

Fiche technique sur le système de signature électronique de documents

DocuSign eSignature

Le Groupe de la Banque mondiale a adopté le système de signature électronique **DocuSign**. Ce dernier permet d'envoyer et de signer des documents par voie électronique, aisément et de manière sécurisée à partir d'un ordinateur ou d'un appareil mobile quelconque.

1. Informations générales sur le processus de signature

- Le système de signature électronique DocuSign eSignature est un modèle de logiciel en tant que service (SaaS) en nuage.
- La messagerie électronique est le moyen le plus couramment utilisé pour obtenir des signatures avec le système DocuSign : celui-ci envoie à chaque signataire un courriel contenant un lien sécurisé donnant accès à l'enveloppe qui doit être signée.
- Les personnes devant signer des documents envoyés par le Groupe de la Banque mondiale qui se sont enregistrés auprès de DocuSign doivent se connecter – au moyen de leur nom d'utilisateur et de leur mot de passe, ou d'un moyen d'identification unique si l'organisation pour laquelle ils travaillent en ont un – pour lire et signer le document. Les signataires qui ne sont pas enregistrés auprès de DocuSign peuvent simplement cliquer pour voir et signer le document.
- Il est important de ne pas transférer à d'autres correspondants les courriels de DocuSign car ces derniers sont exclusivement destinés aux personnes auxquelles ils sont adressés. L'emploi de codes d'accès et de méthodes de vérification de l'identité peut réduire le risque que des personnes autres que les destinataires prévus lisent les documents et prennent des mesures les concernant.
- Les éventuels signataires doivent lire une note d'information sur les documents et les signatures électroniques (rédigée par les départements juridiques de la BIRD, d'IFC, de la MIGA et du CIRDI) et indiquer leur agrément avant de pouvoir consulter le document qui leur est transmis et le signer par voie électronique.

2. Informations sur les questions techniques et de sécurité

- Les documents transmis par le Groupe de la Banque mondiale sont chiffrés (norme de chiffrement AES pour les méthodes conformes aux normes FIPS les plus récentes) par des [dispositifs de sécurité](#) installés dans nos centres de données et protégés par nos pare-feu institutionnels. Le vendeur, DocuSign, n'a, de ce fait, jamais accès aux documents que nous soumettons.
- DocuSign utilise la technologie PKI (infrastructure à clés publiques) validée par un certificat X.509. L'Autorité de certification assure la sécurité des clés. La Banque mondiale ne maintient ni ne conserve aucune clé utilisée pour les signatures et ne conserve aucune des informations sur l'identité des personnes qui se sont enregistrées.
- Le Groupe de la Banque mondiale retire ses documents du nuage du vendeur à l'issue d'une période de 90 jours. À ce stade, tous les documents sont éliminés des systèmes de DocuSign. Tous les

documents signés sont stockés dans un système de fichiers institutionnels du Groupe de la Banque mondiale, et administrés conformément à la politique de conservation et d'élimination des documents de l'institution au lieu de demeurer dans le nuage du vendeur.

- Des informations sur la sécurité du processus DocuSign eSignature sont disponibles sur le site Web [Trust Center](#) du prestataire
 - DocuSign eSignature utilise la technologie PKI validée par un certificat X.509.
 - DocuSign est conforme à la norme ISO 27001, aux normes SOC 1 Type 2 et SOC 2 Type 2, et à la norme de sécurité des données PCI (DSS).
 - [DocuSign est conforme au règlement RGPD](#).
- DocuSign suit les meilleures pratiques en vigueur dans le secteur pour procéder à la séparation logique des données des différents clients et chiffrer ces dernières — toutes les opérations d'accès aux données et de transfert de ces dernières utilisent HTTPS et d'autres protocoles sécurisés, notamment SSL, SSH, IPsec, SFTP, ou passent par des réseaux sécurisés pour l'apposition de la signature et du cachet électroniques.
- Les destinataires peuvent bénéficier d'un niveau de sécurité supplémentaire lors de la signature en utilisant un [code d'accès](#), par exemple un code valable une seule fois, qu'il leur faut entrer avant de pouvoir voir et de signer le document. Les codes d'accès offrent un moyen simple de renforcer le degré de confidentialité et de non-répudiation. Seuls la personne envoyant le document et le signataire connaissent le code d'accès, qui doit être communiqué en dehors du système DocuSign.
- Les organisations destinataires peuvent [établir une liste blanche des domaines et des adresses IP de DocuSign](#).
- Les destinataires peuvent également recourir à la fonction de vérification de l'expéditeur intégrée dans le protocole Sender Policy Framework (SPF) ainsi que le protocole d'identification des courriels DMARC pour réduire le risque d'hameçonnage.

3. Niveaux de signature

- Par défaut, DocuSign utilise sa plateforme pour la signature de tous les documents au format PDF qui sont téléchargés à partir de son système et validés par un certificat numérique X.509 établi par Entrust.
 - Il s'agit dans ce cas d'une **Signature électronique simple**. Le PDF est signé au moyen du système de signature de la plateforme de DocuSign et porte la mention « Signé par DocuSign, inc ». Sa non-répudiation et les informations du signataire sont présentées dans un document récapitulatif distinct inclus dans la piste d'audit, qui indique qui a signé, à quelle date et de quelle manière, sur la base de l'authentification du courriel.

4. Authenticité, intégrité et non-répudiation

- Lorsqu'une signature simple est utilisée, DocuSign signe le PDF sur sa plateforme de manière à assurer son inviolabilité. Toute modification apportée au document sera indiquée dans le panneau de signature du logiciel que vous utilisez pour vos PDF.
- Un [document récapitulatif et piste d'audit](#) supplémentaire, appelé certificat d'achèvement par DocuSign, énumère tous les éléments de l'opération de signature (l'identité du signataire, la date et l'heure de la signature, le type de signature, etc.). Cette information est communiquée à tous ceux qui ont participé au processus. Toute modification apportée apparaît dans le panneau de signature du logiciel que vous utilisez pour vos PDF.