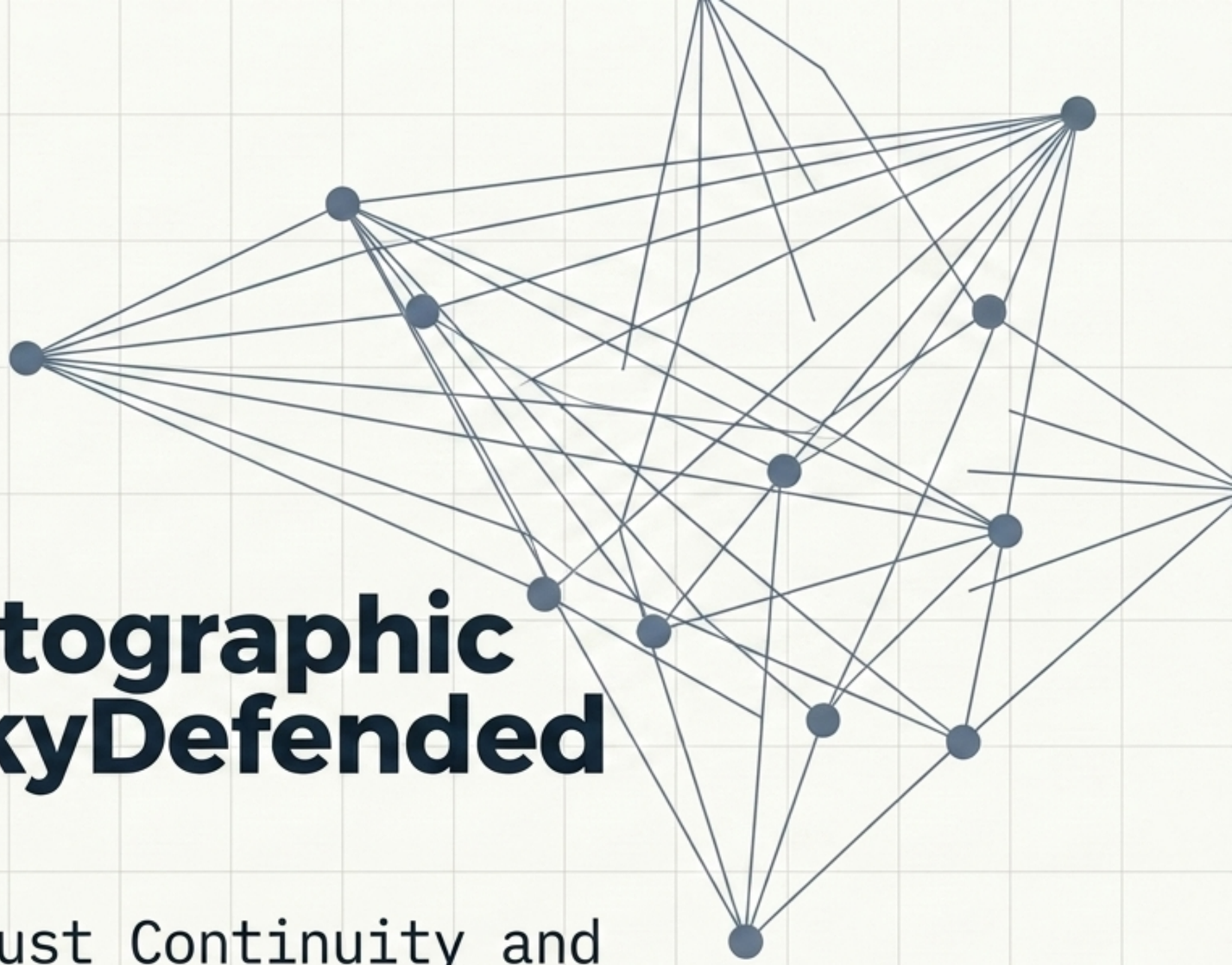
NEXOCYBER NETWORKS

NCN



Distributed Cryptographic Governance in SkyDefended InfraApp (D04)

Lifecycle Architecture, Trust Continuity and Minimum Exposure on Ephemeral Infrastructure

STATUS: V1.2 CORE GOVERNANCE

TONE: ZERO TRUST ARCHITECTURE

AUTHORITY: ISMAEL CRUZ CASASOLA

What this system is NOT

- The goal is NOT to store secrets.
- We do NOT rely on environment variables.
- We do NOT use static hardcoded secrets.
- We do NOT issue permanent infrastructure tokens.
- We do NOT base trust purely on the runtime.

