

PROOFSNAP FILE CERTIFICATE

Proof of Prior Existence — Provenance Certificate

Evidence ID: FC-5a28c97d-f72e-42df-a9be-85e1b465a448
File: sample_contract.pdf
Size: 235,826 bytes (230.3 KB)
Type: application/pdf

SHA-256:

f59820cde0548e6bff832e3067001a903edf3f1b9069c95d74ef414aad2122a0

Certified: Sun, 31 May 2026 12:38:28 GMT

INTEGRITY CHECKS

[PASS] **SHA-256 Hash**
Computed locally — file never uploaded

[PASS] **RSA-4096 Signature**
Manifest signed — tamper-proof

[PASS] **Blockchain (Bitcoin)**
OpenTimestamps pending confirmation

[PASS] **EU Qualified (eIDAS)**
Disig a.s. qualified

[PASS] **Custodian**
enterprise@xx.com

[PASS] **Environment**
Asia/Dubai

The original file never leaves your device. Only its SHA-256 hash is sent to timestamp servers.
The RSA-4096 signature locks the manifest — any tampering invalidates the package.

Bitcoin: Verify with 'ots verify manifest.json.ots' or upload ZIP to <https://getproofsnap.com/verify/index.html>

eIDAS: Qualified timestamp by Disig a.s. — Art. 42 EU Reg. 910/2014

Verify: <https://getproofsnap.com/verify/index.html>

HOW TO VERIFY THIS CERTIFICATE

1. Go to <https://getproofsnap.com/verify/index.html>
2. Upload this ZIP file — all cryptographic checks run automatically
3. Upload the original file to verify it matches the SHA-256 hash above
4. All checks should show PASS

Bitcoin blockchain: Run 'ots verify manifest.json.ots' for independent verification
or use <https://opentimestamps.org> for browser-based verification

WHAT'S IN THIS PACKAGE

- manifest.json** — SHA-256 hashes of all files + evidence ID
 - manifest.sig** — RSA-4096 digital signature (tamper-proof)
 - publickey.pem** — Public key for signature verification
 - chain_of_custody.json** — Who, when, where, file metadata, integrity info
 - forensic_log.json** — ISO/IEC 27037 certification steps with hash chain
 - manifest.json.ots** — Bitcoin blockchain timestamp (OpenTimestamps)
 - manifest.json.tsr** — EU qualified timestamp (RFC 3161, eIDAS)
 - eidas_validation.json** — Long-term validation data (cert chain, OCSP)
-

LEGAL NOTICE

This certificate package provides cryptographic proof that the referenced file existed at the certified date and time.

- SHA-256 hash: tamper-evident — any change invalidates the hash
- RSA-4096 signature: authenticates the manifest against modification
- Bitcoin timestamp: decentralized, immutable proof of time
- eIDAS timestamp: legally presumed accurate in all 27 EU member states (Article 41, Regulation (EU) No 910/2014)

The original file never leaves your device.
Only its 32-byte SHA-256 hash is sent to timestamp servers.
