



docuProof.io

# System Description & Public Commitment

*Version 1.0 — February 28, 2026*

*This document describes what docuProof is, what it does, what it does not do, and the commitments we make to every user. It is designed to be timestamped using docuProof itself — creating a permanent, independently verifiable record of these representations at the time they were made.*

## 1. WHAT DOCUPROOF IS

docuProof is a cryptographic timestamping service. It creates permanent, tamper-proof evidence that a specific digital file existed at or before a specific point in time.

When you use docuProof, you receive a proof certificate that can be independently verified by anyone, anywhere, at any time — without requiring trust in docuProof or any third party.

### How It Works

**Step 1: Local Hashing** — When you select a file, your browser computes a SHA-256 cryptographic hash entirely on your device. The file itself never leaves your computer. We never see your file — only its unique hash.

**Step 2: Blockchain Anchoring** — Your file's hash is submitted to the OpenTimestamps protocol, which batches multiple hashes together and anchors them to the Bitcoin blockchain. This creates an immutable record that cannot be altered or backdated.

**Step 3: Certificate Delivery** — You receive a PDF Certificate of Proof containing your proof details, including a QR code for instant verification. Your certificate is delivered by email once your proof is permanently anchored to a Bitcoin block — typically within 1–3 hours.

The entire process is designed so that verification requires zero trust in docuProof. Anyone with your original file and proof receipt can independently confirm the timestamp — even if docuProof ceases to exist.

## 2. WHAT DOCUPROOF IS NOT

Clarity about boundaries is essential to trust. Here is what docuProof does not do:

### Not a storage service.

docuProof does not store, host, or have custody of your files. We never see the contents of what you timestamp. You are responsible for preserving your original file.

### Not a notary or legal certification.

A docuProof timestamp does not constitute legal certification, notarization, or attestation of the file's contents, authorship, ownership, or validity. It proves only that the file existed at or before a certain time.

### Not a guarantee of authenticity.

Timestamping proves existence, not truth. A false document can be timestamped just as easily as a true one. docuProof makes no claims about the accuracy, authenticity, or legal standing of timestamped content.

## 3. OUR COMMITMENTS

These are the promises we make to every docuProof user:

Commitment	What It Means
Privacy First	Your files never leave your device. We process only cryptographic hashes — never file contents.
No Vendor Lock-in	Proofs can be verified independently using open-source tools, without relying on docuProof.
Transparent Operation	We use the public OpenTimestamps protocol anchored to the Bitcoin blockchain.
Conservative Claims	We will never overstate what a timestamp proves. Existence is not authenticity.
Version Discipline	Material changes to these guarantees will be clearly documented and timestamped.

## 4. INDEPENDENT VERIFICATION

The value of a docuProof timestamp lies in its independence. Here is how anyone can verify a proof without relying on docuProof:

1. Compute the SHA-256 hash of the original file using any standard cryptographic tool.
2. Use the OpenTimestamps verification tools (open source, freely available) to check the timestamp receipt against the Bitcoin blockchain.
3. Confirm that the hash in the receipt matches the hash of your file.

If all three steps succeed, you have cryptographic proof of the timestamp's validity — no trust in any third party required.

## 5. REDUNDANT IDENTITY PRESERVATION (RIP)

docuProof offers an optional Redundant Identity Preservation (RIP) add-on. RIP allows users to cryptographically verify that three independent copies of their original file are bit-identical to the blockchain-anchored hash. This provides an additional layer of evidentiary integrity by ensuring that proof survives even if one copy is lost, corrupted, or destroyed.

RIP verification is documented on an enhanced Certificate of Proof, which includes the RIP Verified badge and details about the redundancy verification performed.

## 6. VERSIONING & FUTURE EVOLUTION

docuProof maintains versioned system descriptions to ensure clarity about guarantees over time. This document represents Version 1.0.

### Changes that require a new major version:

- Change to cryptographic primitives (hash algorithms, anchoring protocol)
- Change to the meaning or scope of what a proof claims
- Introduction of file custody or storage
- Any change affecting verification independence

### Changes that do not require a new version:

- User interface improvements or performance optimizations
- New optional features that do not alter core guarantees
- Pricing or packaging changes

## 7. WHY THIS MATTERS

In a world where digital files can be easily created, modified, or backdated, proving when something existed has become increasingly valuable:

Use Case	Why Timing Matters
Intellectual Property	Establish priority for inventions, designs, or creative works.
Legal Evidence	Prove documents existed before a dispute arose.
Regulatory Compliance	Demonstrate policies were in place at required times.
Business Records	Create tamper-proof audit trails for contracts and agreements.
Personal Documentation	Protect important moments with verifiable timestamps.

## 8. ABOUT THIS DOCUMENT

This System Description is itself timestamped using docuProof. The timestamp creates a permanent record that these commitments and representations existed at the date shown.

By timestamping our own documentation, we demonstrate our commitment to transparency and create an independently verifiable record of what we promised, and when.