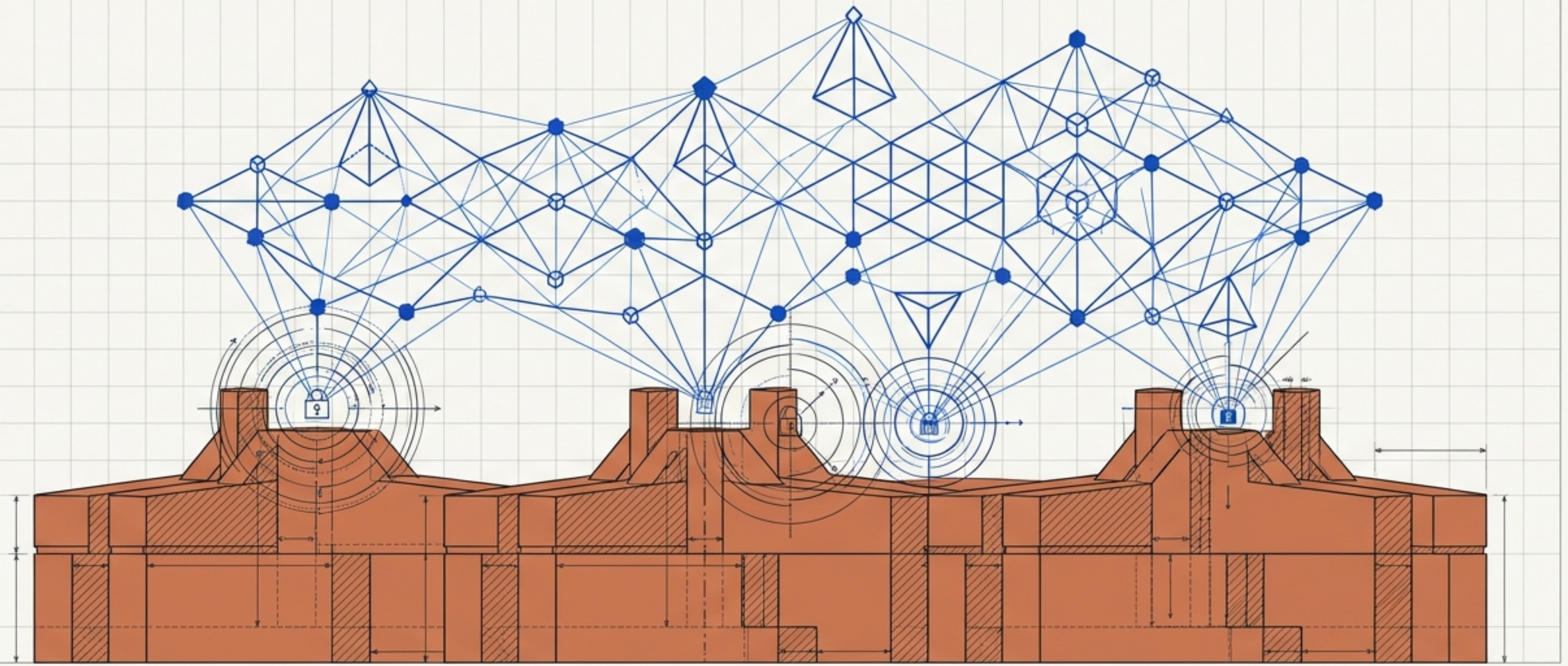
KERI + MLS: The Ultimate Architecture for Identity-Centric Group Communication

Engineering decentralised trust, forward secrecy, and autonomous key lifecycles without Certificate Authorities.



The Fragmented Security Paradigm

Traditional messaging systems solve only half the equation. Identity frameworks lack scalable confidentiality, while encryption protocols deliberately ignore identity management. True autonomy requires synthesising both.

Architectural Gap Analysis Matrix	Decentralised Trust (No CAs)	Efficient Group Messaging	Forward Secrecy	Post-Compromise Security	Autonomous Key Lifecycle
Traditional PKI	✗	✗	✗	—	✓
MLS (Standalone)	✗	✓	✓	✓	✗
KERI (Standalone)	✓	✗	✗	✓	✓
KERI + MLS (Combined)	✓	✓	✓	✓	✓

Separation of Concerns: Identity vs. Confidentiality

By strictly separating 'Who you are' from 'How we speak', each layer scales and evolves independently. MLS never manages identity; it solely references KERI Autonomous Identifiers (AIDs).

