SITESEALED

Every record sealed the moment it's made.

FOUNDING WHITEPAPER

Version 1.0 — Genesis Edition

A neutral proof layer for the construction industry

sitesealed.com | August 2026

This document fixes the founding principles of the project (Part I, immutable) and its initial technical specification (Parts II–V, versioned).

Table of Contents

Abstract

Construction is the world's most dispute-intensive industry. When conflicts arise — over delays, defects, variations, or damage — the outcome is decided less by what actually happened on site than by **what can be proven, by whom, and at what cost**. Today, the evidentiary record of a construction project is fragmented across phones, inboxes, proprietary platforms and paper minutes. Each party holds its own version; every document can be contested as backdated, altered, or selectively produced.

SiteSealed proposes a simple inversion: instead of reconstructing evidence after a dispute, the industry should **generate self-proving records at the moment of capture**. Every site photograph, inspection note, delivery slip or handover report is hashed on the device, receives a qualified electronic timestamp under the EU eIDAS framework, and is aggregated into a Merkle tree whose root is anchored on a public blockchain. The result is a record whose existence, timing and integrity can be verified by any party — including an opposing one — without trusting SiteSealed itself.

This paper states the problem, derives the design from first principles, specifies the sealing pipeline and trust model, analyses the legal foundations of admissibility, and defines the economic model. Part I constitutes the immutable founding principles of the project. Subsequent parts are the Genesis specification, versioned and improvable, in the same way Bitcoin's implementation evolved while its whitepaper's principles did not.

1. The Problem: Evidence Is the Bottleneck of Construction Justice

1.1 Observations

The design of SiteSealed rests on five observations, each drawn from professional practice in permitting, public procurement and post-disaster reconstruction, and corroborated by the dispute-resolution literature:

- **O1 — Fragmentation.** Project records are scattered across personal phones, email threads, messaging apps, contractor platforms and paper site diaries. No single, complete, ordered record of the project exists anywhere.
- **O2 — Asymmetry.** The party with the best archive wins arguments regardless of the merits. Small contractors, subcontractors and private owners are structurally disadvantaged against organisations with document-management departments.
- **O3 — Contestability.** Ordinary digital files prove almost nothing by themselves. A photo's EXIF date can be edited in seconds; a PDF can be regenerated; an email chain can be selectively disclosed. In adversarial proceedings, every uncertified record invites a challenge to its authenticity.
- **O4 — Cost inversion.** The cost of producing a record at the moment of the event is near zero; the cost of reconstructing the same fact years later — through discovery, expert forensics and witness testimony — is enormous. Disputes are expensive precisely because evidence is produced at the wrong end of the

timeline.

- **O5 — Timing is the battlefield.** Construction disputes rarely turn on whether something happened, but on *when*: when a defect appeared, when notice was given, when a design was issued, when site conditions changed. Time is the single most contested — and most falsifiable — attribute of a record.

1.2 Why existing tools do not solve this

Two categories of tools exist today, and a structural gap lies between them. **Project-documentation platforms** (photo apps, daily-log tools, common data environments) organise records efficiently but store them on servers controlled by one party or vendor; their timestamps are database entries, alterable by administrators and unverifiable by an opponent. **Forensic certification services** produce legally strong evidence but are generic, priced per act, unknown on job sites, and disconnected from construction workflows. Neither offers what a dispute actually requires: **construction-native capture with proof-grade sealing, verifiable by the adverse party**. That intersection is the product.

2. The Reasoned Argument

The solution follows from the observations by a short chain of propositions:

