digicert

DIGICERT® DOCUMENT TRUST MANAGER

Signatures numériques, cachets électroniques et horodatages pour protéger vos documents numériques partout dans le monde.

Continuité des activités où qu'elles s'exercent

DigiCert® Document Trust Manager permet aux entreprises d'obtenir des signatures numériques, des sceaux électroniques et des horodatages vérifiés et conformes qui couvrent un vaste éventail de cas d'usage à travers le monde. DigiCert aide les entreprises à adhérer en toute confiance aux réglementations sectorielles et locales aux États-Unis, dans l'Union européenne (UE), au Royaume-Uni, en Suisse et dans bien d'autres pays.

Conformité à l'échelle mondiale

Dans de nombreux pays, la loi exige des signatures numériques haute assurance adossées à des certificats émis par un prestataire de services de confiance (PSC) agréé dans la région concernée. Par exemple dans l'UE, au Royaume-Uni ou en Suisse, une signature électronique qualifiée (QES) ne peut être émise que par un prestataire de services de confiance qualifié (PSCQ) comme DigiCert. Les signatures numériques haute assurance de DigiCert sont conformes aux spécifications de l'AATL (Adobe Approved Trust List), au règlement 910/2014 de l'UE sur l'identification électronique et les services de confiance pour les transactions électroniques (eIDAS), à l'équivalent britannique du règlement eIDAS et à la norme ZertES en Suisse.

Principaux avantages

- Accélération des processus de signature de documents à distance, sans compromis sur la sécurité et la conformité
- Compatibilité avec les applications leaders de signature électronique telles qu'Adobe, Ascertia et DocuSign
- Niveau maximal d'authentification des identités appliquée aux signatures électroniques
- Conformité aux réglementations sectorielles de type Know Your Customer (KYC) ou Anti-Money Laundering (AML)
- Obtention de signatures électroniques vérifiées aux États-Unis, dans l'UE, au Royaume-Uni, en Suisse et dans bien d'autres pays

Confiance numérique, la carte maîtresse

Signez vos documents à tout moment, en tout lieu et sur n'importe quel appareil mobile moderne. Notre solution ultraflexible couvre les identités, les certificats et les technologies numériques, combinés à des options d'automatisation pour renforcer la confiance dans les documents numériques. Au menu de Document Trust Manager :

Signatures numériques
Une signature numérique ou électronique s'appuie sur un certificat numérique lié cryptographiquement au champ de signature à l'aide d'une infrastructure à clés publiques (PKI). Communément désigné par le terme d'identité numérique (ID numérique), chaque certificat numérique s'applique à un seul individu et est obtenu après vérification de son identité.

Cachets électroniques
Un cachet électronique est une signature numérique utilisée par une entité juridique telle qu'une entreprise ou une organisation pour certifier l'origine, l'authenticité et l'intégrité de documents. Les cachets électroniques peuvent fournir une preuve juridique solide de la provenance et de l'intégrité du document. Ils sont couramment utilisés dans les systèmes automatisés pour traiter des processus à forts volumes comme la facturation en masse ou les fiches de paie.

Horodatages
Un horodatage correspond à l'enregistrement signé numériquement de l'heure et de la date d'un événement. Il renforce la validité et l'intégrité d'un document, d'une signature ou d'un cachet électronique à un moment précis.

Confiance intégrée aux signatures électroniques

Toutes les signatures électroniques ne se valent pas. Le terme renvoie d'ailleurs à une multitude d'éléments qui vont d'une simple case à cocher ou d'initiales griffonnées sur une tablette à une signature numérique haute assurance dans le cloud, sous-tendue par une vérification rigoureuse de l'identité effectuée par une autorité accréditée comme DigiCert. Ces signatures numériques de confiance relient réellement le signataire à un document spécifique et vous aident à protéger vos transactions électroniques les plus importantes pour votre entreprise, où qu'elles s'effectuent.