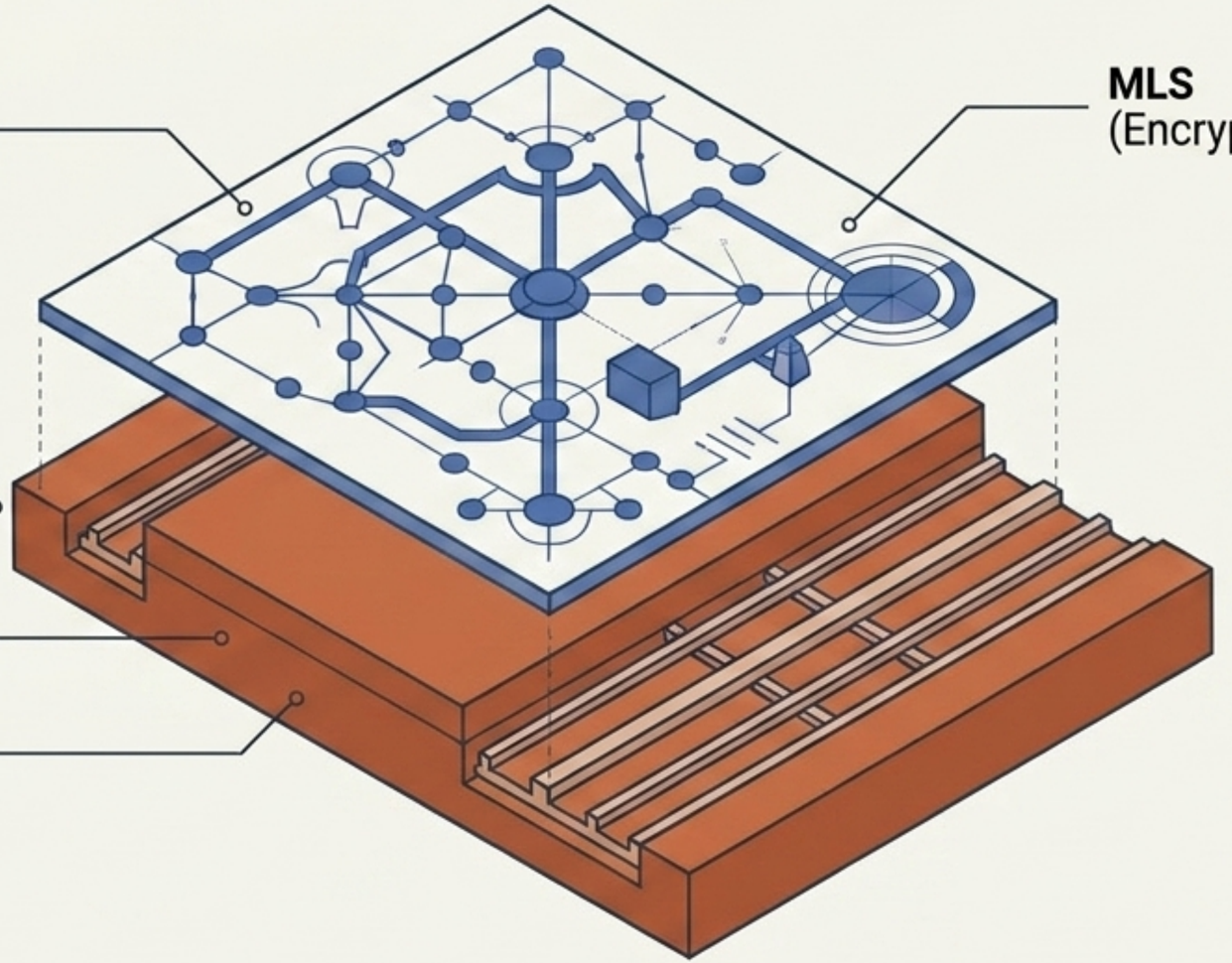
Answers: What is the current shared encryption state?

Implements:
Scalable Encrypted Group Communication
Forward Secrecy
Efficient Member Changes

KERI (Identity Layer)

Answers:
Who are you?

Implements:
Decentralised Identifiers,
Autonomous Key Rotation,
Immutable Key Event Logs (KEL)

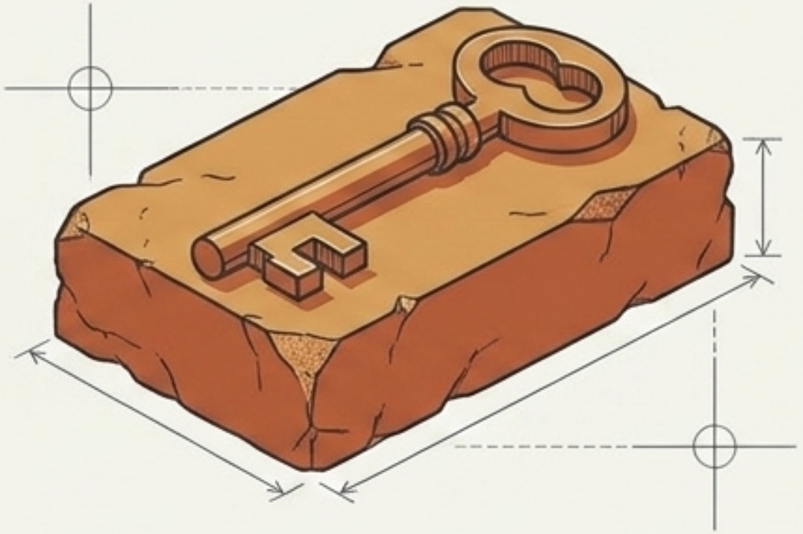


MLS
(Encryption Layer)

The Dual-Key Topology

Every participant maintains two distinct classes of keys. Identity remains durable and verifiable, while encryption state remains ephemeral and dynamic.

Identity Keys (KERI)



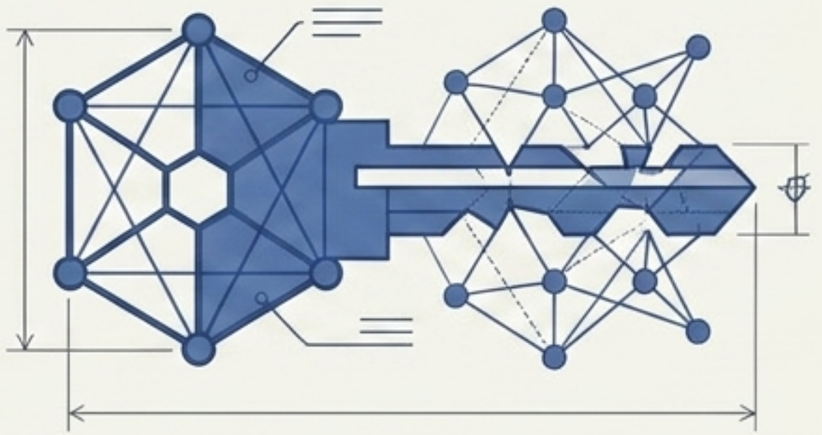
Purpose: Authentication, Signatures, KEL events

Data Structure: Key Event Logs (KEL)

Lifespan: Long-lived & Durable

Primitives: Ed25519

Encryption Keys (MLS)