- **P1.** From O3 and O5: a record is only decisive if its *integrity* (unaltered content) and its *time of existence* are independently verifiable.
- **P2.** From O2: verification must not depend on trusting the party that produced the record — nor the vendor that stored it. A proof held by one side is merely a claim; a proof checkable by the other side is evidence.
- **P3.** From P2: the trust anchor must sit *outside* all parties. Two such anchors exist at industrial maturity today: qualified trust service providers operating under statutory supervision (eIDAS), and public blockchains whose consensus no single actor controls.
- **P4.** The two anchors have complementary strengths and weaknesses. Qualified timestamps carry a statutory presumption of integrity before EU courts but rely on a supervised provider and a specific legal order. Public-chain anchors are jurisdiction-neutral and verifiable by anyone forever, but courts treat them as ordinary evidence to be weighed, not presumed. **Therefore every record must carry both.** This dual-rail principle is the technical heart of SiteSealed.
- **P5.** From O4: sealing must be automatic and invisible, embedded in the natural gesture of taking a site photo or filing a report. Any workflow that adds friction at capture time will not be used, and an unused proof system proves nothing.
- **P6.** From O1: sealing individual files is insufficient; the product must produce a *continuous, ordered project record* — a chain of sealed entries — so that absence of a record also becomes meaningful (what was never sealed was arguably never notified).
- **P7.** A hash proves existence, not authorship or truthfulness. The system must therefore control the capture context (in-app camera, attested device, satellite positioning, network time) to bind the record to a

place, a device and an account — while stating honestly, in every report, what is proven and what is merely attested.

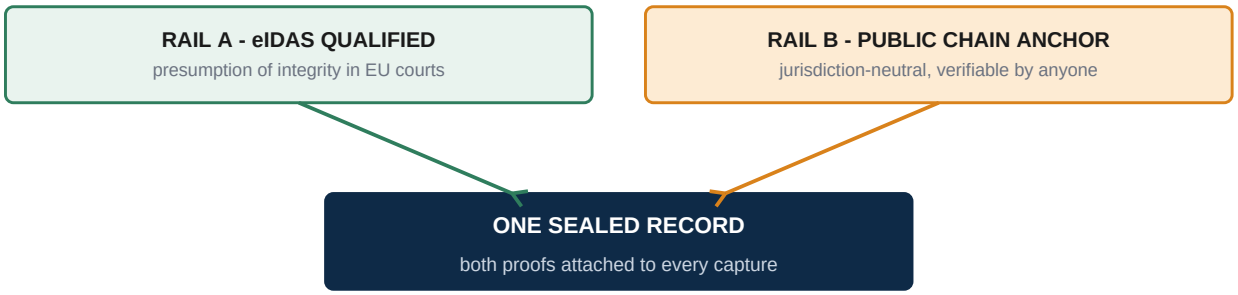

Figure A — The dual-rail principle (P4): every sealed record carries a qualified eIDAS timestamp and a public-chain anchor. Legend: green = statutory presumption rail; amber = neutral verification rail; navy = the sealed record itself.

Part I — Founding Principles (Immutable)

The following seven principles are fixed for the lifetime of the project. Any future specification, feature or commercial decision that contradicts them is, by definition, not SiteSealed.

Principle 1 — Proof over storage.

SiteSealed sells verifiable proof, never mere storage. If the company disappears, every proof already issued must remain independently verifiable.

Principle 2 — Verifiable by the adversary.

Every proof must be checkable by the opposing party using public information and open tooling, without SiteSealed's cooperation.

Principle 3 — Dual rail, always.

Every sealed record carries both a qualified timestamp (statutory rail) and a public-chain anchor (neutral rail). Neither alone is sufficient.

Principle 4 — Capture is sacred.

Sealing happens at the moment of capture, on the device, before any human has an incentive to alter the record. Importing pre-existing files is a separate, explicitly-labelled class of record, never silently mixed with live captures.

Principle 5 — Honest scope.

Every Evidence Report states in plain language what is cryptographically proven (existence, integrity, time), what is attested (device, location, account), and what is not claimed (truthfulness of content, authorship beyond the account). The product never overstates its legal effect.

Principle 6 — Privacy by architecture.

Original files remain encrypted under client-held keys; only hashes leave the client's control. SiteSealed must remain unable to read the records it seals.

Principle 7 — Fees on value, not on volume of trust.

Verification is free, forever, for everyone. Revenue comes from sealing capacity and report generation, never from reading or verifying proofs.

Part II — System Design (Genesis Specification)

3. Architecture Overview

The system is deliberately minimal: a capture client, a stateless sealing service, two external trust anchors, and a public verification portal. Everything that touches trust is either on the client, on a supervised third party, or on a public chain — never solely in SiteSealed's database.

