Comprendre la signature électronique

LES ENJEUX DE LA DEMATERIALISATION

Pour les entreprises, la transformation numérique représente une formidable opportunité de fluidifier les processus métiers ; elle est devenue un impératif pour qu'elles puissent rester compétitives. Cette transformation s'opère à tous les niveaux : elle demande d'adapter les usages métiers et passe inévitablement par la dématérialisation des flux documentaires.

Pourtant, même si le document électronique se démocratise, trop souvent ces processus ne sont que partiellement automatisés. Les parcours digitaux sont notamment interrompus pour signer les documents de façon manuscrite.

Intégrer la signature électronique dans la chaine de dématérialisation permet de donner une valeur légale aux documents numériques. La signature électronique garantit une expérience 100% numérique aux clients, partenaires et utilisateurs de l'entreprise.

Pour vous accompagner dans vos réflexions et dans la mise en œuvre de votre projet de signature électronique, il est utile de faire le point sur les enjeux de la signature électronique et les bénéfices attendus, les types et les niveaux de signature utilisés en Europe.

DEFINITION DE LA SIGNATURE ELECTRONIQUE

Il est important de comprendre ce que la signature électronique n'est en aucun cas un «scan» de la signature manuscrite.

La signature électronique est un procédé technique dans lequel une personne (le signataire) appose son accord à valeur juridique sur un document électronique. Il y a donc réunion de 3 éléments : le document, le signataire et l'outil de signature.

Si l'outil nécessaire à la signature manuscrite n'est ni plus ni moins qu'un stylo, les outils de signature électronique sont multiples, autant que les moyens techniques nécessaires à leur réalisation. Il s'agit dans la majorité des cas d'un certificat numérique porté sur différents supports (carte à puce, clé USB, carte d'identité, PC, smartphone, etc.) qui a pour fonction d'identifier le signataire d'une part, et de sceller le document pour en garantir l'intégrité d'autre part.

En résumé la signature électronique permet plusieurs choses, se montrant bien plus efficace que son pendant manuscrit :

- authentifier le signataire ;
- garantir l'intégrité du document ;
- assurer la non-répudiation (l'émetteur du document ne peut nier l'avoir envoyé).

LES ENJEUX DE LA SIGNATURE ELECTRONIQUE

Vecteur de performance, la signature électronique transforme durablement la façon de fonctionner d'une entreprise. Prendre le temps de structurer un projet est essentiel. Cette démarche permet d'identifier les freins, de cadrer les attentes et de fédérer les équipes informatiques et métiers. Vous augmentez ainsi vos chances de succès et pérennisez les bénéfices du changement.

- **Identifier et fixer les objectifs** pour dresser un cahier des charges précis et impliquer les utilisateurs internes, il est important de déterminer les objectifs d'un projet de signature électronique.

- **Offrir un parcours 100% numérique** en B2C ou en B2B, pour la souscription d'un service en ligne, la vente en ligne, la souscription d'un contrat d'assurance ou d'un prêt, la validation d'un document comptable.

- **Fluidifier les processus internes** et recentrer les équipes sur des tâches à forte valeur ajoutée : pour les entreprises qui traitent de larges volumes de documents (factures, bons de commandes, contrats…).

- **Renforcer la sécurisation des échanges** et plus spécifiquement ceux qui demandent un haut niveau de confidentialité et de sécurité : comptes rendus médicaux, actes d'huissiers, actes notariés, réponses aux appels d'offres publics.

- **Former et fédérer le groupe projet** qui mobilise des ressources transverses dans l'entreprise comme la DSI, la Direction Juridique, la DRH, la Direction Marketing, la Direction Commerciale. Former une équipe pluri-métiers permettra de fédérer toutes les parties prenantes autour du projet. Les rôles de chacun se complètent et sont nécessaires au succès du projet. Le chef de projet est moteur pour rythmer et animer le déploiement de la signature électronique.

CHOISIR SON MODE DE SIGNATURE ÉLECTRONIQUE

La signature électronique est un gage de confiance pour les échanges numériques. Ses caractéristiques en font un outil qui apporte davantage d'efficacité, de fiabilité et de sécurité qu'un processus manuel. En effet, elle permet d'identifier avec certitude le signataire (particulier ou entreprise), de sceller son engagement et de garantir l'intégrité du document signé.