Purpose: MLS Key Agreement, Group Encryption

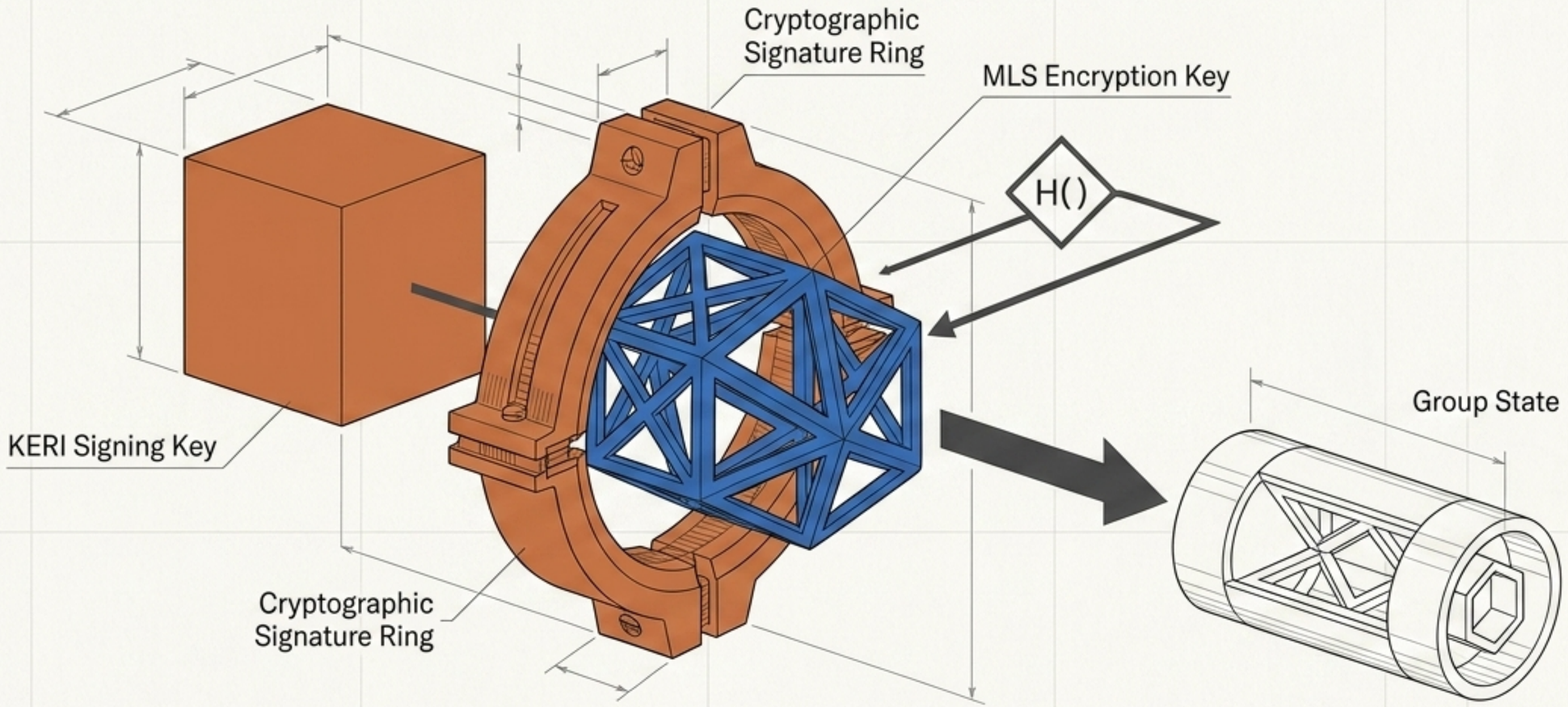
Data Structure: MLS Epochs

Lifespan: Ephemeral (Continuously rotating)

Primitives: X25519 / AES-GCM

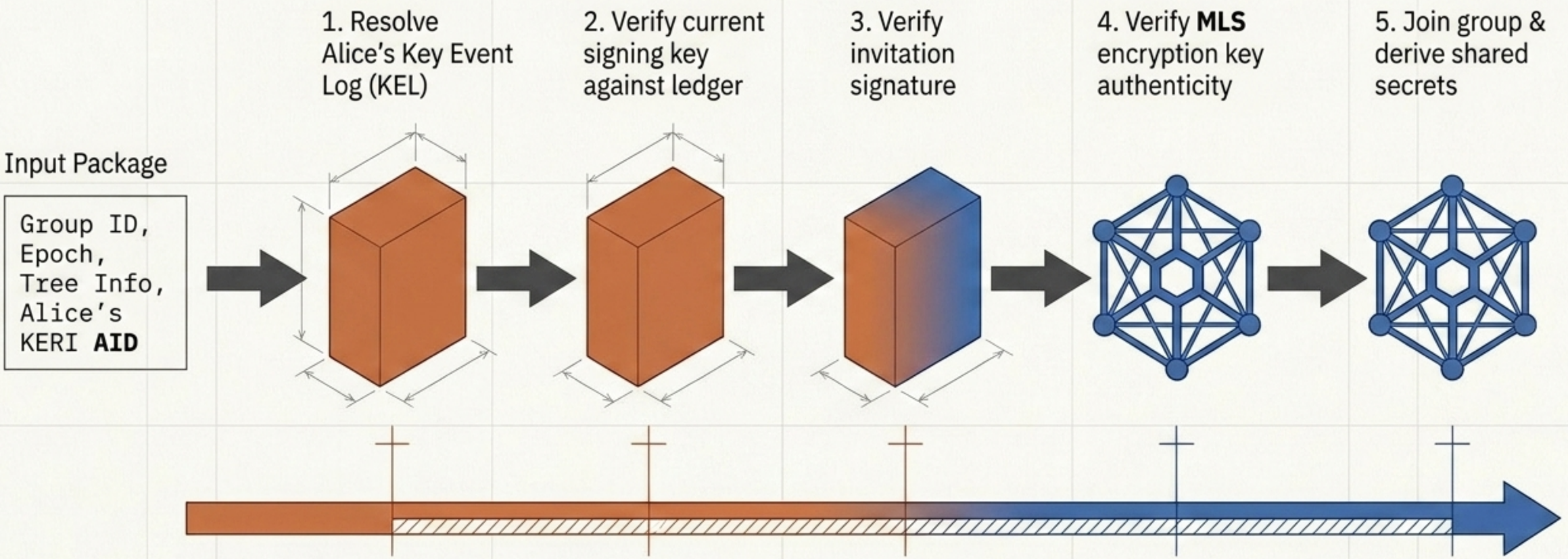
The Cryptographic Binding

The synthesis relies on a strict cryptographic wrap. By signing the ephemeral MLS key with the authoritative KERI signing key, attackers are locked out from substituting fraudulent keys. No Certificate Authorities are required.



