EXEMPLE · DÉMONSTRATION — certificat réel présenté à titre d'illustration

Certificat d'horodatage

Établi le 10 octobre 2026 à 21:56 UTC+2 à partir de la preuve VerifBox et de ses ancrages Bitcoin.

Élément de preuve d'horodatage électronique — horodatage non qualifié — ne prouve ni l'auteur ni la propriété.

> Le fichier « document-exemple.txt » (40 octets), dont l'empreinte SHA-256 figure ci-dessous, existait au plus tard le 10 octobre 2026 à 20:53:10 UTC+2, selon la preuve signée par VerifBox. Cette empreinte est en outre inscrite dans la blockchain Bitcoin, dans le bloc n° 970 811 du 10 octobre 2026.

Fichier

Nom	document-exemple.txt
Taille	40 octets
Empreinte SHA-256	`0d94170ac58605a91251bb6b2b6bf5f9243995ecd23ed2c83af20b64ffa95529`

Horodatage signé par VerifBox

Date et heure	10 octobre 2026 à 20:53:10 UTC+2
Temps universel	2026-10-10 18:53:10.995 UTC
Identifiant de preuve	`54b07a24cc8d404da5a127dfa2d818f6`
Clé de signature	258e57366bcdb6ce (publiée sur verifbox.com)
Signature Ed25519	`z0kdqMNBMULXwuL7yYZx7zc4X5rICPvHxf5cp8Uxe9mi2o4pjq6nHGOX72rPRF3dfQCl_SwwDv-pH8PE9QfcCA`
Signature ML-DSA-65	Post-quantique (FIPS 204), 3 309 octets ; empreinte SHA-256 : `10ce809519f520f7727635f86db467e3d11d00922f80500ef480d1115e63ea79`

Double ancrage dans la blockchain Bitcoin

Ancrage du fichier	bloc n° 970 811, du 10 octobre 2026 à 21:00:07 UTC+2
Transaction	`ea43d20ad4f936319bb48ca241975853a80705b3a47b0c5c7abc897b3deec525`
Explorateurs	blockchain.com · mempool.space · blockstream.info
Ancrage de l'attestation	bloc n° 970 811, du 10 octobre 2026 à 21:00:07 UTC+2
Transaction	`ea43d20ad4f936319bb48ca241975853a80705b3a47b0c5c7abc897b3deec525`
Explorateurs	blockchain.com · mempool.space · blockstream.info
Empreinte de l'attestation	`bd19eb760bb02c361faf3a6ecd8ca496c811beb83f7f6fde47caf16e08a7cddf`
Contrôle	Ancrages vérifiés contre l'en-tête des blocs le 10 octobre 2026 à 21:56 UTC+2, auprès de blockstream.info

Jeton d'horodatage RFC 3161

Autorité	IIC TSA, exploitée par l'éditeur de VerifBox (pas un tiers indépendant)
Heure du jeton	10 octobre 2026 à 18:53:11 UTC, précision ± 1 s
Politique, n° de série	`1.3.6.1.4.1.67100.1.1.1.1` · `47d70c22c4f47cf4e0766104d85b056e`

EXEMPLE DÉMONSTRATION

Ce certificat est une présentation lisible de la preuve ; il n'est pas lui-même signé. Seuls le fichier de preuve (.verifbox.json) et le fichier d'origine font foi. Horodatage électronique simple, non qualifié au sens du règlement (UE) n° 910/2014 (eIDAS) ; il ne crée aucune présomption légale et sa valeur probante est appréciée par le juge. Éditeur : HTTPS CARD — Internet Identity Card Limited, 124 City Road, London EC1V 2NX, Royaume-Uni, société n° 09168431.

Comment vérifier ce certificat

1. Sur verifbox.com/fr/verifier, avec la preuve (.verifbox.json) et le fichier d'origine.
2. Hors ligne, sans VerifBox : la page verifbox-verify-offline.html et le script Python verifbox_verify.py, publiés sur github.com/httpscard/verifbox-cles.
3. Ancrages Bitcoin seuls : avec l'outil libre OpenTimestamps, commande « ots verify » sur les fichiers .ots.
4. Clés publiques de VerifBox : verifbox.com/.well-known/verifbox-cles.json, publiées aussi sur GitHub et dans l'enregistrement DNS _verifbox.internetidentitycard.com.
5. Jeton RFC 3161 : « openssl ts -verify », avec la racine IIC TSA publiée sur verifbox.com/.well-known/iic-tsa.json.

EXEMPLE
DÉMONSTRATION

Ce certificat est une présentation lisible de la preuve ; il n'est pas lui-même signé. Seuls le fichier de preuve (.verifbox.json) et le fichier d'origine font foi. Horodatage électronique simple, non qualifié au sens du règlement (UE) n° 910/2014 (eIDAS) ; il ne crée aucune présomption légale et sa valeur probante est appréciée par le juge. Éditeur : HTTPS CARD — Internet Identity Card Limited, 124 City Road, London EC1V 2NX, Royaume-Uni, société n° 09168431.