Ainsi la signature électronique authentifie les signataires qui ont donné leur consentement ; ces derniers ne pourront nier qu'ils ont signé le document scellant leur accord.
Avec la réglementation européenne eIDAS qui définit trois niveaux de signature, comment choisir le mode de signature le plus adapté aux documents et aux projets de l'entreprise ? Il n'est pas toujours simple de répondre à cette question.
Vous trouverez ci-après des conseils pragmatiques pour vous aider dans vos arbitrages.

Le fonctionnement de la signature électronique

Pour signer un document électroniquement, il est nécessaire de respecter un processus qui garantira la valeur légale du document. Il repose notamment sur :

- ✓ Un certificat électronique, délivré par un Prestataire de Certification Electronique (tel que celui fournit par CertEurope), qui agit comme une véritable carte d'identité numérique pour authentifier le(s) signataire(s).

- ✓ Un outil de signature électronique permettant de sceller l'engagement du signataire et de garantir l'intégrité du document, en conformité avec la réglementation européenne.

Mais attention : être en possession d'un certificat électronique n'est pas suffisant pour signer.

- ✓ Si l'entreprise répond à un appel d'offre des marchés publiques, c'est le profil d'acheteur qui guidera l'entreprise dans la soumission de ses pièces et qui, en quelque sorte, les signera pour le compte de l'entreprise.

- ✓ Si l'entreprise doit dématérialiser, par exemple un contrat par voie électronique, elle devra au préalable être en possession d'un outil de signature. Il en existe beaucoup sur le marché. e-btp préconise eDocparaph car il permet de faire valider en interne les documents à valeurs probantes, de les faire signer à l'intérieur de l'entreprise par les personnes habilitées mais également à l'extérieur de l'entreprise par les co-signataires.

Selon la nature de vos documents, leur valeur légale et le degré de sécurisation que votre entreprise souhaite obtenir, vous aurez le choix entre trois types de signature et trois niveaux de certification imposés par le règlement eIDAS.

Le règlement eIDAS concerne principalement les organismes du secteur public et les prestataires de services de confiance établis sur le territoire de l'Union européenne. Il instaure un cadre européen en matière d'identification électronique et de services de confiance, afin de faciliter l'émergence du marché unique numérique. Il couvre notamment le sujet de la signature électronique, et abroge la directive 1999/93/CE. L'ANSSI est l'un des organismes nationaux chargés de la mise en œuvre de ce règlement.

Les 3 formats de signature

Le format utilisé dépend essentiellement du type de document à signer.

Le format **PADES** (PDF Advanced Electronic Signatures) est comme le nom l'indique prédisposé à la signature des documents PDF. Il est adapté à la dématérialisation des, factures, des commandes, des contrats. Le visualiser intègre généralement la vérification des signatures.

Le format **CAdES** (CMS Advanced Electonic Signatures) est particulièrement adapté à du contenu binaire car il ne nécessite pas de transformation (exemple : vidéos, images, programmes, etc).

Le format **XAdES** (XML Advanced Electronic Signatures) présente l'avantage de gérer nativement les co-signatures de même niveau. Particulièrement adapté à du contenu XML car celui-ci apparaît en clair. Il est très utilisé par l'administration française et par les profils d'acheteurs.