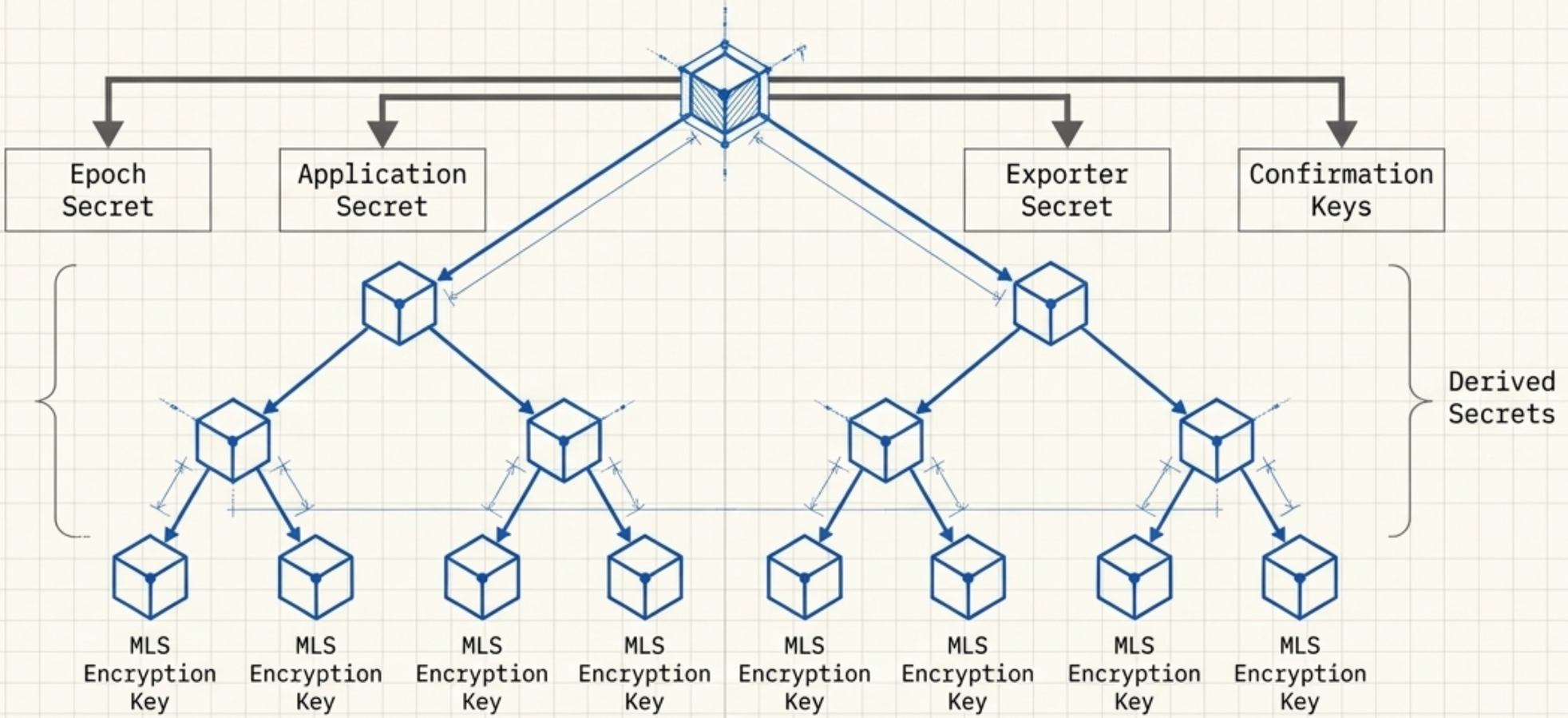
Group Initiation: Joining the Lattice

When Bob receives an invitation from Alice, he independently verifies the mathematical proof of Alice's identity before joining the shared state. No blind trust.



