Sandbox — QA

Chain brief — the thesis, the claims and the exhibits that carry them.

ROOM	sandbox
PREPARED FOR	—
SCOPE (OWNER'S WORDS)	QA room for maya and noah. Nothing here is evidence.
GENERATED	2026-11-11T00:34:34Z by cli
EXHIBITS CITED	1 of 17 files in the room
LATEST SEALED SNAPSHOT	none yet

ENIACoc Labs, Inc. · Delaware file 10808046 · This brief restates what the room's files, thesis and timeline contain. It makes no legal finding. Every exhibit is identified by its SHA-256 fingerprint; the room's chain and snapshots carry the record of who added, read and cited what, and when.

1. The thesis

— no summary written yet —

2. The claims

> **CLAIM 1 · OPEN · SHQA · 2026-11-09**
>
> The permission ledger records that com.example.remotehelper held four sensitive grants simultaneously — Screen Recording, Accessibility, Input Monitoring, and Send Keystrokes & Mouse Events — all set via System Settings and last modified between 2026-10-02T21:14:05Z and 2026-10-02T21:15:02Z.
>
> Four high-sensitivity controls granted to one bundle id within ~1 minute — the most concentrated grant cluster in the ledger.
>
> Proposed by Sherlock (session 067cd617), applied by shqa.
>
> **A** TCC.db `permission ledger` `sha256 04448fb52305be98…` — access row 1, access row 2, access row 6, access row 7 · proposed by Sherlock

3. The timeline

No events written by the reviewers.

4. The exhibits

	FILE	WHAT IT IS	SIZE	SHA-256	FIRST SEEN · VERSIONS · STATE
A	TCC.db Artefacts (synthetic)	permission ledger	52 KB	04448fb52305be98306fb67e0c0eea832 6821052e90a6ec0054471f05dea25f0	1 version · preview_ready

Custody of parsed exhibits

	INPUT SHA-256	PARSER	OUTPUT SHA-256	PARSED
A	04448fb52305be98306fb67e0c0eea8326821052e90a6ec0054471f05dea25f0	sherlock_artifacts/3.1.0	7d29374d5e15a4c8a14e4692ef99f0a8aa8158d1b884ff90075fb5cc27cf03c4	2026-11-09T11:58:42Z

5. Glossary

permission ledger
The macOS record of which program held which access (screen recording, keystrokes, files, camera…), how the access was granted, and when the record last changed.

SHA-256 fingerprint

A 64-character code computed from a file's bytes. The same bytes always give the same code; one changed byte gives a different one. It identifies an exhibit exactly.

snapshot
A sealed zip of the whole room at a point in time, with a signed manifest. Its own fingerprint is listed; it can be verified without this platform.

chain (audit chain)
The room's append-only log: every upload, read, download, claim and note, each entry hashed with the one before it, so nothing can be removed or reordered unnoticed.

claim
A numbered sentence in the thesis, with the exhibits that support it. Status: open, supported, contested or withdrawn.

exhibit
A file in the room. It is never edited; a replacement becomes a new version and both stay.

UTC
Coordinated Universal Time. Every time in this brief is UTC unless marked otherwise; a device whose clock was wrong stays wrong in its own records.

custody
For parsed exhibits: the input fingerprint, the parser version and the output fingerprint — how a reading was obtained from the raw file.

6. How to verify

1. Any exhibit: compute its SHA-256 (`sha256sum <file>`) and compare with section 4.

2. The room at a point in time: the sealed snapshot's zip fingerprint above; inside the zip, `manifest.json` lists every item with its fingerprint and the room's signing key id; the platform's `verify-export` checks the signature offline.

3. This brief: its own SHA-256 is written beside it (`brief-<ts>.sha256`) and recorded in the room's chain when it was generated.

ENIACoc Labs, Inc. · Delaware file 10808046 · brief.py 1.0.0