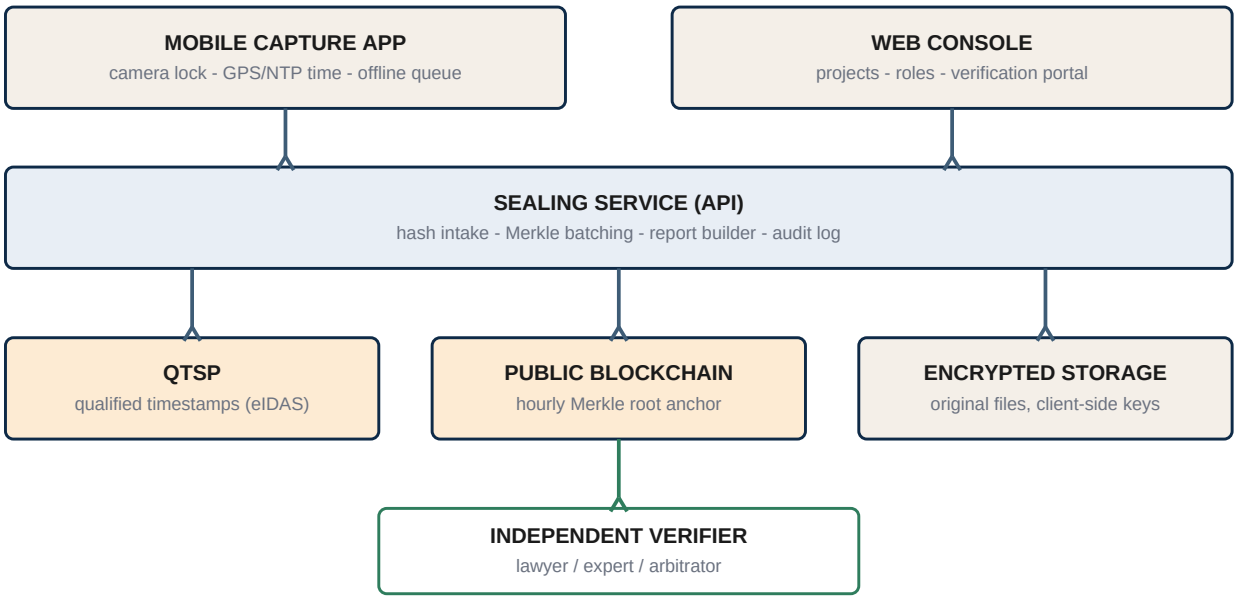

Figure 2 — System architecture. Legend: sand = SiteSealed components; light amber = external trust anchors; white/green = independent verifiers, who need no account and no permission. Arrows indicate the primary data flow (hashes and proofs; original files flow only to encrypted storage).

4. The Sealing Pipeline

Each record follows five steps from lens to ledger:

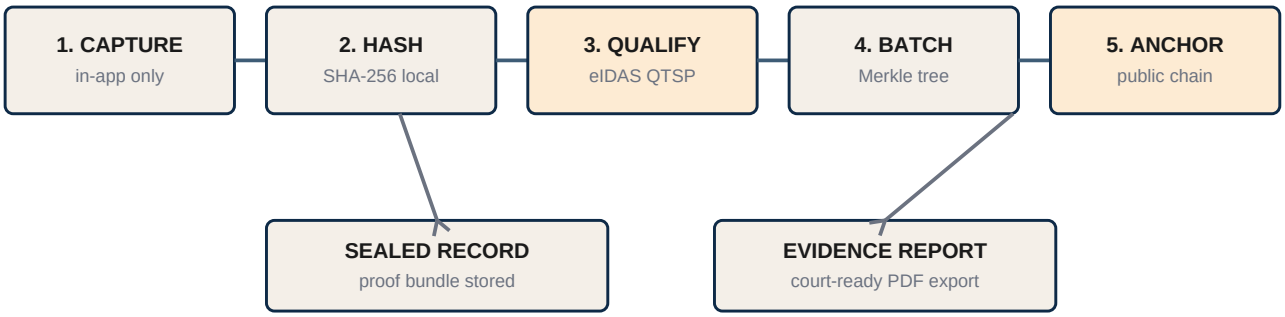

Figure 1 — The five-step sealing pipeline. Amber steps involve external trust anchors.