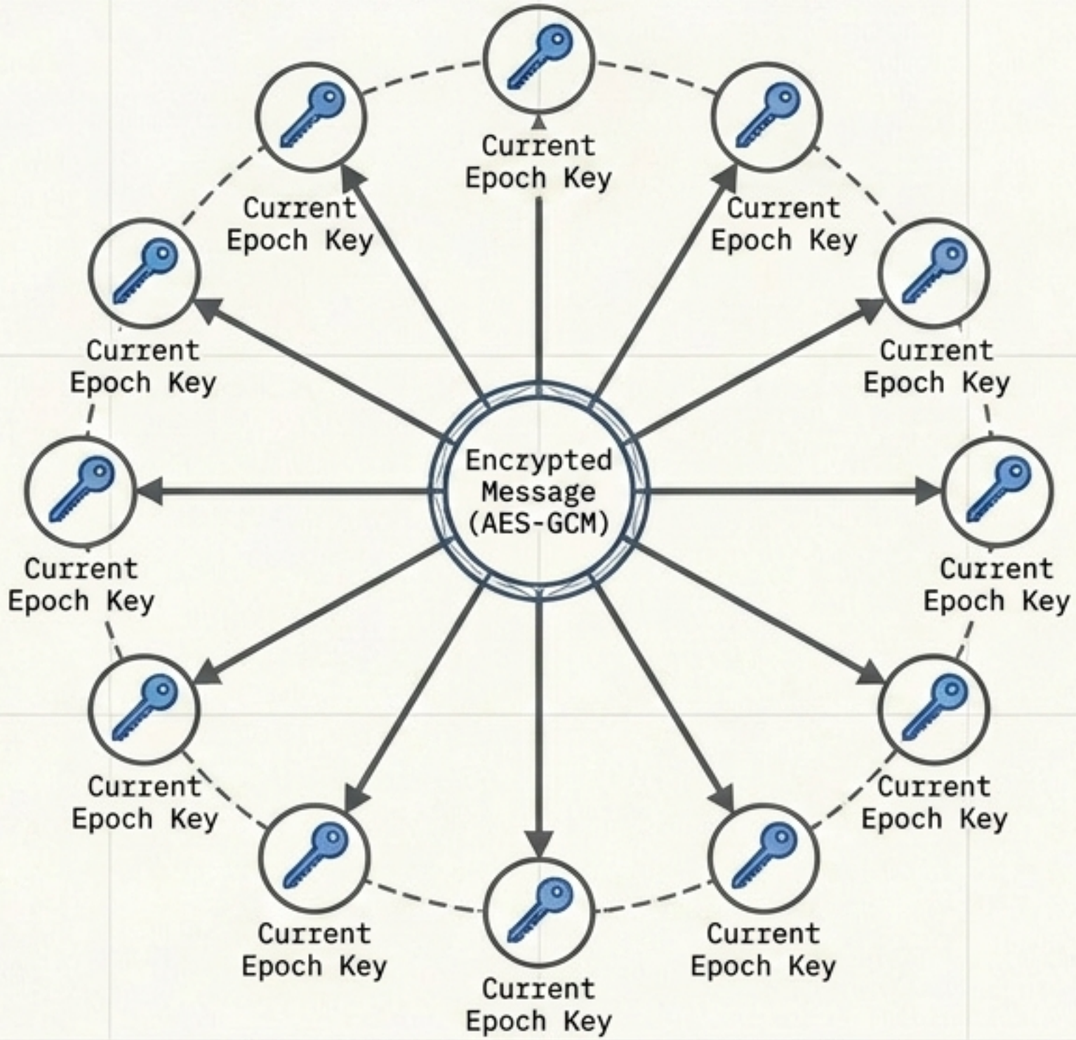
State Management: The MLS Binary Tree

Group encryption state is maintained in a strictly ordered binary tree. Derivation of the shared state is cryptographically bound to the specific configuration of group members.



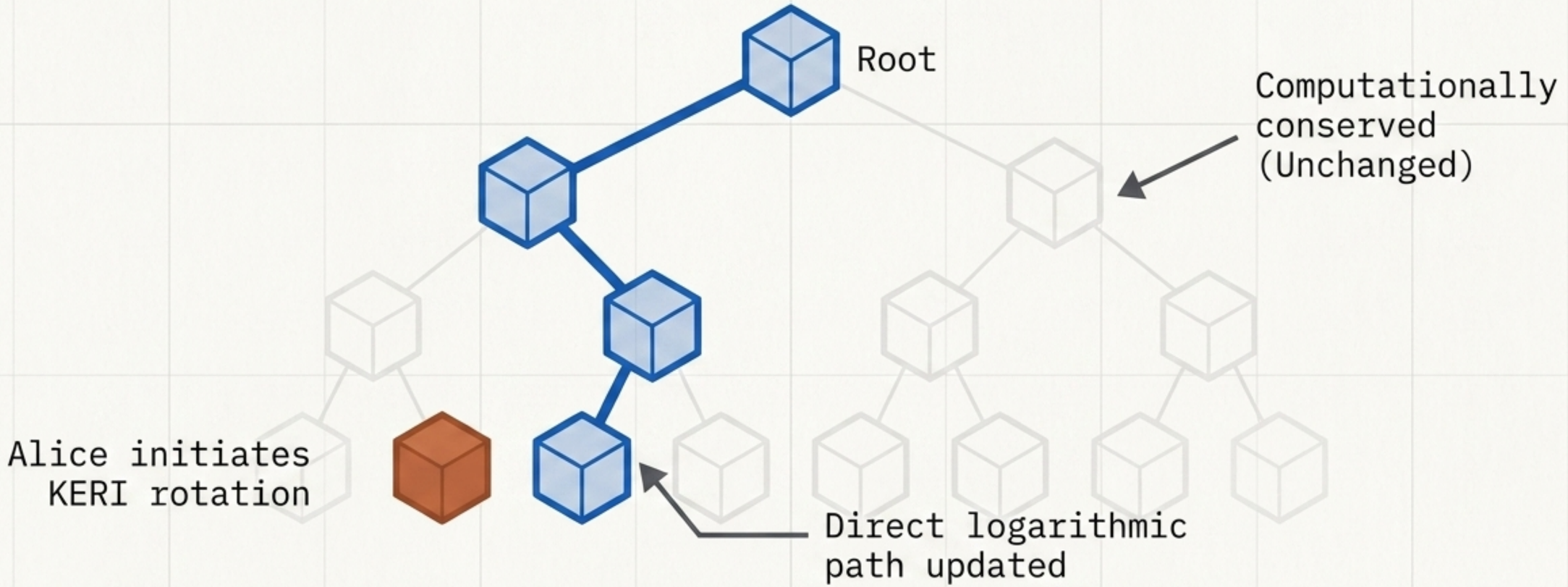
Seamless Application Flow

Once the group is established and keys are bound, messaging is highly efficient. Messages are encrypted exactly once, regardless of group size, as every authorised member possesses the current epoch key.



