

CERTSIGNER

certsigner.com



Project Description

Operation, architecture, products and legal aspects

Authors: Fabricia Carpenter Soraire and Luna Carpenter Pires

Document CS-DOC-02 · Version 1.0 · 2026-09-23

CONFIDENTIAL — restricted to authorized recipients

1. Overview

CertSigner is a digital certification service for proof of existence (*timestamping*) and priority of ideas, created by Fabricia Carpenter Soraire and Luna Carpenter Pires. The platform receives content — a document, work, project, code or idea description — computes its cryptographic fingerprint and records that fingerprint, with UTC date and time, in several independent public repositories. The result is public, immutable evidence that any third party can verify.

Core principle: the Certifier **does not need to publish the original content**. It publishes verifiable evidence that references that content. A confidential 50 MB PDF, for example, never leaves the client's control — only its hash and metadata are made public.

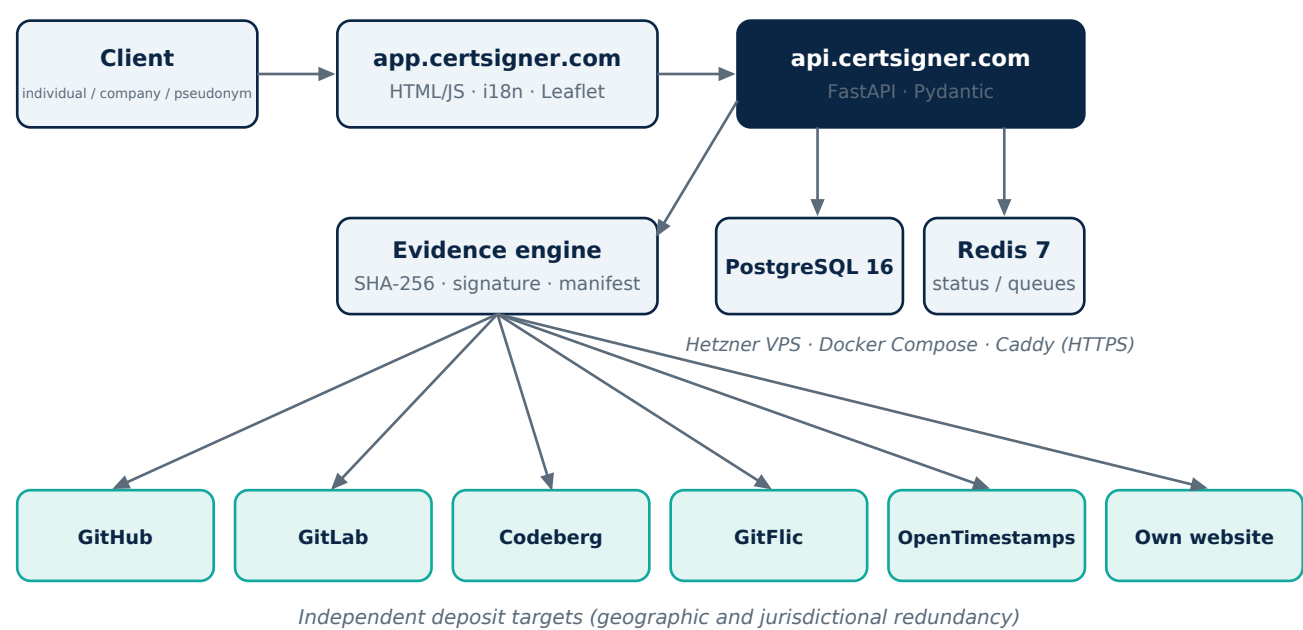
2. How it works

Step	Description
1. Sign-up	Individual or company client (or pseudonym) creates an account and chooses visibility options.
2. Upload	Upload of file or text; content type (idea, document, work) and fixed or dynamic mode.
3. Hash	SHA-256 computation (optionally SHA3-512 and BLAKE3), size, MIME type, UTC date.
4. Manifest	Generation of README.md, metadata.json, sha256.txt and the Certifier's signature.
5. Timestamp	OpenTimestamps record (anchored in Bitcoin) and, where applicable, RFC 3161.
6. Multi-source deposit	Publication of the evidence on GitHub, GitLab, Codeberg, GitFlic, OpenTimestamps and our own website.
7. Receipt	Certificate with protocol number, hashes and links to each deposit; dashboard shows "deposit confirmed" per target.
8. Verification	Any third party recomputes the file's hash and checks the public records.