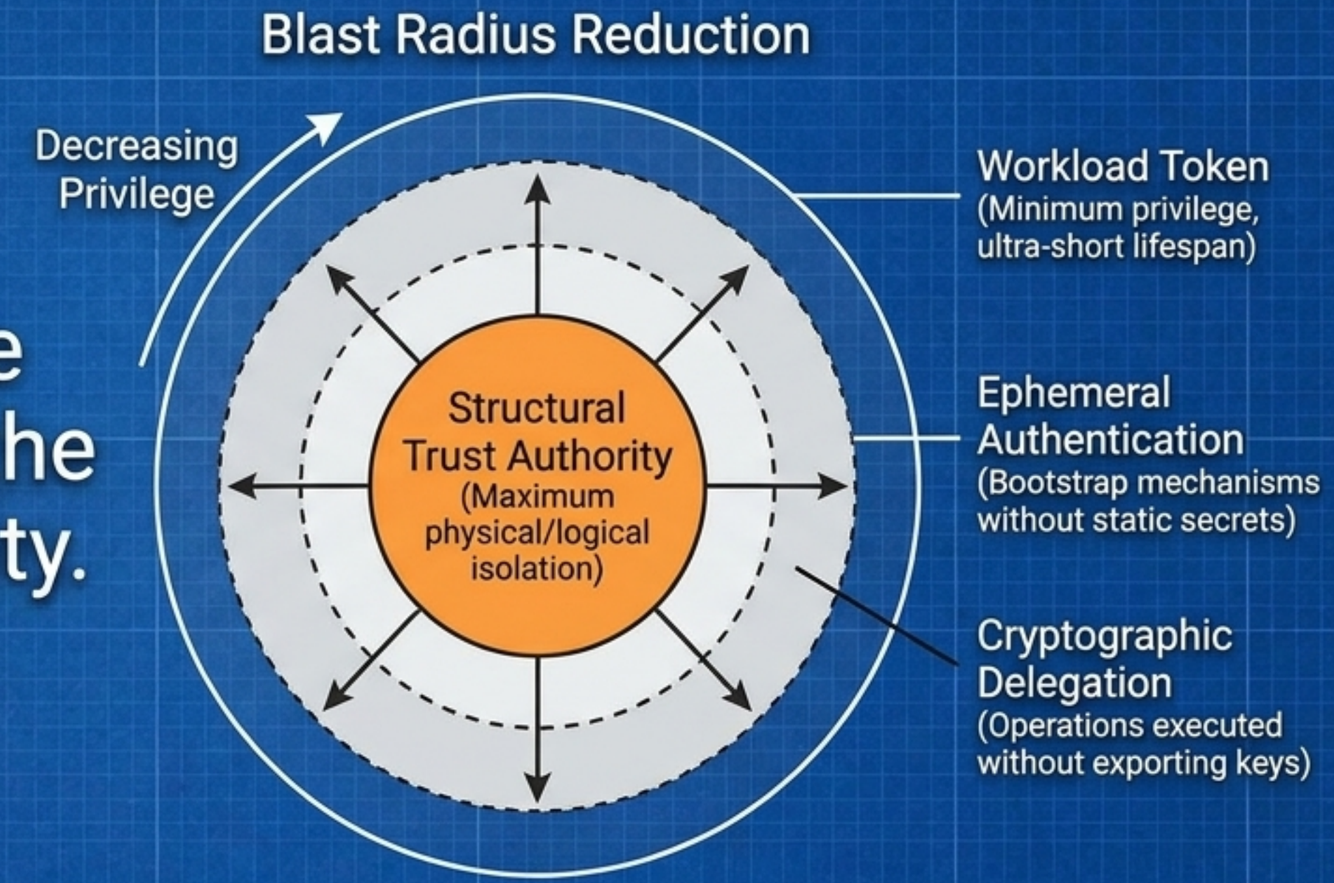
Runtime ≠ Identity.
The workload is ephemeral; the identity possesses continuity.
Custody ≠ Trust.

What D04 really GOVERNS

- The goal is to preserve trust continuity under an ephemeral runtime and partial compromise.
- The cryptographic authority requires explicit governance.