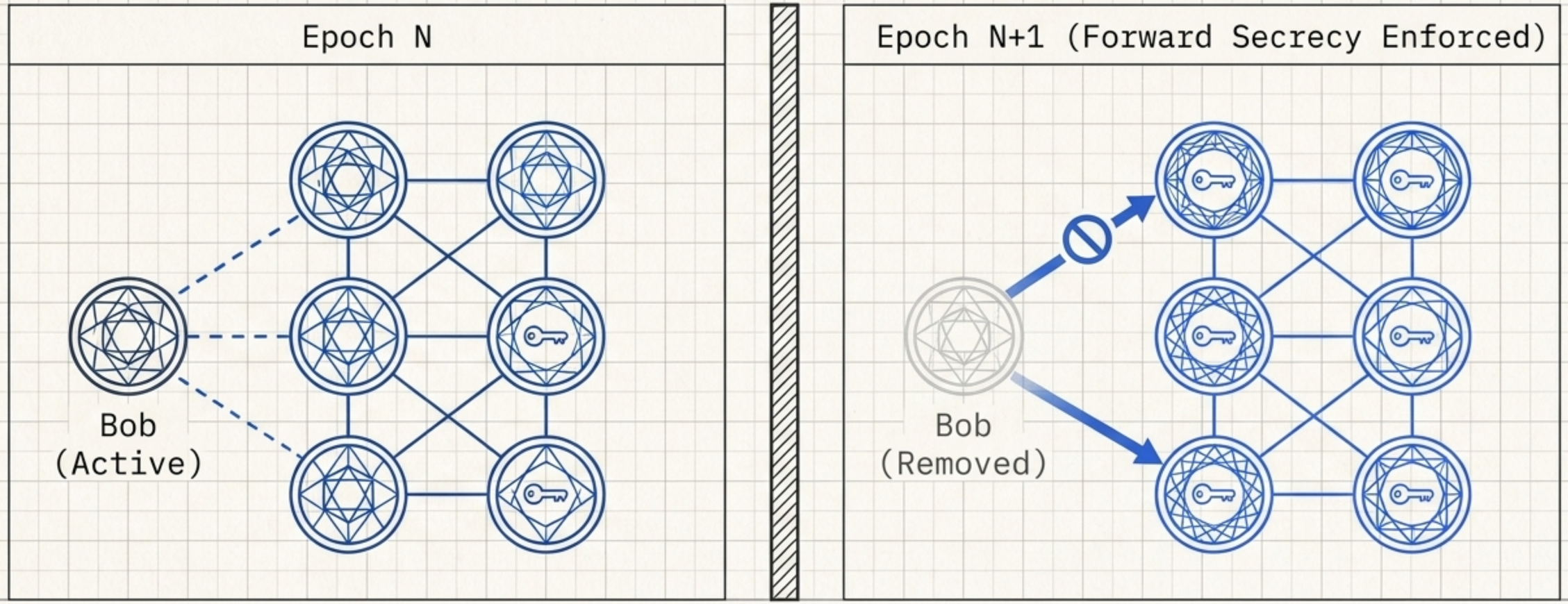
Efficient Scaling via Logarithmic Rotation

When a participant rotates their KERI **identity key**, they sign a new MLS **encryption key**. This update affects **only a logarithmic** portion of the MLS tree, making **continuous key rotation highly scalable** for massive groups.



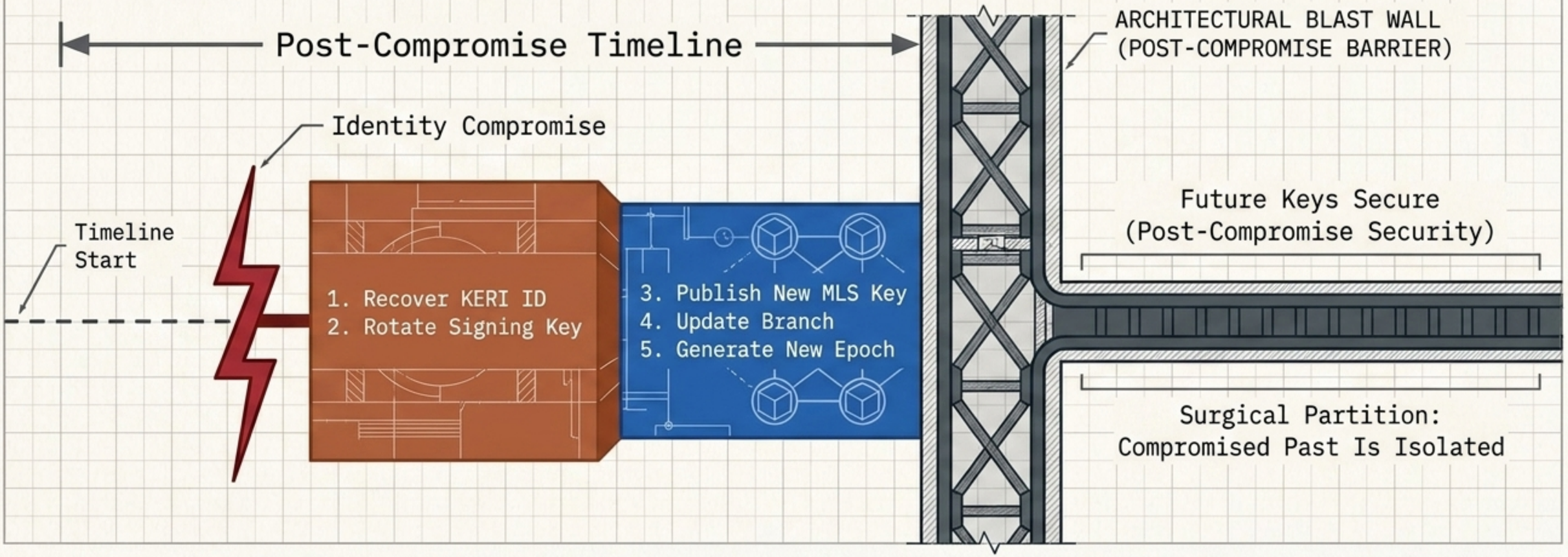
Member Removal & Forward Secrecy

When a participant leaves or is removed, MLS immediately generates a new epoch. The departed member cannot derive future keys, ensuring old messages remain protected and forward secrecy is preserved.



