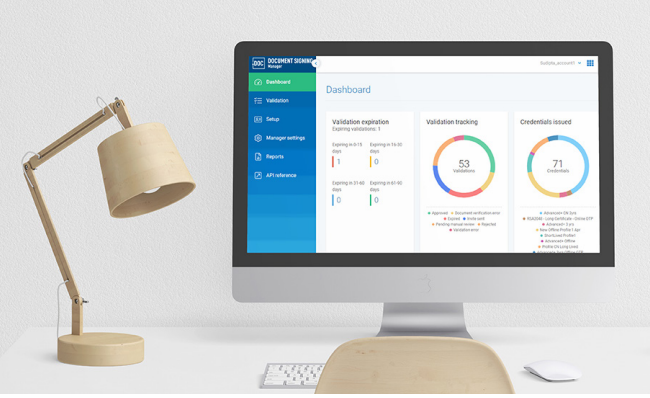
UNE CONFIANCE GARANTE DE VOTRE CONFORMITÉ LÉGALE ET RÉGLEMENTAIRE

Confiance et identité : les deux piliers de la dématérialisation

À mesure que les documents numériques se substituent aux processus papier, le besoin en solutions de signature fiables ne cesse de croître. Sans cette confiance, les entreprises, les pouvoirs publics et les particuliers n'ont aucune certitude quant à la validité et la légitimité des signataires, qu'elles soient personnes physiques ou morales. Le risque de manipulation ou de fraude sur les transactions, accords et contrats existe bel et bien.

DigiCert Document Signing Manager : identité et confiance

Même dans le domaine de la signature sécurisée, toutes les solutions de signature de documents ne se valent pas. DigiCert Document Signing Manager s'appuie sur une infrastructure à clés publiques (PKI), une technologie éprouvée de chiffrement, d'authentification et de gestion des identités. Ainsi, le document est signé à l'aide d'une identité sécurisée et chiffrée qui non seulement garantit au destinataire que le signataire est bien qui il prétend être, mais aussi que le contenu n'a fait l'objet d'aucune altération pendant sa transmission.



Qu'est-ce qu'un prestataire de services de confiance qualifié ?

En matière de sécurité des signatures et des identités, les réglementations établies par l'Union européenne et l'Institut européen des normes de télécommunications (ETSI) constituent la référence mondiale absolue pour les services de signature et la protection des identités. Le prestataire de services de confiance qualifié (PSCQ) représente le niveau de garantie maximale de ce standard. Par son rachat de QuoVadis, DigiCert est aujourd'hui reconnu par l'UE et l'ETSI comme remplissant les normes de signature fixées par le règlement eIDAS de l'UE. DigiCert entre ainsi dans le club très fermé des quelques PSCQ à l'échelle planétaire. L'entreprise satisfait également à toutes les exigences de signature qualifiée en Suisse, selon la loi ZertES en vigueur dans la confédération.

De fait, la signature de document DigiCert + QuoVadis est reconnue comme équivalente à la fois à une signature manuscrite et, dans de nombreuses juridictions, à une preuve d'identité au même titre qu'une pièce d'identité délivrée par une administration.

En tant que PSCQ, DigiCert et ses solutions de signature respectent, voire dépassent, les standards les plus stricts de sécurité des signatures, d'authentification et de gestion des identités partout dans le monde.

À chaque type de document son niveau d'assurance

Les critères de reconnaissance et de validation des signatures électroniques varient selon le niveau de garantie requis par les particuliers ou les organisations.