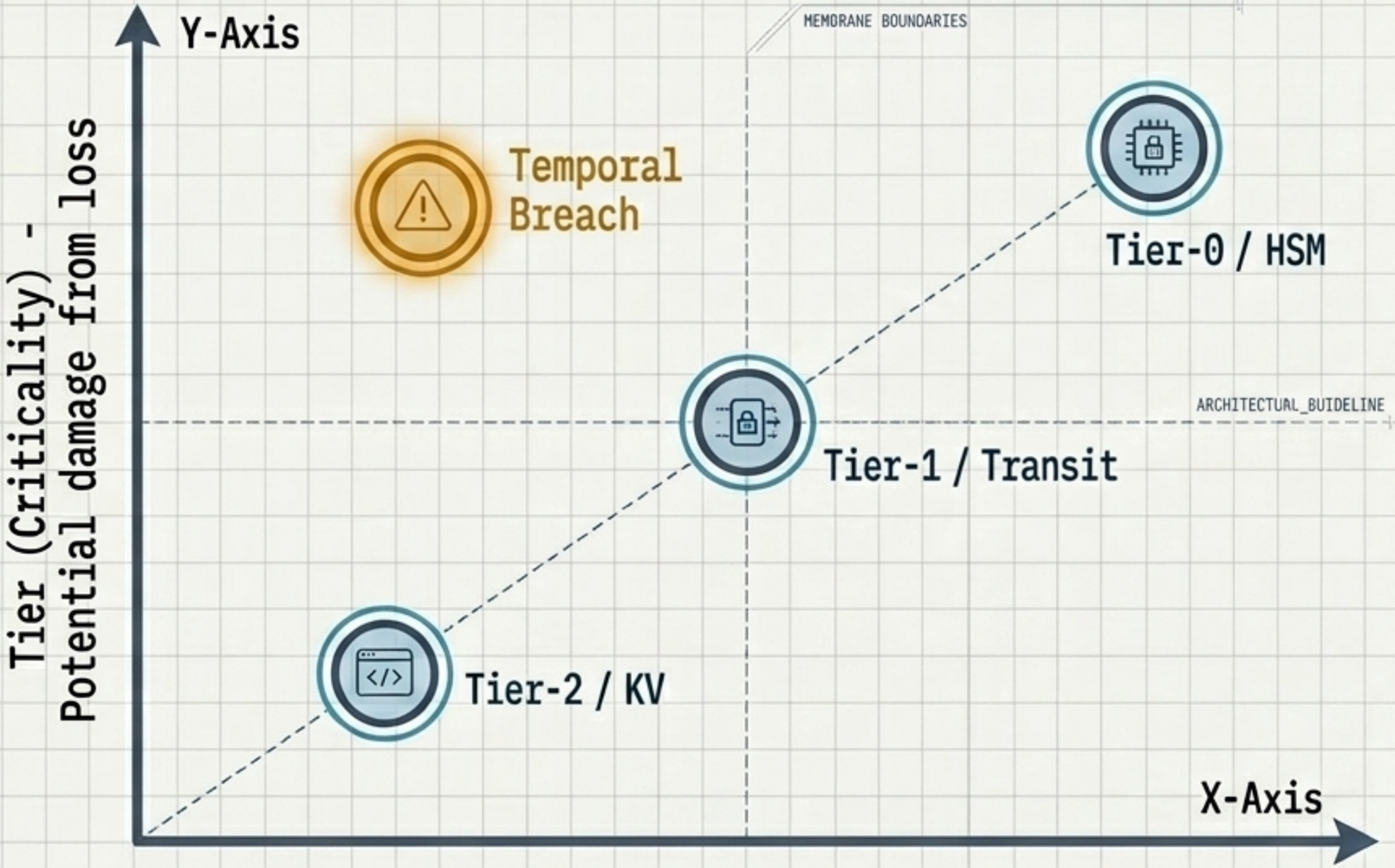
The Principle of Minimum Exposure

The architecture progressively reduces the operational exposure of the cryptographic ɑic authority.



Success Metric: Elimination of private keys in runtime	Zero permanent tokens	Guaranteed compromise containment