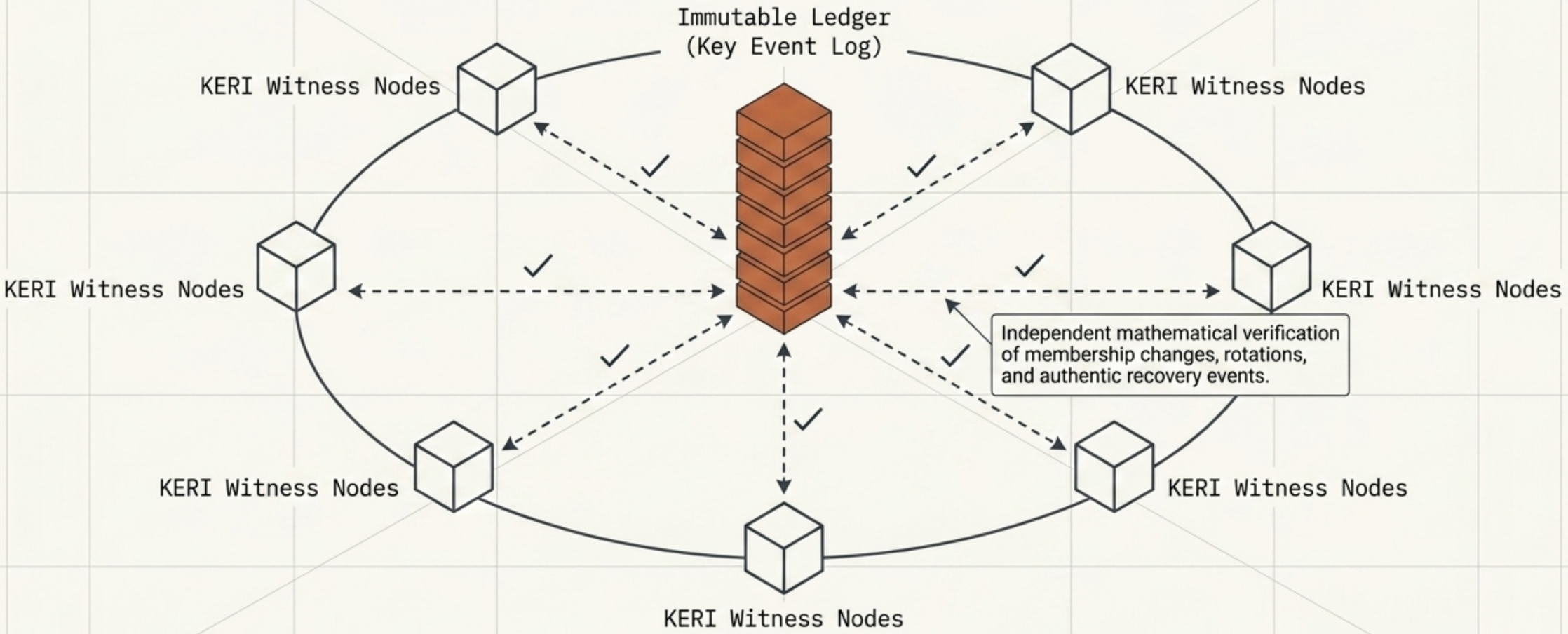
Identity Recovery & Post-Compromise Security

A compromised identity does not doom the group. Because KERI manages identity independently, a recovery event securely partitions the compromised past from the secure future without requiring global certificate revocation.



Verifiability Without Blind Trust

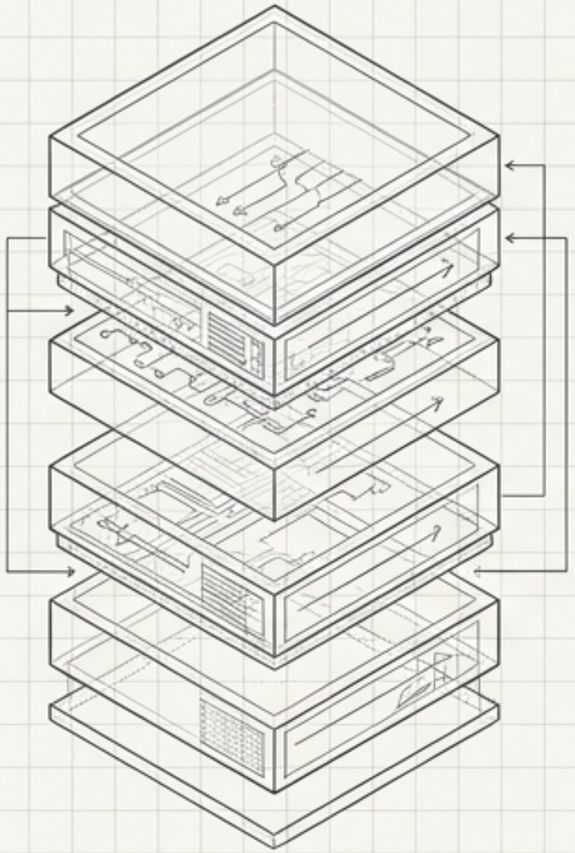
The system does not rely on blind trust. KERI witnesses provide independent, mathematical verification of the ledger's integrity. Identity changes are permanently recorded and auditable within KERI Key Event Logs.



Cryptographic Agility & Implementation

Designed for immediate deployment and modular upgrades. Algorithms can be upgraded independently at either the identity or encryption layer without breaking the structural binding.