Type de signature	Signature électronique simple (SES)	Signature électronique avancée (ADS/AATL)	Signature électronique qualifiée (QES)
Exigences relatives aux signatures	Signature électronique apposée par un signataire sur un document en guise d'accord ou d'approbation. Cela peut notamment consister en une image scannée ou un clic sur le bouton « J'accepte ».	Signature électronique qui satisfait à des exigences particulières, offrant ainsi une vérification renforcée de l'identité des signataires, de la sécurité et de l'intégrité des documents.	Signature électronique conforme aux exigences avancées, et certifiée par un prestataire de services de confiance qualifié (PSCQ) figurant soit sur la liste de confiance de l'UE (ETL) et accrédité par un État membre, soit sur la liste de confiance suisse. La signature électronique avancée est souvent considérée comme l'équivalent d'une signature manuscrite.
Exigences de garantie et devalidation des identités	Aucune	Association de la signature à un signataire unique Identification possible, mais pas garantie, du signataire à l'aide d'une pièce d'identité officielle Création de la signature à l'aide des données personnelles d'identité contrôlées exclusivement par le signataire Association de la signature à des données de signature dont le moindre changement est détectable Qualification de la signature pour Adobe Approved Trust List (AATL)	Il incombe au PSCQ d'établir l'intégrité et l'authenticité du signataire : 1. Les données de création de la signature électronique sont sûres et confidentielles 2. Le PSCQ peut prouver l'identité du signataire à l'issue d'une interaction en face à face ou de processus de vérification tout aussi rigoureux
Exemples	Documents d'onboarding de nouvelles recrues Contrats commerciaux entre personnes morales Contrats de particuliers Contrats de licence de logiciels	Contrats de crédit à la consommation ou prêts bancaires Conventions collectives Contrats d'embauche	Contrats immobiliers de bail, de transfert ou d'achat Documents afférents au droit de la famille Statuts de sociétés
Niveau de garantie eIDAS	Faible garantie	Garantie substantielle	Garantie élevée
Niveau de validation	Aucune validation	Validation partielle	Validation (rigoureuse) maximale

Deux signatures disponibles

Personne physique (eSignature)

En tant que personne physique, un signataire individuel peut facilement sécuriser la signature de documents personnels : transactions immobilières, documents bancaires et informations confidentielles présentes notamment dans les dossiers médicaux.

Personne morale (eSeal)

Dans le cas d'une entreprise ou d'une administration, un fondé de pouvoir peut signer des documents au nom de l'entreprise ou de l'entité, tout en veillant au maintien de l'intégrité des informations qu'ils contiennent. La signature groupée ou en masse est disponible en option.

De l'avantage de la signature de documents

Avec DigiCert Document Signing, vos clients disposent d'une solution tout-en-un pour apposer leur signature électronique, en tout lieu et à tout moment. Certificats, technologies, automatisation... autant d'options proposées dans une double optique de compétitivité et d'amélioration de l'expérience client.

Fonctionnalités

Personnalisation des workflows de signature
Instaurez des workflows complets intégrant un large choix de technologies (Ascertia SigningHub, Adobe Sign ou DocuSign).

Validation facile
Autorisez vos clients à créer une identité à distance en quelques minutes seulement à l'aide de Verify by DigiCert piloté par IDnow.

Gestion simplifiée des clés
Protégez vos clés au sein d'un dispositif de création de signature qualifiée (QSCD), hébergé dans un environnement fiable.

Rationalisation des tâches administratives
Simplifiez le travail de gestion des administrateurs en centralisant la politique et le contrôle pour les utilisateurs et les signataires.

Suivi détaillé
Recevez des rapports et vérifiez les pistes d'audit afférentes aux réglementations et politiques des entreprises et des pouvoirs publics.

Sécurité renforcée
Optez pour l'authentification à deux facteurs et renforcez votre sécurité.

Intégration facile
Intégrez des services web et des workflows tiers comme Adobe Sign, Ascertia Signing Hub, etc.

Déploiement flexible
Déployez votre solution sur site ou en mode cloud (hébergé).

Principaux avantages

- Faites des économies de papier et réduisez les frais administratifs et de port
- Offrez une expérience fidélisante en simplifiant les exigences de création de compte et de signature pour vos clients
- Gagnez du temps sur vos transactions en finalisant les signatures en quelques minutes seulement, contre plusieurs jours auparavant
- Renforcez la sécurité des transactions de haute valeur
- Instaurez la confiance avec des signatures juridiquement valides et contraignantes
- Assurez la continuité de votre activité tout en bâtissant un avantage concurrentiel
- Respectez la gouvernance et les réglementations mondiales et sectorielles