Published evidence package

File / field	Purpose
SHA-256 (+ optional SHA3-512, BLAKE3)	Content fingerprint
Size, name (optional), MIME type	Technical identification of the file
UTC date	Time of registration
timestamp.tsr (RFC 3161)	Authority timestamp
document.ots	OpenTimestamps proof anchored in Bitcoin
signature.sig	Certifier's digital signature
README.md · metadata.json · sha256.txt	Human- and machine-readable manifest

3. Technical architecture



Layer	Technology
Frontend	Static HTML/JS, Leaflet maps, i18n (PT/EN/ES/ZH/CS) with preference saved in the browser
Backend	Python · FastAPI · Pydantic · async SQLAlchemy 2.x (asyncpg)
Data	PostgreSQL 16 (production) with automatic SQLite detection in development
Real-time state	Redis 7 — live status endpoint; job queues (Celery/RQ) planned
Infrastructure	Hetzner VPS (Ubuntu 24.04), Docker Compose, Caddy with automatic HTTPS
Documents	PDF generation with ReportLab
Payments	PaymentService abstraction: Mercado Pago (BRL) and Stripe (USD/EUR), routed by currency/country
Payment security	Webhooks validated by provider signature; card data never reaches the backend (tokens only)

Implemented modules

- **Activation map** (“Global Activation Pattern”): geographic view of deposit targets and status per target.
- **Admin configuration**: display modes (city+country, country+continent, country+hash, names only).
- **Price synchronization**: spreadsheet export/import, versioning and conflict resolution, with a pytest test suite.
- **Internal and external accounting**: Brazilian tax regime selector (Carnê-Leão, MEI, Simples Nacional, Lucro Presumido, Real and Arbitrado).
- **Legal pages**: Terms of Use, Privacy (LGPD/GDPR) and Refunds.

4. Why multiple repositories

A proof deposited with a single provider depends on that provider's continuity and policies. CertSigner distributes the same evidence across platforms in different jurisdictions, so that removal, blocking or failure of one does not invalidate the proof.

Target	Jurisdiction	Role
GitHub	USA	Public, dated Git history; good indexing
GitLab.com	Europe	Independent Western redundancy
Codeberg	Germany	Non-profit, community platform
GitFlic	Russia	Evidence outside the Western ecosystem; lower risk of removal due to sanctions
OpenTimestamps	Bitcoin blockchain	Immutable, decentralized cryptographic anchor
Own website	certsigner.com	Centralized registration, search and verification by the Certifier

Expansions under evaluation: Zenodo (DOI and academic indexing), Internet Archive (search and OCR), OSF and Gitee.

5. Products and options

Dimension	Options
Registration type	Fixed (single record) · Dynamic (progressive entries in a continuous stream)
Certificate authorship	Named · Bearer · Encrypted · Hidden · Pseudonym (individual or company)
Visibility	Public · Private · Anonymous public content (for oneself / for others)
Progressive confidentiality	Starts encrypted and becomes named after a period (e.g. 1 year) · starts under a pseudonym and becomes named (e.g. 6 months) · disclosure at a fixed or open time
Project status	Active · Hidden · Paused · Archived
Services for ideas	Registration · Protection · Promotion · Sale · Purchase
Third-party advertising	Linking a URL, website or brand to the record

6. Legal aspects and limitations

- The certificate proves the **existence and integrity** of content on a given date. It does not declare originality, does not compare ideas and does not replace registration with INPI or patent offices.
- The user declares responsibility for the authorship (or for submission without authorship) of the uploaded content.
- The privacy policy explicitly addresses the tension between the right to erasure (LGPD/GDPR) and the immutability of hashes already deposited in distributed sources.
- The contract provides for notice of changes and preservation of records after any termination of the service (term being defined; 5-year reference).
- Tax tables and legal documents are at draft stage and require review by a lawyer and an accountant before production use.

7. Validation

Validation of the registration and search model is planned with librarians and information professionals, along with market research to calibrate plans (free, per document and monthly).