Orthogonal Topology: Tier ≠ Level



Temporal assignment can be misaligned (Tier ↔ Level Breach).

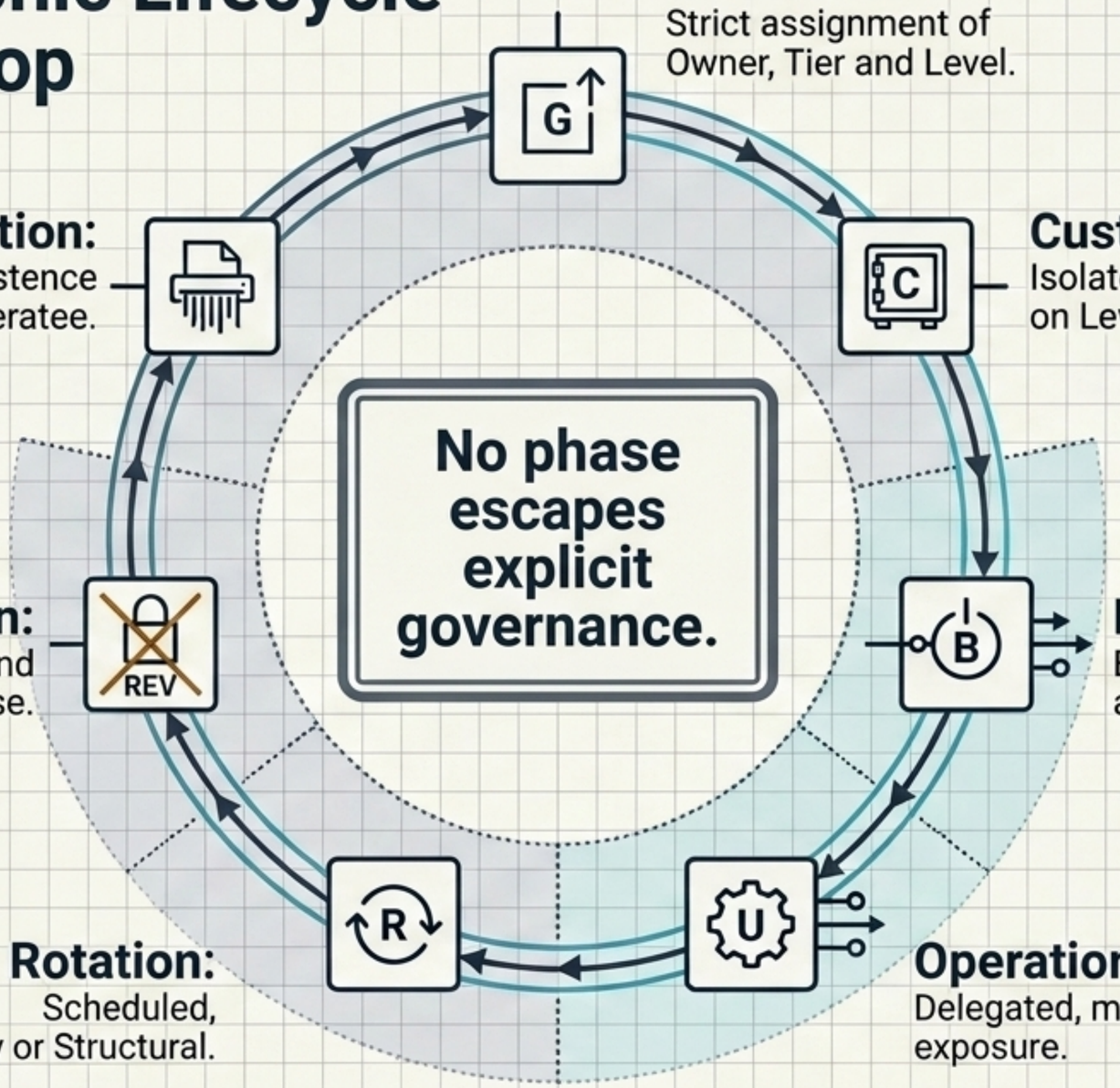
The architecture supports and audits this temporal coexistence while prioritizing migration to the target Level.

