EGOIST PROVENANCE IDEATHON SUBMISSION

Provenance:
Built on AI Passport - Controlled Work Disclosure & Audit Receipts

Turning uncompensated work disclosure into leverage

Team: Parth Kharche
Track: Work
Lane: Concept

---

1. Short Summary

Provenance turns uncompensated, high-risk work disclosure into something provable and controllable. Before any contract or payment exists, a freelancer, candidate, founder, or researcher can share original work through a passkey-protected, time-boxed, watermarked view, with every access event logged as a signed Audit Receipt on their passport page. Share confidently, knowing exactly who saw what, when, and under what terms.

2. Problem Statement

Anytime someone has to show unpublished, original work before a formal agreement exists, they lose control the moment it's seen — and today, there's no record of what was shown, to whom, or under what terms.

New freelancers, often students taking on side income, deliver a website, design, or video and wait for payment. When the client ghosts them, legal action is disproportionate to the amount owed, and public complaints on social media platforms rarely produce results.

Engineering candidates face a related problem. Asked to demonstrate original work — a self derived and designed actuator, an unconventional boat hull profile, a novel wind tunnel design — during an interview, they hand over a CAD file or report. If the company uses the idea internally without acknowledgment or employment/internship offer, the candidate has, at best, a file with a creation date: proof the file existed, not proof of what was disclosed or under what terms.

This isn't an isolated complaint. On professional forums like Blind, candidates describe an identical pattern at major companies — multi-day take-home assignments treated as free consulting work, with no compensation and no hire/offer at the end. The design industry has had a formal position against uncompensated “spec work” for decades, through AIGA — proof the underlying problem is old and widespread, but that no enforcement mechanism has ever existed for it, only a voluntary ethical stance. Provenance is that missing mechanism.

Existing tools don't close this gap: NDAs are slow and disproportionate for a single interview or pitch; static watermarks don't restrict access or expire; expiring Drive/Dropbox links solve part of it, but the access record lives inside one platform, isn't portable, and isn't verifiable to a third party.

3. Affected User Groups

Primary:

- Freelancers and engineering job candidates, frequently asked for uncompensated speculative or take-home work.

Secondary:

- Hardware founders and engineers, exposed to IP risk during vendor quoting.
- Startup founders, sharing financials, roadmaps, and prototype details with investors before any funding or NDA exists.
- Researchers, required to prove novelty or priority without revealing unpublished results.

4. How Provenance Is Used

- Owner selects the work asset to disclose from their Passport Visibility Settings.
- Owner selects exactly which components of the work are visible — any combination of title, abstract, images/renders, 3D model, data, graphs, and references, independently toggled, rather than a fixed tier — and sets the expiry window. The raw file itself stays withheld by default, reserved for the payment/escrow gate.
- System generates a passkey-protected access link tied to the owner's passport page.
- Recipient accesses the link — view-only, session-watermarked, no download or export, account required for maintaining verified entries and logs.
- Every view triggers a cryptographically signed Audit Receipt, logged permanently to the owner's passport page.
- Access auto-expires, or is manually revoked by the owner, or instantly revoked on detected tampering.

5. Context, Permission, Proof & Access

Context: which asset, which recipient, what time window, which specific components are exposed (abstract, images, model, data, graphs, references, each independently toggled).

Permission: view-only, time-boxed; no download, no further re-share.

Proof: a cryptographically signed, timestamped Audit Receipt, visible on the owner's passport page.

Access: recipient needs only the link, passkey and registered account; revoked on expiry, manual kill-switch, or detected tampering.

6. Why This Must Travel Across Tools

An expiring Drive or Dropbox link solves part of this, but the record of what was shared lives inside that one platform — it isn't portable, isn't verifiable to a third party, and disappears if the link or account is deleted. A freelancer's disclosure might happen over WhatsApp, an interview submission through a company's internal

portal, or a research draft sent by email — three different tools, none of which share a common, trustworthy record of what was shown or when. Provenance needs to be the one constant across whichever tool the work happens to pass through, because the disclosure record must outlive and outrank the platform it was shown on — otherwise the proof disappears the moment the conversation moves elsewhere, which is exactly what happens today.

7. Access Control & Revocation Matrix

Scenario	Who Controls?	Auto Expiry?	Manual Kill-Switch?	Tamper Detection?
Freelance / Client Disclosure	Owner (freelancer)	Yes	Yes	Yes
Candidate Submission	Owner (candidate)	Yes	Yes	Yes
Vendor Engagement	Owner (founder)	Yes	Yes	Yes
Investor Pitch	Owner (founder)	Yes	Yes	Yes
Researcher Pre-Release	Owner (researcher/founder)	Yes	Yes	Yes
Third-Party Re-Share	Not permitted	N/A	N/A	N/A

8. Privacy & Risk Mitigation

Data minimization: recipients need account only for cryptographic signature; only access metadata (who, when, which components, duration) is logged, never the underlying content beyond a volatile, encrypted view session.

Attack vectors and mitigations:

- Screenshot/screen recording: mitigated via session-unique watermarking, not prevented outright — the honest claim is traceability, not absolute prevention.
- Log fabrication: prevented via cryptographic timestamping and signing at the moment of access, not editable afterward.
- Network exfiltration: session-unique links and rapid expiry limit exposure.

We're explicit about the limit here: nothing stops a camera pointed at a screen, or a determined internal leak. The system's value is evidentiary weight and access discipline after the fact, not an unbreakable seal.

9. V1 Scope vs. V2 Roadmap

V1 (this submission's working principle, only UI): Passkey share drawer with a granular component selector (title, abstract, images, 3D model, data, graphs, references — each independently toggled, raw file withheld by default), auto-expiry timer, signed Audit Receipt log, and manual revocation.

V2: Deployable Session-based dynamic watermarking, integrated escrow/payment gate, anti-tamper canvas.

As an ideathon Concept-lane entry, this document demonstrates the working principle — the claim structure and the flow — rather than a built product; a functioning demo is not required for this lane.

The same underlying primitive (prove, carry, revoke) could extend to enterprise data-sharing contexts already served by data-exchange and supplier-trust platforms — this entry stays focused on the individual case, where no comparable protection exists today.

Closing line

This entry is for freelancers and job candidates, who need to prove their work was disclosed under specific, time-limited terms to clients and hiring companies, so they can protect their authorship and payment leverage without giving away more context than necessary.

P.S.: Random bonus idea, feel free to ignore – **NFC**[Near Field Communication]! Most new phones already have the chip, so instead of scanning a QR code, you just tap your phone to the card and the page loads. No scanning, no fumbling, and the chip could live right inside the card itself. Also, ngl, it just looks cool, like a little magic trick when your profile pops up instantly. The egoist page of user basically becomes a digital business card too, thus no more card exchanges.