

Vérifier une signature électronique dans un PDF

Un PDF « signé » l'est-il vraiment ? Qui l'a signé, le document a-t-il été modifié, et la signature est-elle simple, avancée ou qualifiée ? Deux méthodes gratuites, pas à pas.

À qui s'adresse cette fiche ?

Aux conseillères et conseillers numériques, aux agents France services, aux secrétariats d'associations et de petites entreprises qui reçoivent des documents signés (contrats, attestations, procès-verbaux, synthèses de formalités) et doivent s'assurer qu'ils sont recevables.

Au sommaire

1. Une signature électronique ne se « voit » pas toujours
2. Méthode 1 — Le panneau Signatures d'Adobe Acrobat Reader
3. Méthode 2 — Le validateur de la Commission européenne
4. Lire le résultat : simple, avancée ou qualifiée ?
5. Les erreurs fréquentes et que faire

1. Une signature électronique ne se « voit » pas toujours

Une **image** de signature collée dans un PDF (scan, dessin au doigt) n'est pas une signature électronique au sens technique : elle ne prouve ni l'identité du signataire ni l'intégrité du document.

Une vraie signature électronique est une donnée **cryptographique** intégrée au fichier. Elle peut être accompagnée d'un visuel sur la page, mais ce n'est pas obligatoire. Elle permet de vérifier trois choses :

- **qui** a signé (le certificat du signataire) ;
- **quand** (date et, idéalement, horodatage) ;
- que le document **n'a pas été modifié** depuis.

Réflexe à transmettre : un PDF signé ne doit plus être « imprimé en PDF », fusionné, compressé ou annoté. Chacune de ces opérations produit un nouveau fichier... sans la signature, ou avec une signature invalidée.

Version du 17 septembre 2026 · Licence Etalab 2.0 : réutilisation et diffusion libres, avec mention de la source.

Fiche rédigée par l'équipe Certyne (certyne.com), éditeur français de signature électronique. Les libellés des logiciels cités peuvent évoluer d'une version à l'autre.

2. Méthode 1 — Adobe Acrobat Reader (gratuit)

La méthode la plus simple pour un usage courant, sur ordinateur.

- 1 Ouvrir le PDF avec **Adobe Acrobat Reader** (et non dans le navigateur, qui n'affiche souvent pas les signatures).
- 2 Regarder le **bandeau en haut du document** : il résume l'état des signatures.
- 3 Cliquer sur « **Panneau Signature** » pour afficher le détail de chaque signature.
- 4 Déplier une signature : vérifier le **nom du signataire**, la **date**, et la mention indiquant que le document n'a pas été modifié depuis la signature.
- 5 Ouvrir « **Détails du certificat** » pour voir qui a délivré le certificat (l'autorité de certification) et sa période de validité.

Comprendre le bandeau

Couleur / message	Ce que cela veut dire	Que faire
Vert / bleu : signé, signatures valides	Le document est intact et le certificat est reconnu par Adobe.	Vérifier que le nom du signataire est bien celui attendu.
Jaune : validité inconnue ou problème	Souvent, Adobe ne connaît pas l'autorité qui a délivré le certificat. Cela ne veut pas dire que la signature est fausse.	Passer à la méthode 2 pour trancher.
Rouge : signature non valide	Le document a été modifié après signature, ou le certificat est révoqué.	Ne pas accepter le document ; demander un nouvel exemplaire signé.

Astuce : dans les préférences d'Adobe (rubrique Signatures, puis Vérification), l'option qui permet de valider à partir de la **liste de confiance européenne** (EUTL) réduit les faux « jaunes » pour les certificats qualifiés européens.

3. Méthode 2 — Le validateur de la Commission européenne

La Commission européenne met à disposition une **application de démonstration** de son outil open source DSS (Digital Signature Service), qui produit un rapport détaillé et indique le niveau eIDAS de la signature.

- 1 Aller sur ec.europa.eu/digital-building-blocks/DSS/webapp-demo/validation.
- 2 Déposer le PDF signé dans le champ « Signed document ».
- 3 Lancer la validation et ouvrir le **rapport simple** (Simple report).