Dissection of Cryptographic Criticality

Tier-0 (Trust Root)	Tier-1 (Operational Critical)	Tier-2 (Operational Standard)

Definición:
Its compromise breaks the root trust of the system.
 	
Policy/Level:
HSM / Remote-sign. 100% non-exportable. Mandatory audit and evidence.
 	
Examplos:
`SESSION_SIGNING_KEY`
`NCN_LICENSE_PRIVATE_KEY`
	Definición:
	Critical but recoverable through rotation. Contained blast radius.
	
	Policy/Level:
	Transit. Non-exportable when feasible.
	
	Exemplos:
	`INTERNAL_API_KEY`
	`STATE_SIGNING_KEY`
		Definición:
		Operational secrets that are not part of the structural trust authority.
		Policy/Level:
		KV. Automatable rotation.
		
		Exemplos:
		`DB credentials`
		`tokens SIEM`

The Cryptographic Lifecycle as a Control Loop



Generation:
Strict assignment of Owner, Tier and Level.

Custody:
Isolated storage based on Level.

Bootstrap:
Ephemeral workload authentication.

Operational Use:
Delegated, minimizing exposure.

Rotation:
Scheduled, Emergency or Structural.

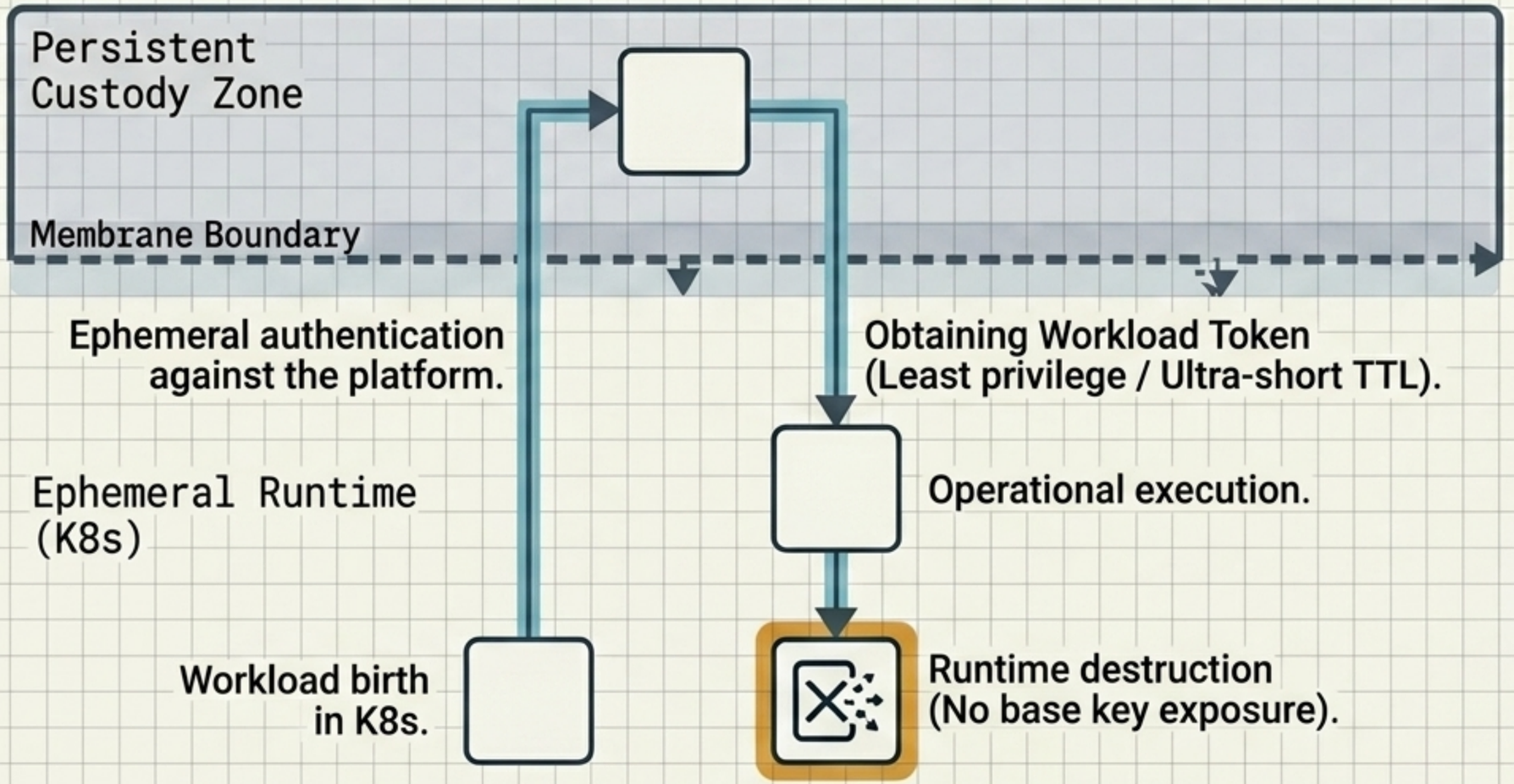
Revocation:
Trust blockage diamage and prevention of reuse.

Destruction:
Actual elimination of persistence and generated generatee.

SCALE

Ephemeral Cryptographic Bootstrap

Secure transition from a Persistent Identity to an ephemeral Workload Authorization.

