Sui Integration Plan

Threshold Ed25519/FROST for Sui account authentication, with ML-DSA retained as the long-term post-quantum migration layer

Public Technical Overview | Luvion Labs | 2026

1. Technical Conclusion

Luvion's near-term Sui integration path uses threshold Ed25519/FROST as the account-auth compatibility route. The current Luvion threshold-signing core uses ML-DSA-65; that path remains the long-term post-quantum migration layer and core technical moat, while a separate Ed25519/FROST transaction-signing backend is added to fit Sui's current native transaction-authentication model.

Under this model, Luvion enforces a 22-of-33 policy off-chain while Sui sees one standard Ed25519 signer and one standard Sui address on-chain. This preserves compatibility with current Sui verification rules without conflating the near-term account-auth path with the longer-term post-quantum path.

2. Goals and Scope

- Support 22-of-33 Luvion authorization for Sui transaction workflows.
- Output a Sui-native Ed25519 signature envelope accepted by current Sui account authentication.
- Integrate object and gas resolution, transaction building, simulation, submission, and effects/checkpoint monitoring.
- Keep Sui protocol verification unchanged; Luvion's threshold policy is enforced off-chain.
- Use optional Move modules only where application-layer custody, policy transparency, or shared-object workflows require them.

3. What Can Be Reused

The existing Luvion repository already provides reusable foundations for the Sui adapter: 22-of-33 orchestration, round coordination, retry behavior, timing, TCP cluster runtime, request-scoped state handling, network envelopes, VRF-style proofs, and operational experience from the threshold ML-DSA path.

The Sui integration requires additional components, including a threshold Ed25519/FROST backend, separate FROST share material, new signing-session message types, compatibility tests, and a production-grade key-generation path before any deployment-readiness claim.

4. Sui Compatibility Boundary

The integration plan is designed around Sui's existing authentication boundary. Sui's native transaction verification remains unchanged; the compatibility layer emits one normal Ed25519 signature under one aggregate public key, while Luvion manages committee policy and signer coordination outside the chain.

Mode	Role in the integration plan
Threshold Ed25519/FROST	Near-term Sui account-auth compatibility route.
Threshold ML-DSA-65	Long-term post-quantum migration layer retained within Luvion.
Sui native multisig	Useful reference capability, but not suitable for a flat 22-of-33 account-auth model.
Move shared-vault policy	Optional application-layer custody module, not a replacement for Sui account authentication.

5. Architecture Overview

The proposed flow separates policy, transaction construction, signing, and submission into distinct layers:

- **Custody / Policy API:** approves signing requests and attaches policy context.
- **Luvion Sui Adapter:** resolves objects and gas, builds transaction data, computes the signing digest, and drives the signing session.
- **Luvion Threshold Core:** enforces the 22-of-33 policy and coordinates the threshold signing flow.
- **Sui RPC Boundary:** handles reads, simulation, execution, effects, and checkpoint observation.
- **Optional Move Package:** provides application-layer discoverability or shared-object custody logic when required by product design.

6. Owned / Shared Design Principle

The preferred execution path is address-owned by default because it is simpler and better suited to low-latency institutional signing flows. Shared objects should be introduced only when product requirements demand public state, multi-actor concurrency, or on-chain policy transparency. This preserves a clear boundary between Sui account authentication and optional product-layer custody modules.

7. Current Boundaries

- The current Luvion repository does not yet provide a finished threshold Ed25519/FROST Sui signing backend.
- The current ML-DSA path is retained as the long-term post-quantum layer, not as native Sui account authentication.
- Production readiness still depends on external audit closure, production-grade key generation, authenticated transport, compatibility verification, and controlled validation evidence.
- Optional Move vaults are application-layer modules and only govern assets intentionally placed under those modules.

8. Delivery Path

- Finalize the threshold Ed25519/FROST compatibility design and interface boundaries.

- Implement the Sui adapter, object/gas resolution flow, transaction builder, and signer integration.
- Validate on testnet with compatibility checks, retry handling, and effects/checkpoint monitoring.
- Advance toward production only after audit, hardened key generation, transport controls, and pilot evidence.

Public boundary: this document describes Luvion's Sui integration architecture and delivery path. It does not claim completed production deployment, completed third-party audit, or native threshold ML-DSA account authentication on Sui today.