Implementation Stack

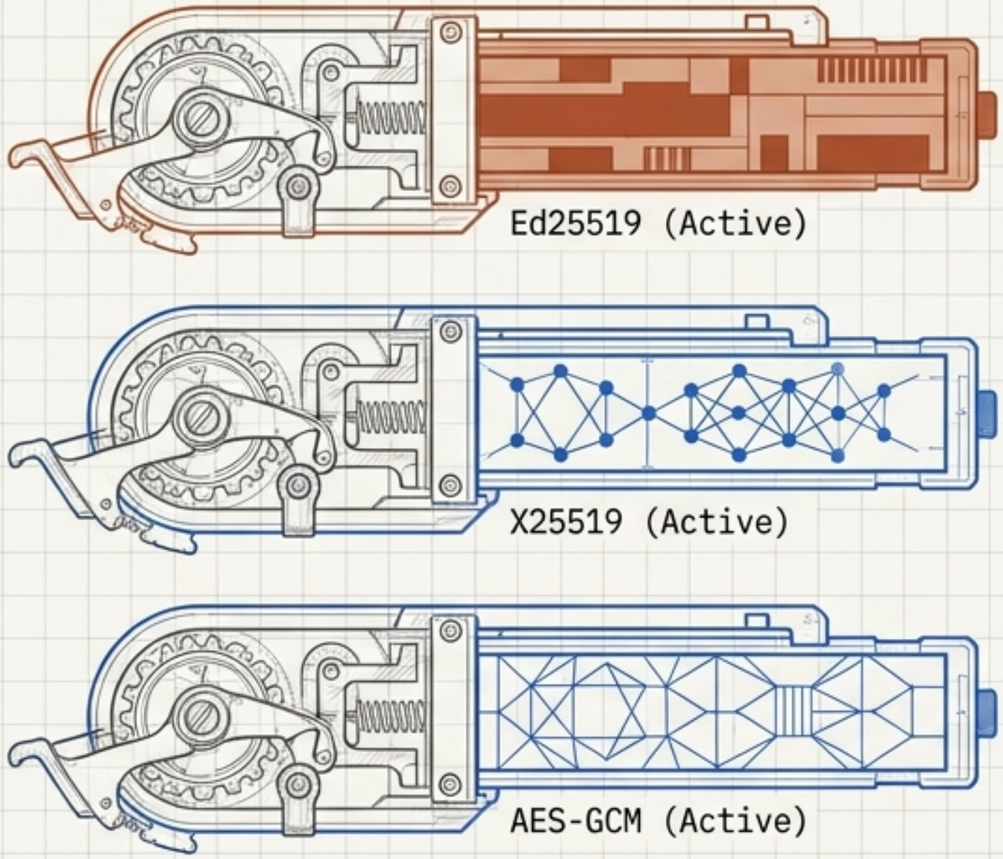


Node.js Reference Implementation

Relies entirely on native crypto module.

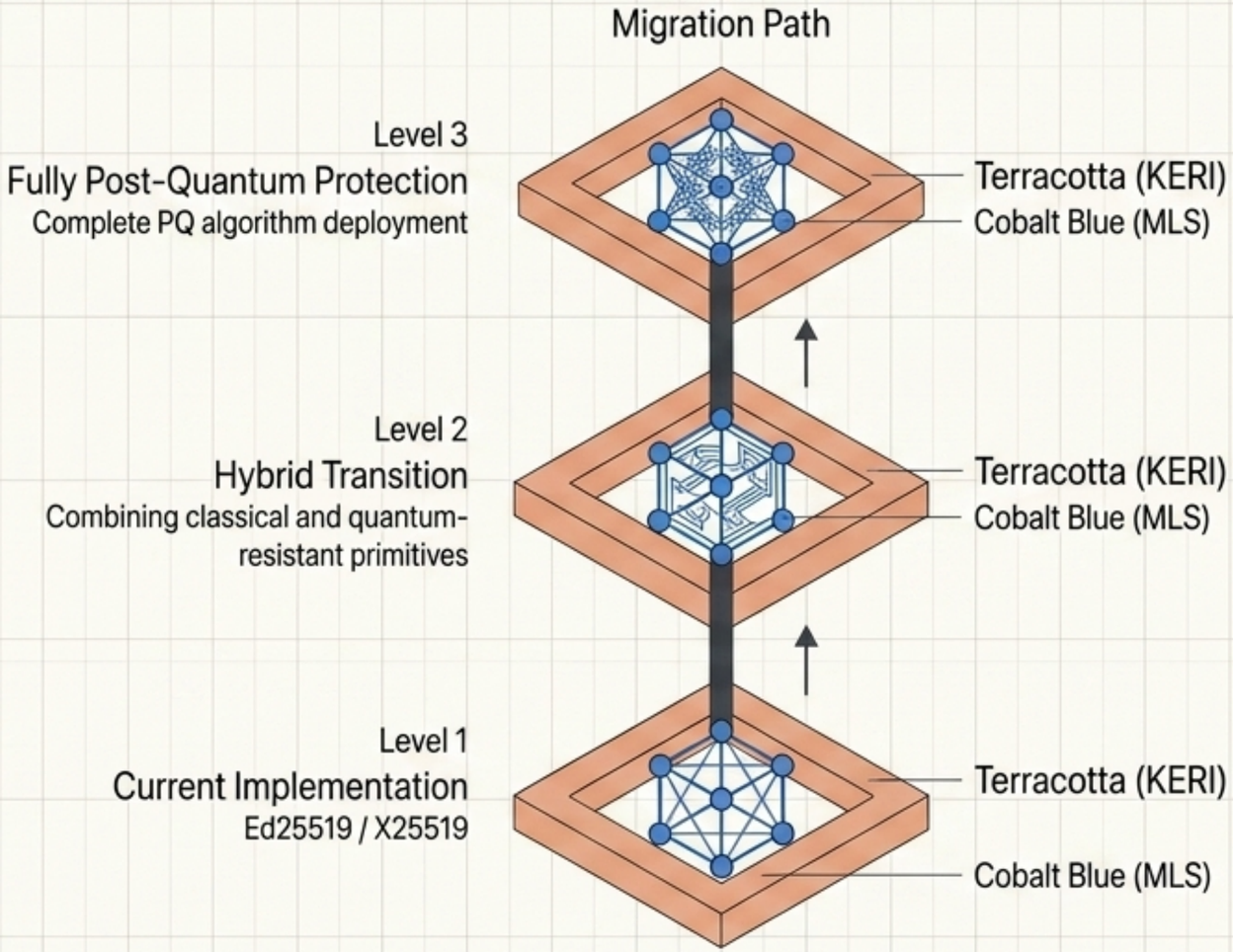
No external cryptographic dependencies required for prototype.

Modular Agility Matrix



The Post-Quantum Horizon

As quantum computing threats emerge, the architecture provides a seamless migration path. The system transitions to hybrid or fully post-quantum algorithms without altering the foundational binding.



Convergence to Autonomy: Beyond Human Messaging

KERI + MLS is the universal collaboration protocol for Autonomous Organisations.
AI agents, IoT devices, and human users securely collaborate as first-class,
verifiable identities within an entityOS ecosystem.