LES COMMUNAUTÉS FACE AUX défis RH

DÉMATÉRIALISATION

5 idées reçues autour de la signature électronique

srci
SOLUTIONS DE DÉMATÉRIALISATION
GROUPE SALVIA DEVELOPPEMENT

ADGCF

Fotolia © chaliya

Gain de temps et sécurité

« La signature électronique représente une évolution naturelle, lorsqu'on l'utilise on ne voit pas comment on pourrait faire autrement. Essayez de reprendre une carte au lieu d'allumer votre GPS, c'est la même chose ici. » *DSI d'une Mairie*

« Le gain de temps est évident avec la dématérialisation des flux et des processus, cela s'est inscrit complètement dans nos habitudes de travail ! »

DSI d'une Mairie

Avec les habitudes de travail qui changent et l'évolution du cadre légal au niveau européen, de réels besoins émergent en termes de dématérialisation.

Depuis plusieurs années, l'évolution des métiers au sein des collectivités, l'impérieuse nécessité de gagner en productivité, notamment du fait de la baisse de dotations et des contraintes budgétaires sur vos budgets de fonctionnement poussent chacun d'entre vous à s'emparer des nouvelles technologies pour répondre à vos nouvelles attentes et à vos nouveaux enjeux parmi lesquels le gain de temps et la sécurisation des transactions figurent en bonne place. L'État encourage vivement les collectivités territoriales à passer à la dématérialisation. Nous vous proposons un zoom sur la signature électronique, aboutissement de la dématérialisation.

Commençons donc par combattre 5 idées reçues :

IDÉE REÇUE N° 1

La signature électronique ne remplacera jamais la signature manuscrite

FAUX !

Aujourd'hui, la digitalisation a pris une place importante dans la société, que ce soit au niveau personnel comme au niveau professionnel, l'État pousse en ce sens, et incite les organismes publics comme privés à utiliser de plus en plus d'outils de dématérialisation.

Dans ce cadre, la signature électronique fait figure d'évolution inéluctable. La nécessité de gagner en temps et en efficacité, mais aussi la mobilité accrue des signataires, placent la signature électronique comme la solution en parfaite adéquation avec ces nouveaux besoins. Il est temps de mettre au placard les stylos !

IDÉE REÇUE N° 2

C'est trop compliqué, ce n'est pas à la portée de tout le monde

FAUX !

La conception technique et l'environnement juridique de la signature électronique est certes plutôt complexe mais son usage au quotidien est d'une simplicité déconcertante. Après avoir renseigné quelques champs d'information et effectué quelques clics, le tour est joué : vous avez signé électroniquement. Un jeu d'enfant !

IDÉE REÇUE N° 3

Il faut que tous les signataires soient dotés d'un certificat de signature RGS (*ou) pour signer**

FAUX !

Le nouveau règlement eIDAS permet la génération d'un certificat de signature certifié (équivalent à une clé RGS*). Cela permet d'envoyer des documents (convention, arrêté d'évolution, contrat de travail, ...) à signer directement à des signataires extérieurs à l'organisation que vous représentez.

Mieux, nous pouvons maintenant aller jusqu'à utiliser sur un même document différents certificats de signature : RGS (*ou**) pour une collectivité et un ou plusieurs certificats eIDAS pour les signataires externes (association, club, agent, citoyen, société, ...).

IDÉE REÇUE N° 4

Cela n'a pas de valeur juridique

FAUX !

Selon l'article 1366 du Code Civil, l'écrit électronique a la même force probante que l'écrit sur support papier à condition qu'il permette d'identifier avec certitude la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à garantir son intégrité.

La signature électronique a donc la même valeur probante que la signature manuscrite tout en bénéficiant d'une sécurité plus élevée. Cette solution répond aux exigences légales qui sont de garantir l'intégrité du document et l'authenticité du signataire.

« La dématérialisation des flux a permis d'unifier et d'harmoniser la gestion interne, permettant une véritable rationalisation des tâches administratives. La consultation des dossiers peut maintenant s'opérer en quelques clics. »

DSI d'une Mairie

IDÉE REÇUE N° 5

C'est un processus onéreux

FAUX !