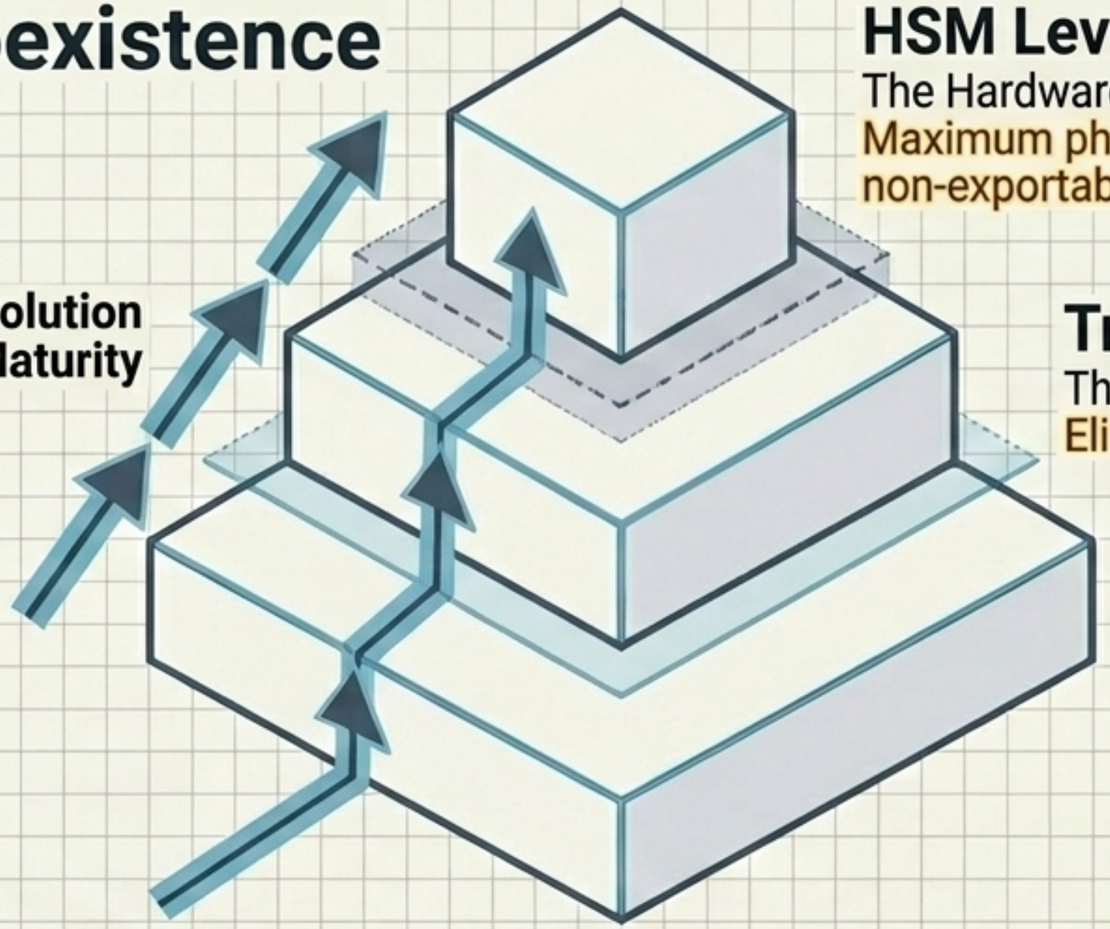


Architecture Mandates:

- Strictly ephemeral authentication.
- Zero hardcoding of secrets.
- Controlled recovery.

SCALE

Operational Boundaries: Evolution & Coexistence



HSM Level:

The Hardware Boundary.
Maximum physical isolation, non-exportable.

Transit Level:

The Operational Boundary.
Elimination of private keys in runtime.

KV Level:

Distributed storage, minimal latency, local operations.

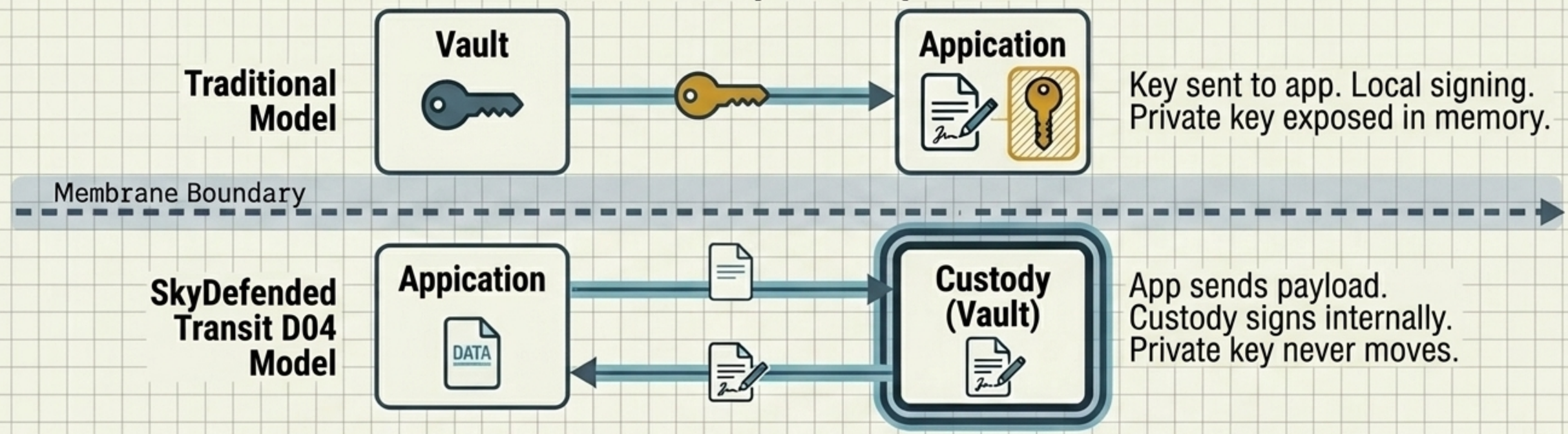
Coexistence Principle: SkyDefended InfraApp does NOT seek 'all in HSM'. Mature architecture uses all three levels simultaneously because not all operations tolerate the same latency or operational dependency.

SCALE

Deep-Dive: Transit as an Operational Frontier

Transit represents the progressive elimination of private keys within the runtime.