- **Step 1 — Capture.** Photographs and videos are taken exclusively through the in-app camera; gallery imports are refused in the live-capture class (Principle 4). The app records satellite position, network-synchronised time (NTP, cross-checked against device clock drift), device attestation, and the operator's account identity.
- **Step 2 — Hash.** A SHA-256 digest of the file plus its capture manifest is computed on the device. The original never needs to leave the client unencrypted; the digest is what travels.
- **Step 3 — Qualify.** The digest is sent to a qualified trust service provider (QTSP) on the EU trusted list, which returns an RFC 3161 qualified timestamp token — the statutory rail.
- **Step 4 — Batch.** Digests are aggregated into a Merkle tree. Batching keeps the marginal cost of sealing near zero regardless of chain fees, enabling the freemium economics of Part IV.
- **Step 5 — Anchor.** At least hourly, the Merkle root is written to a public blockchain — the neutral rail. Each record stores its Merkle inclusion path, so any single record can be verified against the on-chain root without revealing any other record in the batch.

4.1 Merkle aggregation

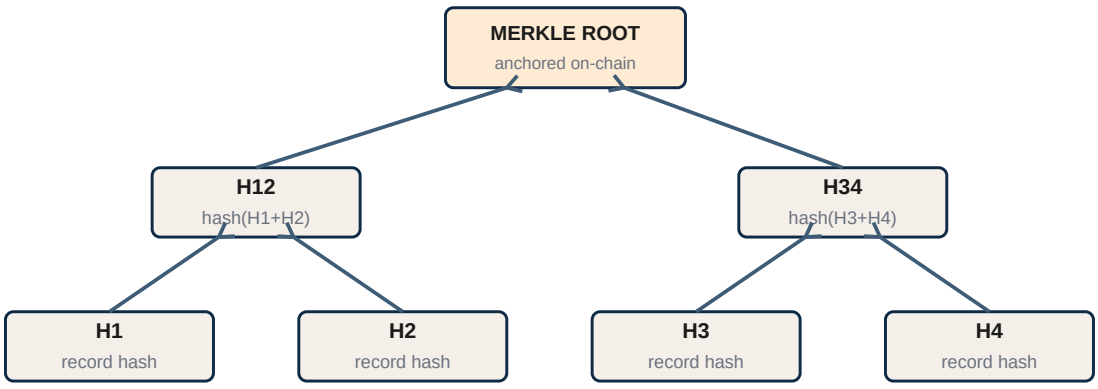

Figure 3 — Merkle aggregation. Legend: H1–H4 = individual record digests; interior nodes = pairwise hashes; root = the only value published on-chain. A record proves its inclusion with a logarithmic-size path (e.g. H2 needs only H1 and H34), preserving confidentiality of all sibling records.

The offline case is a first-class citizen: construction sites often lack connectivity. Captures are hashed and queued locally with the device's attested clock; the qualified timestamp is obtained at first reconnection. The Evidence Report then displays two times — attested capture time and qualified sealing time — with the gap stated explicitly (Principle 5: honest scope).

5. Trust Model and Threat Analysis

The design assumes every actor may be adversarial, including SiteSealed itself. The table summarises the principal threats and the mechanism that neutralises each:

Threat	Attack	Countermeasure
Backdating	Party fabricates a record 'from' an earlier date	Qualified timestamp + chain anchor make earlier sealing impossible to forge
Tampering	Record altered after the fact	Any change breaks the SHA-256 digest against both rails
Vendor capture	SiteSealed alters or deletes records	SiteSealed holds only hashes of encrypted content; proofs verify without it (Pr. 1, 6)
Staged capture	Photographing a screen or a staged scene	Not claimed to be solved: reports state proof scope honestly (Pr. 5); context binding (location, device, operator) raises the cost of staging
Clock spoofing	Device clock manipulated while offline	Dual time display; attested clock drift bounds; qualified time at reconnection
Chain failure	Anchor chain reorganises or halts	Dual rail: eIDAS proof independent of chain; re-anchoring policy on secondary chain
QTSP failure	Provider ceases or loses qualification	Dual rail: chain anchor independent of provider; tokens remain verifiable per eIDAS

Table 1 — Threat model. 'Pr.' refers to the Founding Principles of Part I.