Les économies de papier, de cartouches d'encre, de timbres et la réduction des délais font de la signature électronique une solution très économique avec un retour sur investissement rapide.

4 étapes pour tout connaître de la signature électronique

LA SIGNATURE ÉLECTRONIQUE : LES USAGES

Elle permet de signer tous les documents, qu'ils soient commerciaux, comptables, financiers ou RH de façon légale et sécurisée

Suite à l'adoption de la loi n° 2000-230, entrée en vigueur le 30 mars 2001 en France [1], les collectivités ont la possibilité de dématérialiser leurs documents. Avec les échanges qui se multiplient, il est devenu indispensable de certifier et de donner une valeur légale à certains échanges de documents. La signature électronique est venue répondre à cette nécessité en donnant une valeur probante aux documents numériques échangés.

Cette solution a le mérite de simplifier considérablement les processus administratifs. Elle permet également de réduire la consommation de papier, les risques d'erreurs et donne plus de liberté. Elle accélère les échanges et sécurise les dossiers. Ces nombreux bénéfices font entrer la signature électronique dans les usages des entreprises et des organismes publics. D'ailleurs, aujourd'hui, les aspects techniques de l'outil ne sont plus mis en avant, ce sont ses atouts et son utilisation au quotidien qui priment pour les utilisateurs. C'est 79 % des salariés qui sont favorables à l'utilisation d'un outil de dématérialisation sécurisé pour signer ou gérer les échanges documentaires selon une étude IFOP réalisée pour Néopost France en 2015.

Par ailleurs, la signature électronique évolue considérablement. Les nouveaux outils permettent aujourd'hui de signer ou de faire signer n'importe où et n'importe quand tous les documents (contrats, devis, factures...). Une réelle évolution certifiée par la norme eIDAS [2].

Par exemple, prenons le cas d'une DRH qui doit gérer des personnes présentes sur différents sites : de la demande de congés d'un collaborateur, à la demande d'ouverture de poste d'un manager, en passant par la convocation à une formation ou à la gestion des entrées et sorties de collaborateurs, tous ces processus peuvent être dématérialisés et optimisés grâce à ce système de signature électronique innovant.

ENFIN LA DÉMAT' DES PROCESSUS DE A À Z !

Après des années d'annonces et de réformes, l'administration est entrée dans l'ère de la dématérialisation totale.

Depuis déjà quelques années, toutes les collectivités doivent passer par voie électronique pour transmettre leurs pièces comptables vers la direction des finances publiques, le but étant de supprimer définitivement le papier et ses millions de pages imprimées chaque année. Ces processus permettent d'économiser du papier, de préserver l'environnement et surtout d'améliorer l'efficacité des échanges entre les différents partenaires.

Aujourd'hui, la signature électronique en ligne vient compléter pleinement la dématérialisation de l'ensemble des opérations. En effet, jusqu'à ce jour, la signature manuscrite d'un document obligeait son impression et l'envoi dans certains cas des dossiers si les personnes concernées n'étaient pas sur place (agent, association, fournisseurs...), d'où des coûts non négligeables (affranchissement, papier, toner, ...) et un délai incompressible de plusieurs jours.

Grâce à l'utilisation d'outils innovants (parapheur électronique et signature en ligne, par exemple), les processus sont accélérés et sécurisés. Il est aussi possible d'aller plus loin en utilisant un coffre-fort électronique pour archiver en toute sécurité les documents signés.

(1) Cf : certeurope / Article : les-dossiers-certeurope/reglement-europeen-sur-la-signature-electronique
(2) Cf : Chapitre 3 / Focus sur la réglementation en 3 point – Paragraphe 2

DES BÉNÉFICES ÉVIDENTS

La dématérialisation présente de nombreux avantages en termes :

- **D'optimisation des processus**

Sécurisation des échanges et meilleure fiabilité des données RH par ex., accessibilité renforcée et facilitée, meilleure traçabilité des processus et documents, simplification et gain de temps lors de la recherche d'information, harmonisation des processus, ...

- **De réduction des coûts**

Réduction des dépenses en fournitures papier, diminution des coûts et des temps de traitement et de stockage des données et documents, amélioration de la productivité, ...