Les trois niveaux de garantie selon eIDAS

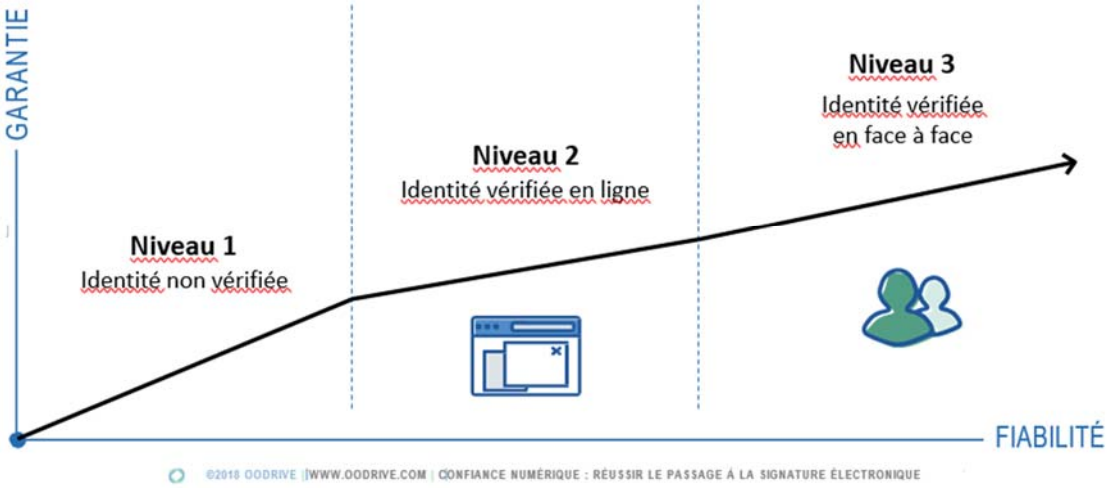
Depuis le 1er juillet 2016, eIDAS renforce et uniformise les transactions électroniques des 28 états membres de la communauté européenne. Le règlement propose 3 niveaux de fiabilité et de garantie pour la signature électronique : simple, avancée et qualifiée (*voir le tableau de la page suivante*).

Quelle signature pour quel document ?

Signature simple	Signature avancée	Signature qualifiée
Risque juridique faible à moyen Contrat d'assurance, souscription à un service, note de frais		**Risque juridique élevé** Facture, Réponse aux appels marché public, validation d'opération bancaire B2B

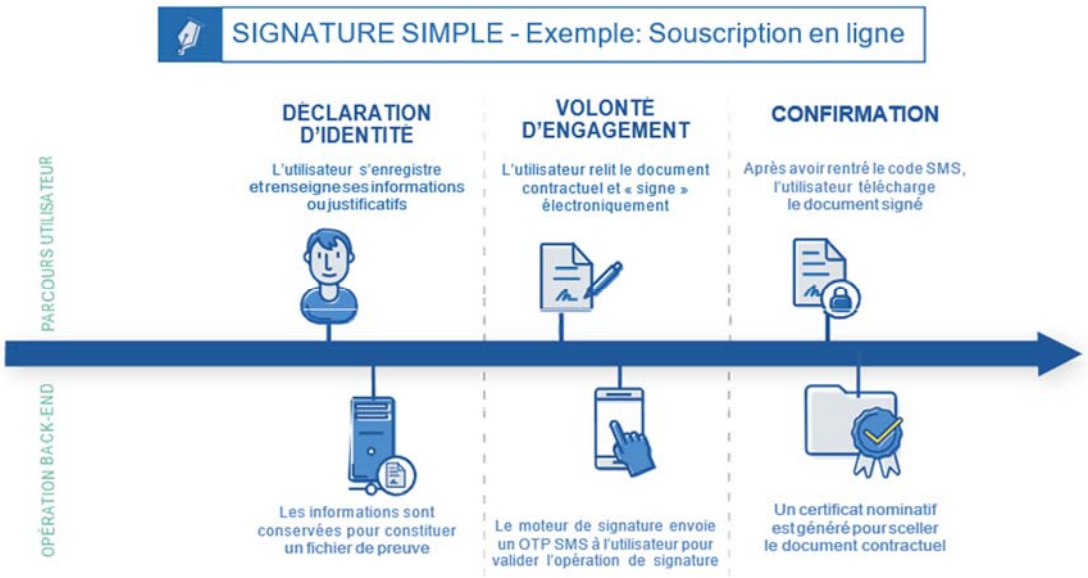
La nouvelle règlementation européenne eIDAS encadre l'identité numérique, harmonise et sécurise les échanges. Les trois niveaux de signature proposés sont des services opérés selon un procédé conforme au cadre réglementaire national du RGS ainsi qu'à la réglementation européenne eIDAS.

