

DocChain

Security Whitepaper

How DocChain protects your data · Rip It Labs, LLC · docchain.ripitlabs.com

Classification: **PUBLIC** · Version 1.1 · Effective 2026-09-03 · Owner: Tim Cavin (CEO / Security Lead) · Review: annual

1. Overview

DocChain is a document-notarization and proof-of-existence service operated by Rip It Labs, LLC. It lets a user prove a file existed, unaltered, at a point in time by recording the file's cryptographic fingerprint on public blockchains and issuing a signed, timestamped certificate. This paper describes the security and privacy architecture.

2. Privacy by design — the file never leaves your device

The defining property of DocChain: documents are hashed **in the user's browser** using the Web Crypto API (SHA-256). Only the resulting 64-character fingerprint and the metadata a user chooses to enter are transmitted. The document's contents are never uploaded, transmitted, processed, or stored by DocChain. This makes the service safe for privileged, trade-secret, and unfiled-IP material and aligns with the GDPR principle of data minimization.

3. Data we do and do not hold

We store	We never receive
SHA-256 fingerprint; user-supplied filename, document type, issuer, note; optional email; the Ed25519 attestation; blockchain transaction IDs; the RFC 3161 token; request IP (for abuse prevention); timestamps.	The document itself, its contents, or any derivative that could reconstruct it.

4. Cryptography

• **Hashing:** SHA-256 (NIST FIPS 180-4). • **Attestation signature:** Ed25519 (NIST FIPS 186-5). • **Trusted timestamp:** RFC 3161 token from the DocChain Time-Stamping Authority. • **Document certificate:** PAdES / ETSI EN 319 142 signed PDF with an embedded RFC 3161 timestamp. • **Anchoring:** the fingerprint is written to public blockchains (XDC, Base, Hedera, XRP, Stellar).

5. Key management

Signing keys (the Ed25519 attestation key and the TSA/PKI private keys) are stored on the production host outside the application directory, with owner-only file permissions, and are excluded from source control and backups of the application. Keys are never transmitted to clients. Hardware Security Module (HSM) custody is on the roadmap as part of eIDAS-qualified readiness.

6. Hosting & network security

DocChain runs on hardened Linux servers (Hetzner) behind Cloudflare. All public traffic is served over TLS 1.2+; the origin is reached only through an authenticated Cloudflare Tunnel (no public inbound ports on the origin). HTTP security headers (HSTS-equivalent via the edge, X-Content-Type-Options, Referrer-Policy, a strict Content-Security-Policy, and X-Frame-Options: DENY) are enforced. Administrative access is key-based SSH only.

7. Application security

Input is validated (e.g., fingerprints must be well-formed 64-hex SHA-256). Anonymous usage is rate-limited to protect availability and cost. The service is stateless per request apart from its datastore; no document content is present to leak. Dependencies are pinned and reviewed.

8. Availability & integrity of proofs

Even in the event of total DocChain outage, issued proofs remain independently verifiable: the blockchain anchors are permanent public records, the RFC 3161 token verifies against our published CA with standard tools, and the PAdES certificate self-validates in any PDF reader. Customers are never locked to our uptime.

9. Sub-processors

Provider	Purpose	Data exposed
Hetzner	Compute / hosting	Stored metadata + fingerprints (no documents)
Cloudflare	Edge TLS, DNS, DDoS/proxy	Request metadata in transit
Public blockchains	Immutable anchoring	Fingerprint (hash) only

10. Compliance & standards

DocChain is built on SHA-256 (FIPS 180-4), Ed25519 (FIPS 186-5), RFC 3161, and PAdES (ETSI EN 319 142); its certificate is structured for self-authentication under U.S. Fed. R. Evid. 902(13)/(14) and aligns with the ESIGN Act and UETA. SOC 2 and ISO/IEC 27001 are in preparation; eIDAS Qualified Trust Service Provider status is on the roadmap. We state only what is true today.

Security contact: ripitlabs@gmail.com · © 2026 Rip It Labs, LLC. This document is provided for informational purposes and does not create warranties or contractual obligations.