LUVION LITEPAPER

High-Threshold Authorization Infrastructure for Institutional Digital Assets

Public Technical Overview

Luvion Labs | 2026

Luvion is developing a high-threshold signing infrastructure layer for institutions operating high-value digital-asset workflows. The system is designed to reduce signer-concentration risk, improve operational continuity under node churn, and preserve a staged migration path toward post-quantum signing.

1. Executive Summary

Luvion addresses a specific weakness in institutional digital-asset infrastructure: the authorization layer beneath custody, treasury, wallet, and protocol operations. Many systems improve on single-key custody while still relying on low-threshold approvals, static signer assignments, or recovery procedures that remain operationally fragile under real-world conditions.

The current technical core is centered on a 22-of-33 threshold signing path using ML-DSA-65, with local and WAN demo evidence already prepared for review. The broader architecture extends this core toward dynamic committee operations, recovery-oriented node management, and chain-specific integration paths. Sui is the first ecosystem integration direction; the near-term account-auth compatibility path uses threshold Ed25519/FROST, while threshold ML-DSA remains the long-term post-quantum migration layer.

This document is a lightweight public technical overview. It explains Luvion's architecture, current evidence, delivery boundaries, and integration direction without replacing the full technical whitepaper, implementation summary, or chain-specific architecture materials.

2. Market Problem

Institutional digital-asset operations increasingly secure stablecoins, tokenized assets, custody balances, protocol treasuries, and enterprise wallet flows. However, the approval logic behind those operations is often still concentrated in a small number of parties or bound to static signer configurations.

- **Low-threshold exposure:** small approval sets reduce the number of parties that must be compromised before an attacker can authorize a high-value action.
- **Static committee risk:** long-lived signer assignments create durable targets for reconnaissance, coercion, and insider-collusion preparation.

- **Recovery fragility:** node loss, coordinator failure, or signer churn can force heavy manual procedures when the authorization layer is not designed for continuity.
- **Migration debt:** classical signing stacks may later require difficult upgrades if post-quantum transition planning is deferred too long.

Luvion treats these issues as parts of the same control problem. The objective is not merely to secure a key, but to harden how institutions approve, recover, and evolve signing authority over time.

3. Luvion Solution Positioning

- **High-threshold architecture:** a 22-of-33 signing path designed to raise the compromise requirement beyond low-threshold defaults.
- **Dynamic committee direction:** architecture intended to reduce the long-window exposure created by fixed signer assignments.
- **Recovery-oriented node design:** protocol direction focused on liveness, resharing, and continuity under node events.
- **Post-quantum migration path:** threshold ML-DSA retained as the long-term cryptographic moat while near-term integrations remain compatible with current chain authentication models.
- **Institutional integration path:** signing infrastructure intended to sit beneath custody, treasury, wallet, and protocol workflows rather than replace them at the interface layer.

4. Architecture Overview

4.1 Signing Core

The implemented repository path uses a two-round threshold signing protocol based on the ML-DSA-65 parameter set. The current system includes 33 signer nodes, a 22-node threshold requirement, Shamir-shared secret material, persistent signer-node runtime, and a coordinator path for probing, committee selection, ceremony execution, aggregation, and verification.

4.2 Authorization Flow

1. Policy and transaction context define the required authorization conditions.
2. An eligible signing committee is selected according to the operating model for the session.
3. Threshold participants complete the signing ceremony without reconstructing the full private key in a single node.
4. The aggregated result is verified and passed into the target transaction workflow.

4.3 Chain Integration Strategy

Luvion separates its cryptographic core from chain-specific compatibility layers. For Sui, the current architecture uses threshold Ed25519/FROST as the near-term account-auth path so that the final output remains compatible with Sui's existing signature-verification model. The ML-DSA path remains the long-term post-quantum migration layer and core protocol differentiator.

5. Current Scope and Delivery Boundaries

Area	Current public status	Next required step
Threshold core	22-of-33 ML-DSA signing path implemented with demo and benchmark evidence.	Continued hardening, review packaging, and broader validation.
Key generation	Current demo materials use a synthetic dealer path; this is not production DKG.	Production DKG hardening and external review.
Transport	Persistent TCP runtime demonstrated in controlled environments.	Authenticated transport and production-grade networking controls.
Sui integration	Architecture defined; near-term compatibility path specified.	Move / PTB prototype, testnet-grade validation, and integration review.
Assurance	Third-party audit not yet completed.	Threat model, audit scope, remediation cycle, and pilot evidence.

6. Why 22-of-33

Low-threshold signing remains useful for many workflows, but it compresses the compromise problem into a small signer set. Luvion's 22-of-33 model is intended for workflows where the value at risk justifies a materially higher authorization bar. The design aims to preserve operational viability while increasing the number of coordinated parties required for unauthorized signing.

The threshold alone is not a complete security guarantee. Its value depends on the surrounding system: key-generation discipline, signer independence, transport security, committee operations, failure handling, monitoring, and audit closure. Luvion's roadmap therefore treats production hardening and operational assurance as part of the protocol, not as afterthoughts.

7. Representative Use Cases

- **Stablecoin issuers:** treasury and mint / burn approval workflows that require stronger authorization discipline.
- **RWA platforms:** issuance, redemption, and treasury operations with long-lived institutional exposure.
- **Custody platforms:** signing-control layers that need to reduce signer concentration and improve recovery posture.
- **Enterprise wallets and treasuries:** high-value transaction workflows that justify broader approval thresholds.

8. Roadmap

Phase 1 — Audit Readiness and Integration Preparation

- Freeze review scope for threshold ML-DSA, DKG, transport, recovery, and coordinator logic.

- Prepare threat model, known limitations, reproducible demo guide, and audit package.
- Finalize Sui object / PTB integration specification.

Phase 2 — Testnet Integration and Controlled Pilots

- Validate testnet-grade Sui integration workflows.
- Run WAN, failover, and node-churn drills with traceable evidence.
- Limit pre-audit pilots to controlled technical-validation environments.

Phase 3 — Productization

- Package institutional API / SDK surfaces, deployment templates, observability, and onboarding flows.
- Convert pilot evidence into repeatable integration and commercial processes.

9. Document Positioning

This litepaper sits between Luvion's public company overview and its deeper diligence materials. Readers seeking business context should begin with the Company OnePager. Readers seeking implementation evidence should continue to the Technical Summary. Readers evaluating chain-specific compatibility should refer to the Sui Integration Plan.

Public boundary: Luvion does not currently claim completed third-party audit, production deployment, or native threshold ML-DSA account authentication on Sui.