- **Et de l'empreinte écologique**

Réduction de l'empreinte écologique, renforcement de la marque employeur, ...

LE PANEL DE DOCUMENTS GÉRÉ PAR LA SOLUTION ET LES DIFFÉRENTS NIVEAUX DE SIGNATURE

La dématérialisation inclut le traitement des documents traditionnellement signés à la main dans les organisations : les arrêtés, les mandats de paiements envoyés en Trésorerie, les marchés publics, et nouvellement les contrats de travail ainsi que les arrêtés RH et ce grâce à la signature en ligne autorisée par la norme eIDAS.

Tous ces documents, qu'ils soient d'ordre administratif, commercial, juridique ou comptable, peuvent être concernés par la signature électronique et associés à un

Fotolia © Andrey Popov

certificat numérique. Leur valeur juridique ainsi que leur intégrité sont ainsi garanties.

Il existe différents niveaux de signature électronique : la signature simple, avancée et qualifiée. Selon le règlement eIDAS, chacune de ces signatures peut être juridiquement valable : 95 % des acteurs du marché utilisent la signature électronique avancée ou SEA. Cette dernière est certifiée au niveau européen et respecte des normes de signature ETSI (institut européen des normes de télécommunications) ainsi que le règlement eIDAS concernant l'identification électronique et les services de confiance pour les transactions numériques au sein du marché intérieur de l'Union Européenne.

Ses avantages sont considérables car cette signature utilise un certificat numérique associé au signataire et dispose d'un système poussé de vérification de son identité. Difficile donc de contrefaire cette signature électronique, qui a tous les avantages de la signature manuscrite tout en bénéficiant d'une sécurité bien plus élevée.

Tous les documents peuvent être concernés par la signature électronique.

FOCUS SUR

La réglementation
en 3 points


Fotolia © phive2015

Confiance, sécurité et défiance numérique

La confiance, chacun pense savoir de quoi il s'agit, mais la confiance numérique, qu'est-ce que c'est ? Cette confiance est nécessaire au développement de l'économie, surtout de nos jours où le numérique prend une place importante dans nos vies personnelles et professionnelles. Mais depuis 2008, la défiance s'accroît et les récents problèmes de l'été 2017 liés à la cybercriminalité sont autant d'alertes qui inquiètent : on se méfie, on a peur que nos données ne soient entre de mauvaises mains, on craint les hackers, les virus et le phishing. Cependant, la défiance envers le numérique n'empêche pas l'utilisation de PC, smartphones, d'applications web, d'outils de dématérialisation ou le développement des usages en mobilité (plus de 65 % de Français sont équipés d'un smartphone, et pour une grande majorité, effectuent des transactions en ligne ou traitent à distance des dossiers professionnels)[3].

Finalement, le manque de confiance ne freine pas les usages. D'ailleurs, nous sommes nombreux dans le monde professionnel à attendre toujours plus des solutions proposées sur le marché. Nous sommes friands de nouveaux services, nous permettant d'aller toujours plus vite et de faire des économies importantes. Mais pas aux dépens de la sécurité, qui reste un point essentiel dans cette métamorphose numérique. Car la véritable inquiétude pour les organismes est la perte du patrimoine informationnel. Pour l'ANSSI, l'agence nationale de la sécurité des systèmes d'information, la sécurité du numérique est l'affaire de tous. Dirigeants, responsables informatiques, employés : chacun est responsable et joue un rôle face à la multiplication des menaces dans le numérique. Aujourd'hui, la cyber sécurité est indispensable pour créer la confiance, gage de réussite dans la transition numérique de tous. Il convient de savoir gérer les crises, d'améliorer l'information des clients et de protéger les données sur toutes les chaînes d'utilisation.

(3) Chiffre avancé par le site la tribune-article : supplement/e-administration-un-developpement-prioritaire-qui-commence-a-porter-ses-fruits

La confiance numérique repose essentiellement sur des bases techniques et juridiques. Elle a besoin de normes, au sens du code civil, c'est-à-dire de règles garantissant les droits et libertés fondamentales auxquelles appartient le droit à la vie privée. Les textes récents en cours d'adoption par le Parlement européen viennent renforcer cette sécurité juridique. C'est notamment le cas du règlement eIDAS sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, qui fait partie de toutes ces normes (Règlement sur la protection des données personnelles, labellisations de la CNIL ou de la FNTC, ...) qui viennent consolider le marché du numérique et renforcer la sécurité des données.