Les niveaux de garantie et de fiabilité de la signature électronique



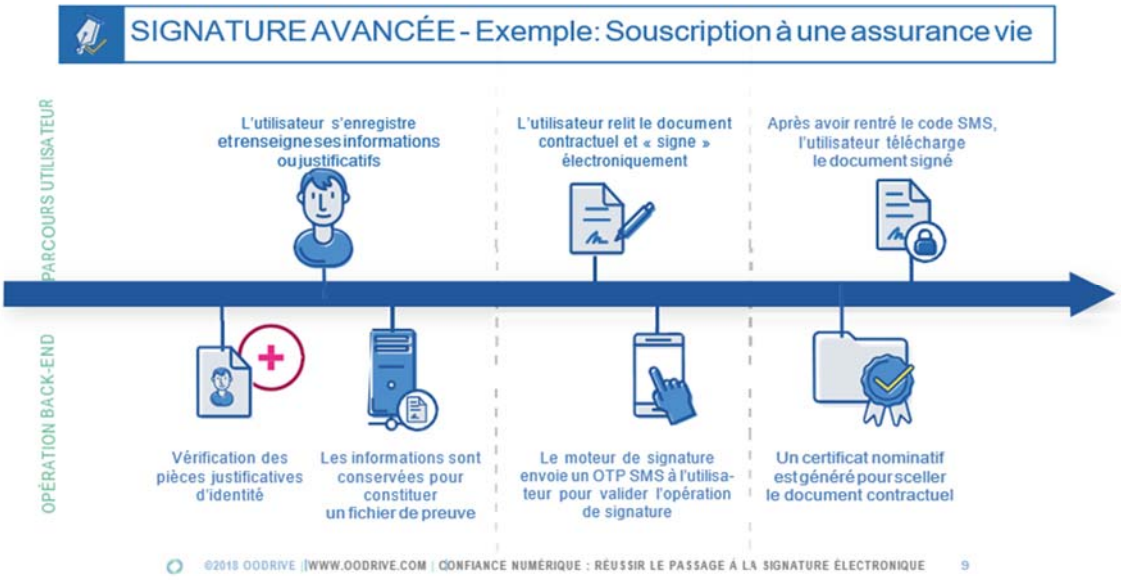
Les différents niveaux de signature

Le niveau 1



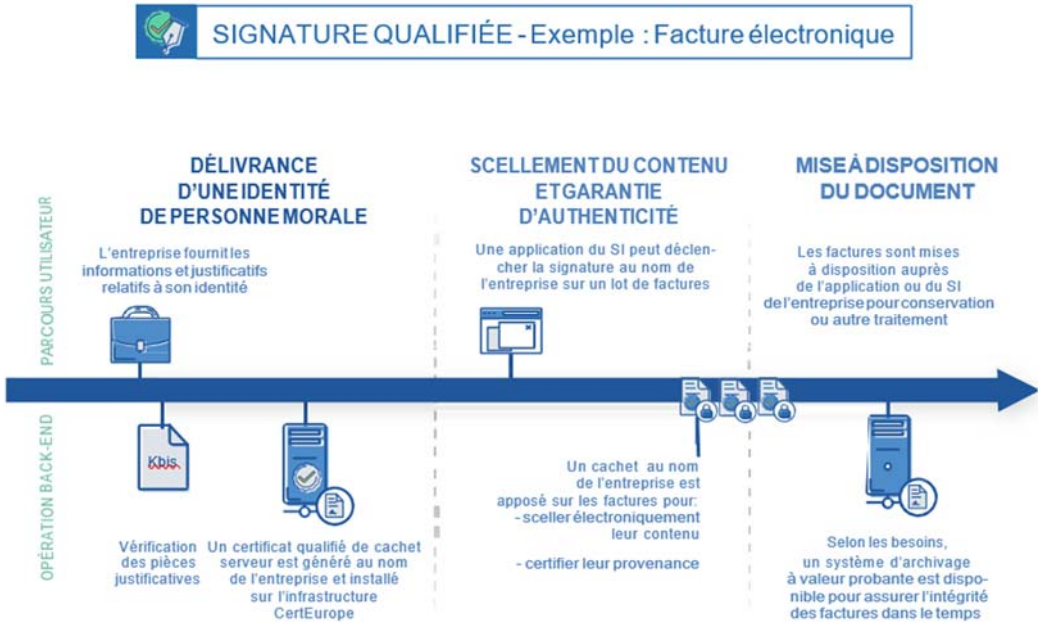
Il n'y a pas de contrôle physique du signataire. Les éléments de preuve sont constitués par le signataire au moment de son identification sur la plateforme de signature. Le contrôle se fait simplement par l'envoi SMS d'un OPT (one time password) pour valider l'opération de signature.

