

Vérifier une signature électronique dans un PDF

Un contrat signé en PDF ne vaut que si vous savez le contrôler. Deux outils gratuits suffisent : Adobe Acrobat Reader et le validateur de démonstration DSS de la Commission européenne. Cette fiche, à jour de septembre 2026, explique ce qu'ils vérifient, ce qu'ils ne prouvent pas, et où consulter les listes de confiance.

À qui s'adresse cette fiche ?

Toute personne qui reçoit un devis, un contrat ou une attestation signés en PDF : particuliers, TPE, associations, secrétaires de mairie. Elle sert aussi aux conseillers numériques et aux agents France services qui accompagnent ces démarches.

Au sommaire

1. Ce que contrôle réellement une validation
2. La marche à suivre dans Adobe Acrobat Reader
3. Quand le certificat apparaît « non approuvé »
4. Le validateur de démonstration DSS de la Commission
5. Savoir si le prestataire est qualifié
6. Niveaux PAdES, horodatage et échec de validation

1. Ce que contrôle réellement une validation

- **Quatre questions** : qui a signé, le document a-t-il bougé depuis, le certificat était-il valide au moment de la signature, et une date fiable y est-elle attachée ?
- **Intégrité** : la signature enferme une empreinte du fichier. Si une seule virgule change après coup, l'empreinte ne correspond plus et l'outil signale la modification.
- **Identité** : le nom affiché vient du certificat, pas d'un champ libre. Sa valeur dépend du contrôle d'identité fait par le prestataire émetteur.
- **Image collée** : une signature scannée, un paraphe dessiné à la souris ou une image insérée ne créent aucune signature électronique. Il n'y a rien à valider et le panneau reste vide.
- **Effet juridique** : l'article 25 du règlement (UE) 910/2014 interdit d'écarter une signature au seul motif qu'elle est électronique, et donne à la signature qualifiée l'effet d'une signature manuscrite.

Version du 25 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. Document informatif : Légifrance et service-public.gouv.fr font foi.

2. La marche à suivre dans Adobe Acrobat Reader

- **Panneau** : ouvrez le PDF, puis sélectionnez Signatures dans le panneau de droite. Le volet liste chaque signature du fichier.
- **Valider** : choisissez Options, puis Valider les signatures. La boîte de dialogue État de validation affiche le détail.
- **Certificat** : pour remonter la chaîne de certification, ouvrez Propriétés de la signature, puis Afficher le certificat du signataire. Vous y voyez l'autorité émettrice et les dates de validité.
- **Horodatage** : Acrobat précise si l'heure vient de l'horloge du signataire ou d'un serveur de tampons temporels. La première n'engage personne, la seconde est vérifiable.
- **Tout valider** : si le document porte plusieurs signatures, passez par Tous les outils, puis Utiliser un certificat, puis Valider toutes les signatures.

3. Quand le certificat apparaît « non approuvé »

- **Inconnu** : un certificat valide s'affiche comme non approuvé tant que son autorité n'est pas dans le magasin de confiance local d'Acrobat. Ce n'est pas l'indice d'une fraude.
- **AATL** : Adobe gère l'Adobe Approved Trust List, un programme qui fait approuver automatiquement, à l'ouverture du document, les signatures issues des autorités membres.
- **Liste UE** : Acrobat embarque aussi un instantané de la liste de confiance européenne, rafraîchi environ une fois par mois, avec jusqu'à trente jours de décalage sur la publication d'un État membre.
- **Indéterminé** : si la chaîne ne remonte à aucune ancre connue localement, Acrobat le signale sans conclure. Vérifiez alors le prestataire dans le navigateur des listes de confiance.

4. Le validateur de démonstration DSS de la Commission

- **Adresse** : l'application publique est hébergée sur ec.europa.eu, rubrique digital-building-blocks. Vous y déposez le PDF signé, sans compte ni installation.
- **Résultats** : l'outil rend l'une des trois indications de la norme ETSI EN 319 102-1. TOTAL_PASSED : la signature passe la vérification. INDETERMINATE : rien n'a échoué, mais les informations manquent. TOTAL_FAILED : le format ou la valeur de signature est incorrect.
- **Démonstration** : la Commission précise que cette application démontre des fonctions de la bibliothèque DSS et que son usage doit rester limité aux tests. Le résultat n'a aucune valeur officielle.
- **Confidentialité** : votre fichier est transmis à l'infrastructure de la Commission, qui recommande de n'envoyer aucun document sensible. Les fichiers ne sont pas conservés.
- **Rapport** : le rapport détaillé ajoute une sous-indication, par exemple certificat révoqué ou expiré. Elle explique pourquoi la validation n'aboutit pas.