Confidentialité : c'est un service de démonstration et le fichier est envoyé sur un serveur. Ne pas l'utiliser pour des documents confidentiels ou comportant des données sensibles ; préférer alors la méthode 1 ou un outil installé localement.

4. Lire le résultat : simple, avancée ou qualifiée ?

Le rapport du validateur européen donne deux informations essentielles.

L'indication globale

Indication	Signification
TOTAL_PASSED	La signature est techniquement valide : document intact, certificat valable au moment de la signature.
INDETERMINATE	L'outil ne peut pas conclure (certificat non reconnu, information de révocation absente, horodatage manquant...). À examiner, sans conclure à une fraude.
TOTAL_FAILED	La signature est invalide : document modifié, signature cassée ou certificat révoqué.

Le niveau de la signature (qualification)

Mention dans le rapport	Niveau eIDAS	Exemples d'usage
QESig	Signature électronique qualifiée — équivalente à la signature manuscrite dans toute l'Union européenne	Formalités INPI hors FranceConnect+, actes à fort enjeu
AdESig-QC	Signature avancée reposant sur un certificat qualifié	Contrats de la commande publique (arrêté du 22 mars 2019)
AdESig	Signature avancée	Contrats commerciaux, documents RH
Non qualifiée / autre	Signature simple ou cachet d'une plateforme	Devis, bons de commande, accords courants

Si une démarche exige une signature qualifiée (ou avancée avec certificat qualifié), c'est cette ligne qu'il faut regarder : un document « valide » mais de niveau simple sera refusé.

Vérifier le signataire

Le rapport indique le nom figurant dans le certificat. Il doit correspondre à la personne habilitée (dirigeant, mandataire, représentant). Si le certificat porte uniquement le nom de la plateforme utilisée, il s'agit d'un **cachet** de la plateforme et non de la signature personnelle du signataire.

Et pour prouver qu'un document n'a pas changé depuis son dépôt ?

Certains services d'archivage calculent une empreinte (SHA-256) du fichier et permettent de vérifier plus tard qu'un exemplaire est identique à l'original déposé. C'est complémentaire à la vérification de signature : l'empreinte prouve l'identité du fichier, la signature prouve l'engagement du signataire.

5. Les erreurs fréquentes et que faire

- ☐ « **Aucune signature** » dans **Adobe** alors que le document porte un visuel de signature : c'est une image, pas une signature électronique. Demander le fichier original signé à l'expéditeur.
- ☐ **Le fichier reçu a été ré-enregistré** (envoi par une messagerie qui convertit, impression en PDF, fusion) : récupérer l'exemplaire téléchargé directement depuis l'outil de signature.
- ☐ **Validité inconnue (jaune)** : vérifier avec le validateur européen ; si le rapport indique QESig ou AdESig-QC avec TOTAL_PASSED, la signature est recevable techniquement.
- ☐ **Certificat expiré aujourd'hui** : ce n'est pas bloquant si le certificat était valable **au moment de la signature** et que la signature est horodatée.
- ☐ **Plusieurs signatures** : chacune doit être vérifiée séparément ; une signature ajoutée après une autre peut être valide même si le panneau signale des « modifications autorisées » (ajout de signature).
- ☐ **Nom du signataire inattendu** : c'est un point à faire confirmer par l'organisme ou l'entreprise, même si la signature est techniquement valide.

Sources et pour aller plus loin

- Règlement (UE) n° 910/2014 « eIDAS » : eur-lex.europa.eu
- Liste de confiance européenne des prestataires qualifiés : eidas.ec.europa.eu
- Validateur DSS de la Commission européenne (démonstration) : ec.europa.eu
- Adobe Acrobat Reader : get.adobe.com/fr/reader
- Vérifier gratuitement qu'un fichier est identique à un document déposé ou signé sur Certyneo (empreinte calculée dans le navigateur) : certyneo.com/fr/verifier-un-document

Utiliser cette fiche en atelier

Imprimer le tableau de la page 2 pour lire le bandeau Adobe, et celui de la page 3 pour interpréter le rapport européen. Fiche sous licence Etalab 2.0 : adaptable à votre structure en citant la source.