KASPA INDUSTRIAL INITIATIVE

TRUSTED TRADE INFRASTRUCTURE · KASPA LAYER 1

Kii has turned the trusted-trade concept into a running system.

Kii has built a working implementation of the trusted-trade design set out in the IDC UAE/ADGM white paper (1 Jun 2026) and the IDC → AD Ports teaser (Jul 2026): running, proven at consensus on a public chain, and reproducible by your own engineer from a kit, without trusting us. It is mapped from Kii's existing KiiWORKS platform and built at our own cost, because the only honest way to answer the feasibility question was to build it.

PROOF OF CONCEPT · PUBLIC TESTNET (KASPA) · AUDIT AND LEGAL OPINION SCOPED, NOT YET COMPLETE

FIVE CONTROLS NO PLATFORM ASSERTION CAN FAKE: EACH LIVE, WITH REJECTION EVIDENCE

1. **Controlled Trade Record (CTR).** One owner, provable everywhere: a transfer signed by anyone but the current controller is rejected by consensus, and the record structurally cannot be duplicated in flight, enforced by the network, not asserted by a database.

2. **Escrow lock.** A locked record rejects transfer, amendment, conversion to paper and a second pledge: every rejection demonstrated live with a recorded transaction id; release only by the declared authority, or at maturity read from the chain's own clock.

3. **Release gate.** An Assurance Certificate (AC) cannot be minted unless the escrow lock exists and a risk partner's approval is cryptographically attested; consensus refuses the mint otherwise, in the estate's first two-covenant co-spend.

4. **Cross-organisation singularity.** A duplicate issuance of the same instrument is rejected by a second operator's independently-run node, perimeter-scoped over the registered set, and we say so.

5. **ZK compliance credential.** A real RISC Zero STARK verified in-consensus (Groth16 receipt): role authority and screening status proven without revealing the underlying identity attributes.

WHY KASPA: IN THREE LINES

- A proof-of-work L1 at ~10 blocks per second: confirmation in seconds, fees in fractions of a cent; trade moves at port speed, not settlement speed.
- Covenants, transaction introspection and in-consensus zero-knowledge verification are mainnet law since mid-2026: shipped protocol only, nothing promised against a roadmap.
- No bridge, no sidechain, no privileged operator: the controls live where no one (not IDC, not AD Ports, **not we**) can override them. That is what makes the assurance sellable.

---

*Discipline behind every claim: a covenant invariant only counts when consensus **rejected** its violation and the txid is recorded beside network, genesis and DAA. A control that has never failed is not known to work.*

THE EVIDENCE, AND HOW TO CHECK IT WITHOUT TRUSTING US

What is proven, how a sceptic verifies it, what remains external

PROPERTY	PROVEN BY	CHECK IT YOURSELF
Exclusive control	Live TN10 consensus rejections: wrong signer, lifted signature, self-endorsement, fan-out, burn; plus the honest accepts they negate.	Resolve every txid in kit/TXID-EVIDENCE.md on the public explorer (api-tn10.kaspa.org).
Escrow lock	Every escrow invariant carries a live rejection: transfer / amend / convert while locked, second pledge, forged release, unmatured release, dead-record resurrection.	Same txid list; each entry states what should and should not resolve.
Release gate	AC mint refused against an unlocked record and refused without attested approval; honest mint accepted, a two-covenant co-spend at consensus.	Explorer plus the line-by-line demo transcript in the kit.
Singularity	A second operator's independently-run TN10 node rejected the duplicate issuance at consensus (perimeter-scoped over the registered set, stated as such).	Transcript + explorer: the duplicate txid does not exist on-chain.
Dispute finality	The determination releases the escrow lock at consensus, not by API; an unauthorised determiner is rejected.	Transcript + explorer.
Evidence pack	Verifies offline with no platform access; a tampered pack fails naming the failing component; anchors resolve from a plain public node via their accepting block.	Run the checksummed verifier binary on both shipped packs: about three minutes, no network needed.
Commitments	One commitment scheme end to end, domain-separated (ADR-003); expected digests are derivable by hand.	printf | sha256sum: three POSIX utilities, none of our software.
Hardening	Red team run to two consecutive dry rounds: six confirmed findings, all fixed or accepted-with-disclosure; mutation matrices show zero unguarded invariants; a 65-finding self-audit preceded any external review.	Read the dispositions in the repo (private; invite on request); delete any named rule and a test goes red.

All live evidence is on testnet-10 (genesis f896a303…1cc4370) and is perishable by nature: a chain reset voids every recorded txid at once. The offline artifacts (packs, commitments, verifier) survive a reset. Network, genesis and DAA are recorded beside every claim for exactly this reason.

WHAT REMAINS EXTERNAL: THE GAP IS PEOPLE AND PAPER, NOT CODE

- **A named counterparty**: the programme's original activation trigger, unchanged; the kit is the conversation opener.
- **Legal opinion (ADGM / English law)**: the MLETR reliable-system question; counsel instruction pack drafted and ready.
- **Independent security audit**: scope document drafted and ready; a firm and funding.
- **External reproduction of the kit**: an engineer outside the project runs the five checks and reports back; their report is the gate.

Kaspa Industrial Initiative · Trusted Trade Infrastructure
[Contact details on request]