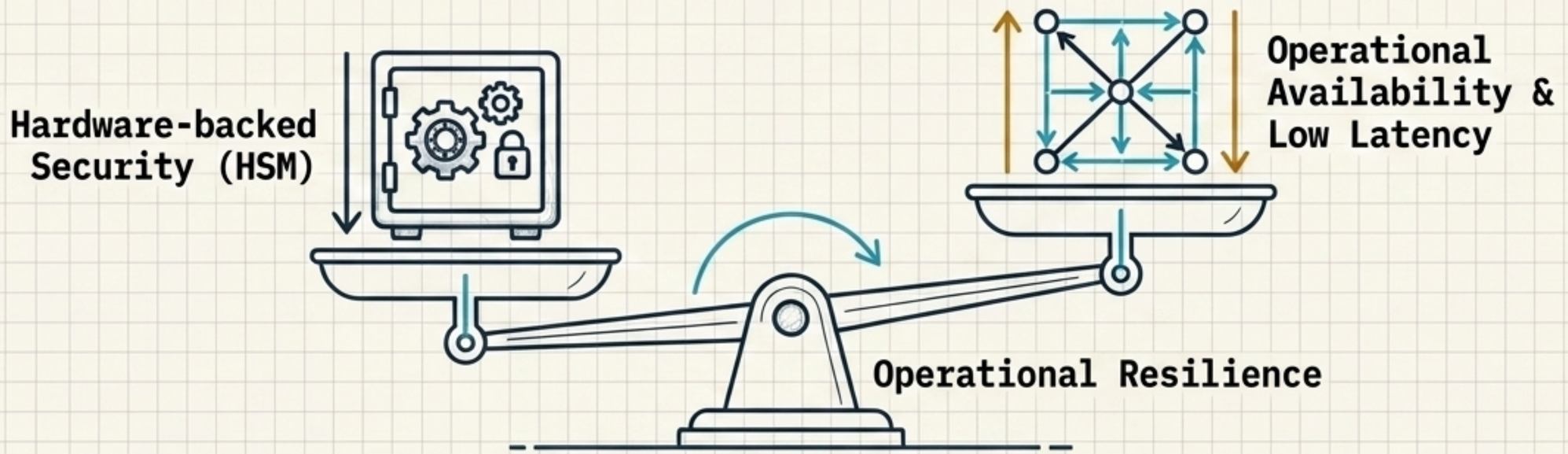
Remote Hot-path Comparison



Definitive Axiom: The private key NEVER leaves the logical vault of the custody system. The workload delegates signing, encryption, and sensitive operations.

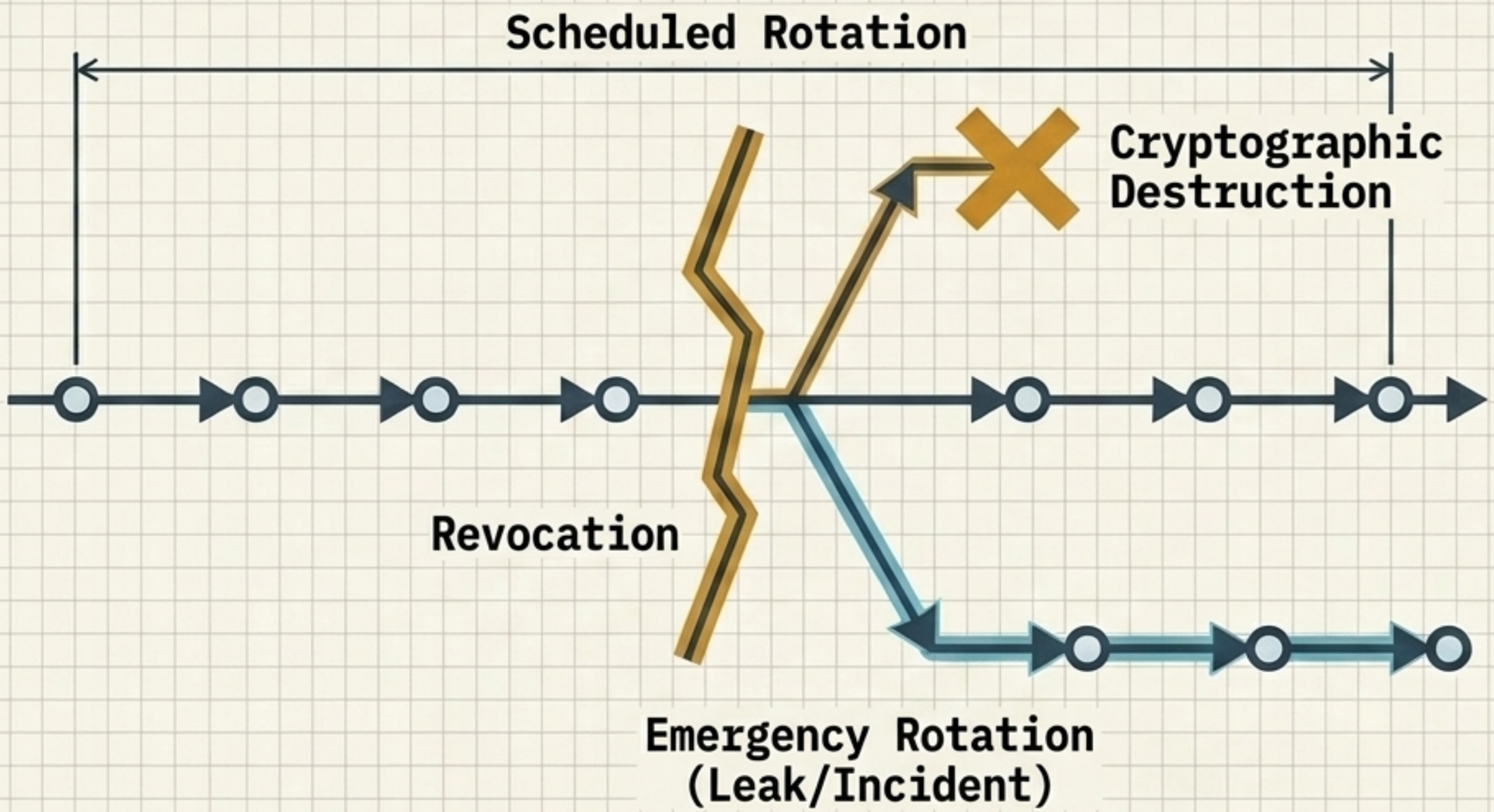
SCALE

The Architectural Paradox: Resilience vs. Maximum Protection



The Conflict	Design Decision
Isolated theoretical maximum security often means operational failure. Custody MUST NOT break the operational continuity of the infrastructure.	- Mitigate operational dependency on the custody system. - Critical for bootstrap, rotation, and recovery. - MUST NOT be a mandatory continuous dependency for distributed validation. - Tier ↔ Level assignment is a resilience decision.