Le tableau suivant présente les différentes signatures électroniques disponibles, ainsi que leurs attributs de sécurité, leur niveau de conformité et d'assurance :

Type de signature	**Signature électronique**	**Signature numérique (AATL)**	**Signature numérique (avec identifiant réglementé/prestataire qualifié)**
Description	Terme générique qui renvoie à un processus électronique indiquant l'acceptation d'un accord ou d'un enregistrement. Dans sa forme la plus basique, une signature électronique peut correspondre à un nom saisi dans un champ prévu à cet effet ou à une case à cocher.	Signature électronique plus sécurisée qui requiert l'utilisation d'un identifiant numérique émis par un prestataire de services de confiance (PSC), conforme aux exigences spécifiques de l'AATL (Adobe Approved Trust List) en matière de vérification et de sécurité des identités.	Signature électronique ultrasécurisée qui requiert l'utilisation d'un identifiant numérique réglementé émis par un PSC certifié dans une région spécifique, tel qu'un prestataire de services de confiance qualifié (PSCQ) dans l'UE ou en Suisse.
Confiance publique	Aucune exigence spécifique	Reconnue par Adobe Acrobat et Reader	Reconnue par Adobe Acrobat et Reader*
Identité numérique	Pas obligatoirement liée de manière unique au signataire	Preuve de l'identifiant numérique unique du signataire liée cryptographiquement au champ de signature (PKI)	Preuve de l'identifiant numérique unique du signataire liée cryptographiquement au champ de signature (PKI)
Niveau de garantie	**Garantie faible** Vérification faible ou limitée des identités	**Garantie substantielle** Vérification obligatoire des identités	**Garantie élevée** Vérification rigoureuse des identités en personne ou de manière équivalente
Authentification à deux facteurs (2FA)	Pas obligatoire pour la signature d'un document	Obligatoire pour la signature d'un document	Obligatoire pour la signature d'un document
Validité à long terme	Pas obligatoire ; peut être incluse avec une solution de workflow de signature	Cachet avec témoin anti-effraction et horodatage appliqué au document signé	Cachet avec témoin anti-effraction et horodatage appliqué au document signé
Équivalent d'une signature manuscrite	Non	Non	Conforme aux réglementations spécifiques appliquées dans l'UE, au Royaume-Uni et en Suisse*

Fonctionnalités clés

Preuve de signature
Vérification rigoureuse de l'identité du signataire, de l'heure de la signature et de l'authenticité des documents liée cryptographiquement aux contrats signés.

Intégrations évolutives
Compatibilité avec des solutions leaders de workflows de signature tels qu'Adobe Acrobat Sign, Ascertia SigningHub et DocuSign.

Vérification des identités à distance
Identification des clients, citoyens et salariés à l'aide d'appareils mobiles modernes et de pièces d'identité.

Options de déploiement flexibles
Déploiement de Document Trust Manager sous forme de solution hébergée, on-premise ou hybride.

Solutions personnalisées
Création d'une instance privée de Document Trust Manager ou utilisation d'une API Cloud Signature Consortium (CSC) pour s'intégrer à des solutions de signature personnalisées.

Contrôle centralisé
Simplification de l'administration des identités et certificats numériques à l'aide de la plateforme DigiCert ONE.

Clés de signature sécurisées
Protection des clés privées utilisées pour les signatures numériques dans des modules de sécurité matérielle (HSM) accrédités et des dispositifs de création de signature qualifiée (QSCD), hébergés dans des environnements sécurisés et certifiés aux États-Unis, dans l'UE et en Suisse.

Protégez vos documents numériques

À l'heure où le support papier disparaît au profit du numérique, les entreprises déploient des solutions de sceaux électroniques de confiance pour protéger l'authenticité des documents. Combinée à des signatures numériques haute assurance, l'application de sceaux électroniques aux contrats, accords et autres documents numériques protège votre entreprise du coût engendré par une cyberattaque ou une fraude potentielle sur vos transactions électroniques.

Document Trust Manager vous aide à sécuriser tous vos documents grâce à des sceaux électroniques, des horodatages et des signatures numériques garantes d'un niveau maximal d'authentification des identités.

DigiCert ONE, plateforme garante de confiance numérique

DigiCert Document Trust Manager fait partie intégrante de DigiCert ONE, une plateforme qui unifie les solutions DigiCert de confiance numérique sur une architecture containerisée de nouvelle génération. Ses caractéristiques : l'évolutivité, la flexibilité de déploiement, une rentabilisation accélérée et une gestion PKI unifiée.

À vous de jouer

Pour en savoir plus sur DigiCert® Document Trust Manager, contactez votre responsable de compte DigiCert ou écrivez-nous à l'adresse sales@digicert.com.