Spécifications techniques et intégrations

Protocoles de signature électronique

- API REST
- API CSC

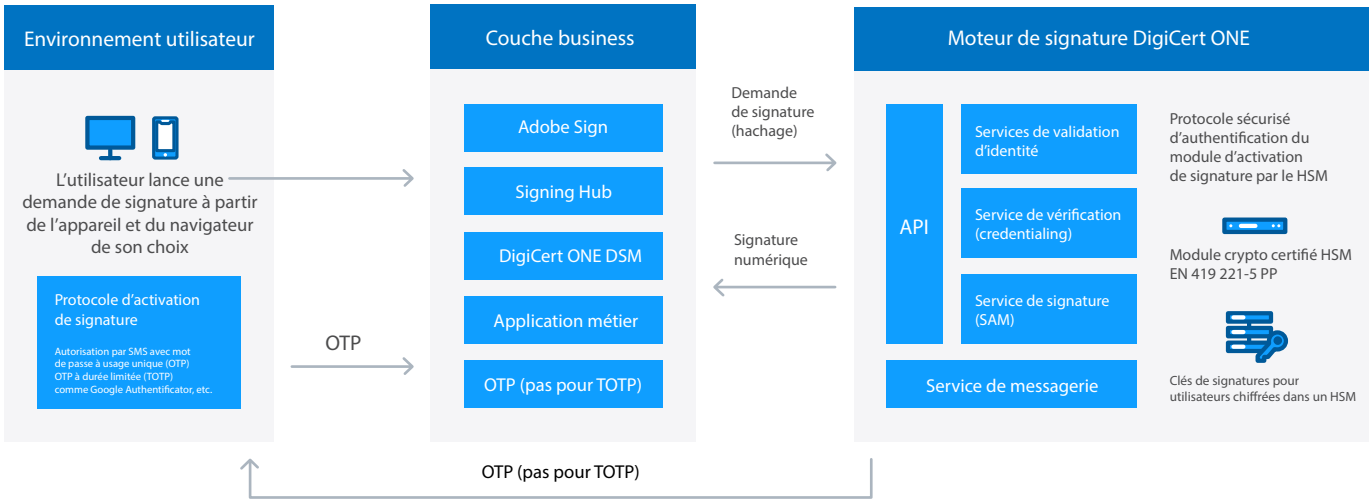
Intégrations disponibles

- Adobe Sign
- Ascertia SigningHub
- DocuSign

Compatibilité avec

- Microsoft Office®
- Adobe® Acrobat et Adobe Reader
- LibreOffice®
- Open Office™
- Autres solutions tierces telles que DocuSign
- En prime, prise en charge d'une grande variété de formats : PDF, ODF, DOCX et XML

Architecture de signature cloud et à distance



DigiCert® ONE

Document Signing Manager fait partie intégrante de DigiCert ONE, une solution nouvelle génération de gestion holistique de l'infrastructure PKI . Grâce à son architecture pointue basée sur les containers, DigiCert ONE permet d'effectuer des déploiements rapides dans n'importe quel environnement, de délivrer de nouveaux services en un rien de temps et de gérer les utilisateurs et les appareils de votre entreprise, quelle que soit sa taille.

Pour de plus amples informations sur DigiCert® Document Signing Manager, contactez l'un de nos experts en documents PKI à l'adresse docsigning@digicert.com

L'assurance d'un leader du PKI

Chez DigiCert, nous sommes toujours restés fidèles à ce mot d'ordre : A better way. Plus qu'un simple slogan, cette quête perpétuelle d'un meilleur moyen de sécuriser Internet est profondément ancrée dans notre ADN. Voilà pourquoi des entreprises du monde entier font confiance à nos certificats pour sécuriser des millions de transactions par jour. C'est aussi pour cela que notre support et nos services atteignent les taux de satisfaction client les plus élevés du marché. Et c'est enfin pourquoi nous continuons à concevoir des solutions de pointe pour un avenir plus

© 2021 DigiCert, Inc. Tous droits réservés. DigiCert est une marque déposée de DigiCert, Inc., aux États-Unis et dans d'autres pays. Toutes les autres marques, déposées ou non, sont des marques commerciales de leurs détenteurs respectifs.