionnelles) ou clients (entreprises ou organismes gouvernementaux) exercent un contrôle

total sur l'émission de ces identités numériques. Une fois la signature émise à un professionnel, celui-ci a le contrôle total sur sa signature numérique et l'image du sceau/de la signature qu'il peut utiliser pour signer un document. En revanche, Notarius peut révoquer sa signature si l'abonnement n'est pas payé en entier, et l'association ou l'entreprise peut révoquer sa signature si celle-ci n'est plus autorisée par l'organisme émetteur (révocation du statut professionnel ou départ de l'employé).

Q Qu'est-ce qu'une autorité de certification?

R Une autorité de certification est un tiers de confiance qui émet des certificats de signature numérique afin de confirmer l'identité d'un signataire. L'autorité de certification offre également des façons de vérifier si un certificat est valide, expiré ou révoqué.

Q Qu'est-ce qui est transmis à l'autorité de certification Notarius (serveur) lorsqu'un document est signé numériquement avec une connexion internet?

R Lorsqu'un document est signé numériquement (avec une connexion internet), une demande de signature est envoyée à l'autorité de certification Notarius afin de vérifier si la signature numérique est valide. Une fois la demande reçue, l'autorité de certification répondra (par l'affirmative ou la négative) et retournera le résultat au document PDF. Si la réponse est négative (signature expirée ou révoquée), il sera clairement indiqué dans le lecteur PDF que le certificat n'est pas valide. Si la réponse est positive, le document comprendra la preuve que la signature numérique était valide au moment où il a été signé. Cette preuve (réponse OCSP ou LCR) sera intégrée au document PDF et, puisque ce dernier est signé numériquement, elle ne pourra être retirée ou altérée sans compromettre l'intégrité du document signé.

Q Peut-on signer un document hors ligne?

R Il n'est pas nécessaire d'être en ligne pour apposer une signature numérique. Toutefois, si la signature numérique est apposée avec une connexion internet, une preuve de validité (une réponse OCSP ou une LCR) sera intégrée au document PDF. Si le signataire n'est pas en ligne, celui-ci pourra tout de même signer le document, mais sans l'ajout de la preuve que la signature numérique était valide au moment où le document a été signé. En revanche, même si la preuve n'est pas intégrée, le destinataire pourra vérifier manuellement le statut de validité de la signature numérique. Notarius recommande que les signataires utilisent une connexion internet pour signer numériquement les documents qui doivent être conservés sur une longue période, mais il est tout de même possible et courant de signer des documents hors ligne. Un cas d'utilisation courant de la signature hors ligne est celui du signataire qui se trouve en région éloignée avec un accès limité à internet.

Q Qu'est-ce qu'un OCSP et une réponse OCSP?

R Le protocole sur le statut des certificats en ligne ou « OCSP » est un protocole couramment utilisé pour obtenir le statut de révocation d'une signature numérique. Ce ne sont pas toutes les autorités de certification qui ont établi un protocole OCSP à des fins de validation par une source externe. La plupart des fournisseurs tiers réputés utilisent un protocole OCSP ou des LCR pour permettre aux destinataires de valider les signatures numériques. Un fournisseur qui n'utilise pas ce protocole devrait être une source de préoccupation puisque cela signifie que le destinataire ne pourra pas vérifier le statut de la signature numérique. Par exemple, les signatures numériques auto-émises dans Adobe Reader n'utilisent pas un OCSP, ce qui les rend impossibles à vérifier avec assurance.

Q Qu'est-ce qu'une LCR?

R Une liste de certificats révoqués ou « LCR » est la liste de toutes les signatures numériques révoquées qui sont associées à une autorité de certification. Cette méthode est utilisée pour valider le statut d'une signature numérique et son autorisation d'utilisation.

Q Qu'est-ce que le format PDF/A-3?

R D'abord et avant tout, le format PDF est une norme ouverte qui permet aux utilisateurs de produire des documents électroniques très similaires au format papier. Puisqu'il s'agit d'un format standardisé (ISO), de nombreux gouvernements ont adopté la norme PDF comme norme commune pour produire et archiver des fichiers électroniques. Les fichiers PDF peuvent être produits de différentes façons afin de répondre à certaines exigences techniques. Par exemple, le format PDF/X est un format courant pour les imprimeurs professionnels. Les formats PDF/A, y compris le PDF/A-3, sont des formats basés sur une norme ISO, qui ont été spécialement conçus pour l'archivage à long terme. Le principal avantage du format PDF/A-3 est qu'il permet de joindre tout type de fichier (DWG, BIM, JPEG, etc.) au document PDF et d'en assurer l'intégrité à l'aide d'une signature numérique.

UTILISATION

Q **Est-ce que plusieurs personnes peuvent signer le même document PDF?**

R Un fichier PDF peut comporter plusieurs signatures numériques. Par exemple, un document peut être signé une première fois, puis signé par un vérificateur, puis par un approbateur.

Q **Est-il possible de signer des fichiers DWG, BIM ou autres?**

R Les signatures numériques sont basées sur un protocole normalisé conçu pour fonctionner dans divers environnements technologiques. Les signatures numériques sont compatibles avec les formats Outlook, Word et PDF. Il est également possible de signer des fichiers BIM et DWG, mais pour ces types de format, il est recommandé de les signer au format PDF/A-3.

Q **Peut-on annoter un fichier PDF signé?**

R De la même façon qu'il est possible d'annoter un document papier, un fichier PDF signé numériquement peut être annoté à l'aide de commentaires, de mises en valeur et d'autres types d'informations ajoutées sur le document PDF signé. Toutefois, puisque la signature numérique scelle le contenu original, l'information source (texte ou images) ne peut être facilement altérée. Par exemple, un dessin technique peut être signé, puis un vérificateur peut annoter le document, mais il ne pourra changer le contenu du dessin. De plus, si le document est annoté, il sera clairement indiqué dans le document PDF que celui-ci a été altéré depuis l'apposition de la signature numérique.

Q **Peut-on modifier ou altérer un document PDF signé?**

R Comme indiqué dans la réponse précédente, un document signé peut être annoté, mais il ne peut être facilement altéré. Si le document signé numériquement est altéré, la signature numérique sera retirée du fichier, ce qui créera une copie du document original. Par exemple, au format papier, un document original qui comporte une signature manuscrite peut être photocopié, ce qui crée une copie du document original, et cette copie peut facilement être modifiée et altérée. La même chose est vraie pour un fichier électronique PDF original qui a été signé numériquement. Il peut être « réimprimé » en tant que document PDF, mais le nouveau document sera une copie de l'original. Cette copie peut être altérée, mais pour le destinataire, il s'agira d'une copie puisque la signature numérique ne fera plus partie du fichier PDF.

Q **Qui peut vérifier la validité d'une signature numérique?**

R Lorsqu'une signature numérique est apposée sur un fichier PDF, il est possible de vérifier les détails de la signature numérique dans la plupart des lecteurs PDF courants, tels qu'Adobe. Le destinataire peut également choisir de faire confiance au signataire et, si la même signature numérique est utilisée, accepter automatiquement la signature numérique lors des validations de documents subséquentes. Grâce à la réponse OCSP et à la LCR fournie à la signature en ligne, le destinataire peut s'assurer de l'identité du signataire et se prémunir contre les risques d'usurpation d'identité.

Pour plus d'information

notarius.com | 1 888 588-0011 | info@notarius.com