Note the deliberate honesty of the fourth row. A sealing system proves existence, integrity and time; it cannot prove that reality was not staged in front of the lens. Competitors who imply otherwise will lose credibility in the first serious cross-examination; SiteSealed's refusal to overclaim is a durable trust asset (Principle 5).

Part III — Legal Foundations

6. Admissibility: the Dual-Rail Rationale in Law

The legal environment converged in the mid-2020s toward exactly the architecture specified above. Three developments matter:

- **Qualified timestamps carry a presumption.** Under the eIDAS framework, a qualified electronic timestamp enjoys a presumption of the accuracy of the date and time it indicates and of the integrity of the bound data. In practice, this shifts the burden: the party contesting a sealed record must prove tampering, instead of the producing party proving authenticity. For an industry where authenticity challenges are the

default litigation tactic, this reversal is the product's core legal value.

- **Public-chain timestamps are gaining recognition as evidence.** Courts in several jurisdictions have admitted blockchain-anchored timestamps as proof of a document's existence at a given date, evaluating them under ordinary electronic-evidence rules rather than rejecting them as a novel category. Recognition is jurisdiction-dependent and weighed case by case — which is precisely why the chain anchor is a complement, never a substitute, to the qualified rail.
- **Arbitration scholarship supports self-proving records.** Recent doctrinal work on international construction arbitration concludes that hashed, timestamped, consensus-anchored project records can satisfy admissibility, relevance and weight thresholds while removing conventional authentication burdens. International arbitration — the venue of the largest construction disputes — is thus the environment where the dual-rail record is most valuable.

7. What a Sealed Record Proves — and What It Does Not

Every Evidence Report carries this scope statement verbatim, as a fixed element of the product (Principle 5):

> *"This report proves that the listed files existed in exactly this form no later than the certified time, that they have not been altered since, and that they were captured through an attested device and account at the recorded coordinates. It does not, by itself, prove who or what is depicted, nor that the depicted scene was unstaged. Those questions remain matters of ordinary evidence and testimony."*

This candour is strategic, not merely ethical: a report that states its own limits survives cross-examination and educates tribunals, becoming the format lawyers ask for by name.

Part IV — Economics

8. The Cost Inversion, Quantified

The economic thesis is observation O4 made explicit: money spent at capture time replaces multiples of that money spent at dispute time. The chart below expresses the conceptual relationship (indexed, illustrative — not a measured dataset):

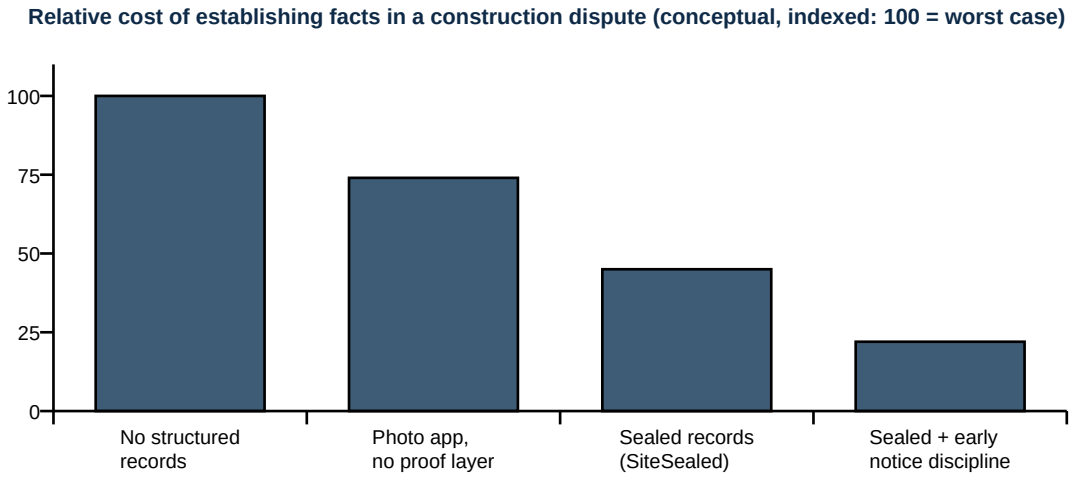

Figure 4 — Conceptual cost of establishing facts in a dispute, by documentation posture. Legend: bars are indexed to the worst case (100). The step from the second to the third bar — proof-grade sealing — is the value SiteSealed captures; the fourth bar adds contractual notice discipline built on the sealed chain (P6).