Le niveau 2



Le signataire doit au préalable envoyer des pièces validant son identité (passeport, facture, carte d'identité…) à l'entreprise pour constituer des éléments de preuve avant de pouvoir signer. Le contrôle se fait simplement par l'envoi SMS d'un OPT (one time password) pour valider l'opération de signature.

Le niveau 3



La signature qualifiée est utilisée pour identifier une personne morale. Elle se présente sous forme de cachet serveur délivré par une autorité de certification pour signer les bulletins de salaire et les factures par exemple. Elle se présente également sous forme de certificat électronique (clé USB) qui est délivré en vis-à-vis par une autorité de délivrance (AED) telles que le sont les Fédérations Départementales du Bâtiment. Elle est obligatoire pour signer les pièces des Marchés Publics.

L'OFFRE E-BTP

e-btp conseille et accompagne les entreprises du bâtiment et de travaux publics dans la mise en place de processus de dématérialisation.
Ci-dessous, le tableau qui résume les services que propose aujourd'hui le portail www.e-btp.fr dans le domaine de la délivrance de certificat et de la signature en ligne.

CERT EUROPE e-btp	Certificat Certeurope, valable 3 ans, contenant le protocole RGS ** et eIADS, délivré en vis-à-vis par les Fédérations départementales du bâtiment et les Fédérations régionales des travaux publics pour signer les pièces de marché, les factures, les bulletins de salaires…..
eDocParaph	Parapheur électronique pour valider, signer les documents qui engagent l'entreprise (devis, commande, facture, contrats, avis de situation…/…) et les archiver automatiquement dans les coffres forts numériques certifiés des différents signataires. Il supporte : • la signature électronique par OTP (one time password) reposant sur certificat délivré par eDocGroup associé à une code SMS ; • la signature électronique de niveau RGS2* et eIADS (support du certificat Certeurope délivré par e-btp).

QUESTIONS-REPONSES

Comment se matérialise la signature électronique PADES d'un document ?
Une fois le document ouvert dans un visualisateur PDF, il est facile de repérer les signatures et de vérifier que le document n'a pas été modifié depuis la signature car la signature fait partie intégrante du document.

Comment se matérialise la signature électronique XADES d'un document ?
La signature se matérialise par un second fichier dont l'extension est ".xml". Exemple : Un fichier intitulé "Note.pdf", s'il est signé, sera accompagné d'un second fichier intitulé "Note.pdf.xml" En cas de communication, vous devez founir le fichier original (note.pdf) et son fichier de signature (note.pdf.xml).

Comment se matérialise la signature électronique CaDES d'un document ?
Le jeton de signature porte l'extension « .p7s ». Un fichier intitulé "Note.pdf", s'il est signé en CaDES, sera accompagné d'un second fichier intitulé "Note.pdf.p7s". En cas de communication, vous devez fournir le fichier original (note.pdf) et son fichier de signature (note.pdf.p7s).

La signature électronique CaDES se voit-elle ?
La signature électronique ne se matérialise pas par une trace visible sur un document électronique. Elle est représentée par un second fichier dont l'extension est .p7s.

Comment vérifier une signature électronique CaDES ?
Pour vérifier la validité d'une signature électronique CaDES, il convient de comparer le fichier original et le fichier de signature qui l'accompagne. Exemple: comparer le fichier note.pdf avec le fichier de signature note.pdf.p7s. Si la comparaison donne un résultat identique, la signature est alors valide.

Où s'enregistre la signature électronique CaDES ou XADES du fichier que je viens de signer?
La signature électronique d'un fichier sera enregistrée par défaut dans le même répertoire que le fichier original.

Que signifie eIDAS ?
Electronic **ID**entification **A**uthentication and trust **S**ervices (eIDAS) est le règlement sur l'identification électronique et les services de confiance pour les transactions électroniques au sein de l'Union Européenne. Il remplacera en 2020 le règlement RGS. La présence du certificat eIDAS permet d'assurer une continuité de service d'authentification et de signature pour les 3 ans à venir.

Que signifie RGS ** ?
RGS ** est le dispositif de protection des éléments secrets qualifié au niveau renforcé par le Référentiel Général de Sécurité. Ce protocole que l'on trouve dans les certificats électroniques va disparaitre en 2020 au profit du protocole eIADS.