5. Savoir si le prestataire est qualifié

- **Listes de confiance** : l'article 22 du règlement eIDAS oblige chaque État membre à publier la liste de ses prestataires de services de confiance qualifiés. La Commission les agrège.

- **Navigateur européen** : le Trusted List Browser, sur le tableau de bord eIDAS, permet de chercher un prestataire par nom, par pays et par type de service.
- **France** : l'ANSSI établit, tient à jour et publie la liste nationale de confiance, en PDF et en XML, avec une empreinte SHA-256 pour contrôler le fichier.
- **Bon réflexe** : un prestataire absent de ces listes peut rendre un service utile, mais sa signature n'est pas qualifiée. La présomption d'équivalence avec la signature manuscrite ne joue pas.

6. Niveaux PAdES, horodatage et échec de validation

- **Quatre niveaux** : la norme ETSI EN 319 142-1 définit quatre niveaux de signature PDF, nommés PAdES B-B, B-T, B-LT et B-LTA.
- **B-B et B-T** : le niveau B-B ne contient que le minimum. Le niveau B-T ajoute un jeton d'horodatage, qui prouve que le document existait déjà à un instant donné.
- **B-LT et B-LTA** : B-LT embarque dans le fichier les certificats et les données de révocation utiles à la vérification. B-LTA y ajoute des horodatages d'archivage.
- **Horodatage** : l'article 41 du règlement eIDAS donne à l'horodatage qualifié une présomption d'exactitude de la date et d'intégrité des données. Sans lui, la validation se complique une fois le certificat expiré.
- **Échec** : ne retouchez pas le fichier. Redemandez l'original au signataire, vérifiez que vous n'ouvrez pas une copie ré-enregistrée par un autre logiciel, puis faites refaire la signature.

Liste de contrôle

- ☐ J'ai ouvert le panneau Signatures et lancé la validation dans Acrobat Reader.
- ☐ J'ai ouvert les propriétés de la signature et consulté le certificat du signataire.
- ☐ J'ai vérifié que le document n'a pas été modifié depuis la signature.
- ☐ J'ai regardé si la signature porte un horodatage ou seulement l'heure du poste du signataire.
- ☐ J'ai cherché le prestataire dans la liste de confiance européenne ou celle de l'ANSSI.
- ☐ Je n'ai envoyé aucun document sensible au validateur de démonstration de la Commission.

Sources et pour aller plus loin

- Commission européenne, DSS Demonstration WebApp : valider une signature : ec.europa.eu/digital-building-blocks/DSS/webapp-demo/validation
- Commission européenne, documentation DSS : indications TOTAL_PASSED, INDETERMINATE, TOTAL_FAILED : ec.europa.eu/digital-building-blocks/DSS/webapp-demo/doc/dss-documentation.html
- Commission européenne, EU Trusted List Browser (tableau de bord eIDAS) : eidas.ec.europa.eu/efda/tl-browser
- ANSSI, la liste nationale de confiance : cyber.gouv.fr/reglementation/reglementation-identite-confiance-numerique/securite-echanges-voie-electronique/reglement-eidas/la-liste-nationale-de-confiance
- EUR-Lex, règlement (UE) 910/2014 eIDAS consolidé au 18/10/2024, articles 22, 25, 32 et 41 : eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:02014R0910-20241018

- ETSI EN 319 142-1 V1.1.1, signatures PAdES baseline B-B, B-T, B-LT, B-LTA :
etsi.org/deliver/etsi_en/319100_319199/31914201/01.01.01_60/en_31914201v010101p.pdf
- Adobe, validation de toutes les signatures numériques dans Acrobat :
helpx.adobe.com/fr/acrobat/using/validating-digital-signatures.html
- Autres fiches pratiques : certyneo.com/fr/ressources/fiches-pratiques-gratuites

Fiche pratique « Vérifier une signature électronique dans un PDF » — version du 25/09/2026 — rédigée par l'équipe Certyneo (certyneo.com). Licence Etalab 2.0. Document informatif. Signaler une erreur : contact@certyneo.com.