Nous sommes en route vers le tout numérique, vers la dématérialisation totale. Il faut donc trouver les moyens d'assurer une sécurité optimale de nos échanges. Dans ce cadre, le rôle des DSI est majeur, car ils sont les garants de la réussite de la transformation digitale de leurs collectivités.

Zoom sur la règlementation eIDAS : qu'est-ce que c'est ?

Comme nous le soulignions précédemment, de nombreuses normes existent afin de répondre aux attentes des utilisateurs et leur garantir une sécurité optimale. Ainsi, de nombreux organismes œuvrent pour vérifier la qualité des produits mis sur le marché, et proposent des normes de sécurité à valeur juridique probante, comme la réglementation eIDAS.

Le système européen de signature électronique reconnaît en effet la validité et la recevabilité de la SEA. La jurisprudence y est de plus en plus favorable voire encourage ce type de signature, grâce au perfectionnement des mesures de vérification de l'identité et de la sécurisation des documents. Dans ce cadre, le règlement eIDAS fait d'ailleurs de la SEA une garantie suffisante de l'intégrité des documents et des données sur le signataire.

Ce règlement abroge l'actuelle directive sur les signatures électroniques et les éventuelles incohérences dans la législation européenne sur les signatures numériques. Adoptée par le Conseil « Affaires générales » en juillet 2014, la réglementation sur les services de confiance est entrée en vigueur le 1er juillet 2016. L'obligation de reconnaissance mutuelle des identités électroniques (eID) s'appliquera à partir du 2e trimestre 2018. L'eIDAS couvre l'authentification, les sceaux de signature, les services d'envoi en recommandé [électronique] et l'horodatage. Aujourd'hui, il existe différents outils répondant à ces exigences comme par exemple, la web signature, ou signature électronique externalisée. Légale et certifiée (eIDAS, ETSI 102 042 et AC Autorité de Certification), c'est plus qu'une solution de confiance, il s'agit d'une solution sécurisée reconnue au niveau national et européen et par la FNTC (Fédération Nationale de Tiers de Confiance).

Intégrité des preuves générées

La signature électronique doit pouvoir garantir l'intégrité des documents en prouvant que le message n'a pas été modifié ni altéré. De plus, elle doit pouvoir certifier l'authenticité de l'émetteur sans être répudiée. Ainsi, de nombreux processus sont mis en place pour garantir toutes ces exigences.

Dans un système de dématérialisation totale du circuit, tous les documents signés dans un parapheur électronique sont convertis au format PDF et la signature appliquée est de type PADES ou XADES détaché, un format essentiellement utilisé par les marchés publics. Pour les fichiers XML, la signature appliquée est de type XADES.

Grâce à ces garanties, les documents sont verrouillés et infalsifiables et toute modification faite altère leur intégrité. Par exemple, les PDF/A permettent de prouver, grâce à des notifications apposées sur le PDF, que le document n'a pas été altéré depuis sa signature. Ces signatures sont accompagnées par différents types de certificats, qui ont plusieurs niveaux de sécurité (RGS 1, 2 ou 3 étoiles, eIDAS) afin d'émettre et de transmettre les documents en toute sécurité.

Pour finir, des rapports de signature vérifient la validité des signatures. Ces fichiers, émis en fin de circuit, vont reprendre les informations de la signature : Nom du fichier, nom du signataire, autorité de certification qui a émis le certificat, les dates de validité du certificat, la date de signature et le type de signature. Ce document, exportable avec toutes ses informations dans une GED ou dans un SAE (Système d'Archivage Électronique) permet de prouver que le certificat utilisé était valable. Une garantie supplémentaire très appréciée des utilisateurs de signature électronique.

Contact

Vous souhaitez en savoir plus ou nous faire part de vos remarques :
retrouvez-nous sur
www.srci.fr
ou sur les réseaux sociaux

Graphisme : Martine Follut - Crédit photo couverture : Shutterstock © turgaygundogdu - Novembre 2017