9. Revenue Model

Tier	Who	Price basis	Includes
Verify	Anyone, forever	Free (Principle 7)	Public verification portal, proof checking, open tooling
Site	Small contractors, architects, owners	Per active project / month	Unlimited sealed captures, offline queue, project timeline
Case	Claims consultants, counsel	Per Evidence Report	Court-ready report, full proof bundle, chain-of-custody annex
Fleet	GCs, insurers, developers	Annual, per portfolio	API, roles and delegation, retention policies, priority anchoring

Table 2 — Genesis pricing structure. Numeric price points are a versioned annex, not part of this document.

Two consequences of Principle 7 deserve emphasis. First, free verification is the distribution engine: every report sent to an opposing party, insurer or tribunal is a demonstration to a new professional audience, at zero acquisition cost. Second, because revenue never depends on holding data hostage, churned customers keep their proofs — which removes the single biggest objection to adopting a young vendor for decade-long liabilities.

10. Go-to-Market

Entry wedge: **handover and snagging documentation**, the moment of maximum dispute density and minimum workflow change. First audience: English-speaking claims consultants, quantity surveyors and construction counsel — the professionals who monetise evidentiary chaos today and can prescribe its cure tomorrow. Expansion follows the record classes: site diaries, contractual notices, delivery and weather

logs, then API integration into existing field platforms, for which SiteSealed becomes the neutral proof layer rather than a competitor.

Part V — Trajectory and Governance

11. Phased Roadmap 2026–2037

Phase	Window	Milestone
0 — Validation	2026	Ten practitioner interviews; mockup; QTSP partnership terms; kill/continue decision on prevention-vs-litigation willingness to pay
1 — Genesis	2027	Capture app + sealing service + verification portal; first hundred sealed projects; first Evidence Report used in a real negotiation
2 — Standard	2028–2030	API for field platforms; insurer pilots; the report format cited by name in professional guidance
3 — Layer	2031–2037	Sealing embedded invisibly in third-party tools; SiteSealed as infrastructure — the proof layer of the built environment

Table 3 — Roadmap. Phase 0 precedes all engineering: the project earns the right to be built by surviving contact with practitioners.

12. Document Governance

Part I of this document is immutable. Parts II–V constitute the Genesis specification and may be superseded by numbered revisions (v1.1, v2.0…), each of which must state its changes and demonstrate conformity with Part I. The SHA-256 digest of this PDF will be sealed through the project's own pipeline upon release — the whitepaper as the first customer of its own proof layer.

Glossary

Anchoring — Writing a digest (here, a Merkle root) into a public blockchain transaction, fixing its existence at that block's time.

eIDAS — The EU regulation establishing electronic identification and trust services, including qualified electronic timestamps with statutory presumption of integrity.

Evidence Report — SiteSealed's exportable PDF bundling records, proofs, capture manifests and the scope statement of Section 7 — the artefact lawyers actually use.

Merkle tree — A binary hash tree allowing one published root to commit to many records, each verifiable individually via a short inclusion path.

QTSP — Qualified Trust Service Provider: a supervised entity on the EU trusted list issuing qualified timestamps (RFC 3161).

Qualified timestamp — A timestamp issued by a QTSP, presumed accurate and integrity-preserving before EU courts.

SHA-256 — The cryptographic digest function binding a record's content to a fixed-length fingerprint; any alteration changes the fingerprint.

Sealing — The full pipeline of Figure 1: capture, hash, qualify, batch, anchor.

Closing Note

Bitcoin's whitepaper succeeded because it solved one narrow problem — double spending — with components that already existed, assembled under a clear adversarial model. SiteSealed follows the same discipline: no new cryptography, no token, no speculative layer; only mature primitives — digests, qualified time, Merkle commitments, public consensus — assembled so that the construction industry's most expensive question, *who knew what, when*, stops being a question. The record is sealed the moment it is made. Everything else is litigation archaeology, and it ends here.

SITESEALED — Founding Whitepaper v1.0 Genesis Edition — August 2026