Continuity Engines: Rotation and Revocation



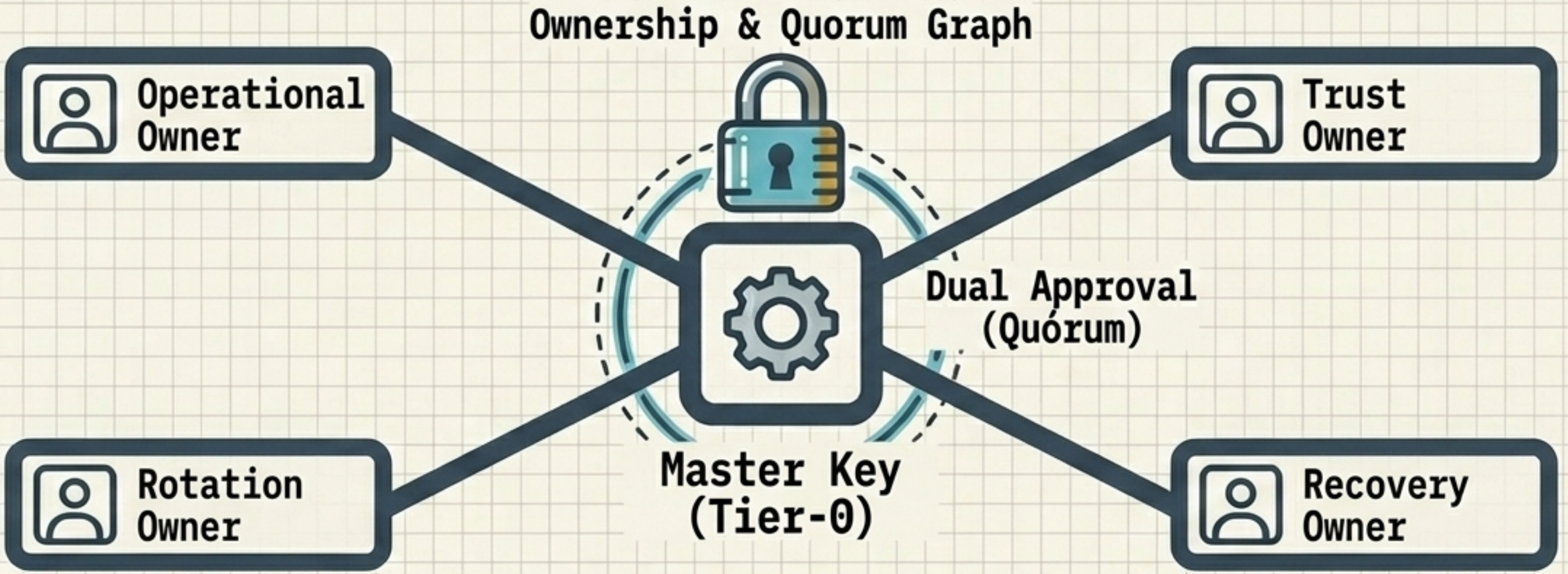
Rotation Types:

1. **Scheduled:** Periodic hygiene to reduce exposure.
2. **Emergency:** Triggered upon suspicion of compromise.
3. **Structural:** Tier/Level Migration.

Destruction Rule:

Cutting the trust continuity requires actual elimination of persistence to prevent reuse, leaving auditable evidence.

Human Governance: Cryptographic Ownership and Quorum



Anchor Axiom	Tier-0 Operational Quorum
A key without an owner is an ungoverned key.	- Mandatory Dual Approval for critical operations. - Strict separation of duties. - Multi-owner control with explicit evidence generated.

Evidence, Audit, and Cryptographic KPIs

Mandatory Evidence: Immutable traceability for all generation, rotation, revocation, destruction, or Tier/Level migration.

0

Detected Breaches: Tier-0 outside HSM / Tier-1 outside Transit.

0

Orphanhood: Count of keys without assigned Owner.

Hygiene: Expired or out-of-target-Tier keys rotated.

Operational Health: Failed rotations and Bootstrap failures at zero.

Deployed Stack: SkyDefended InfraApp v1.2

Orchestration (Ephemeral Runtime)

- Kubernetes Talos
- Dedicated physical cluster OVH

Cryptographic Custody

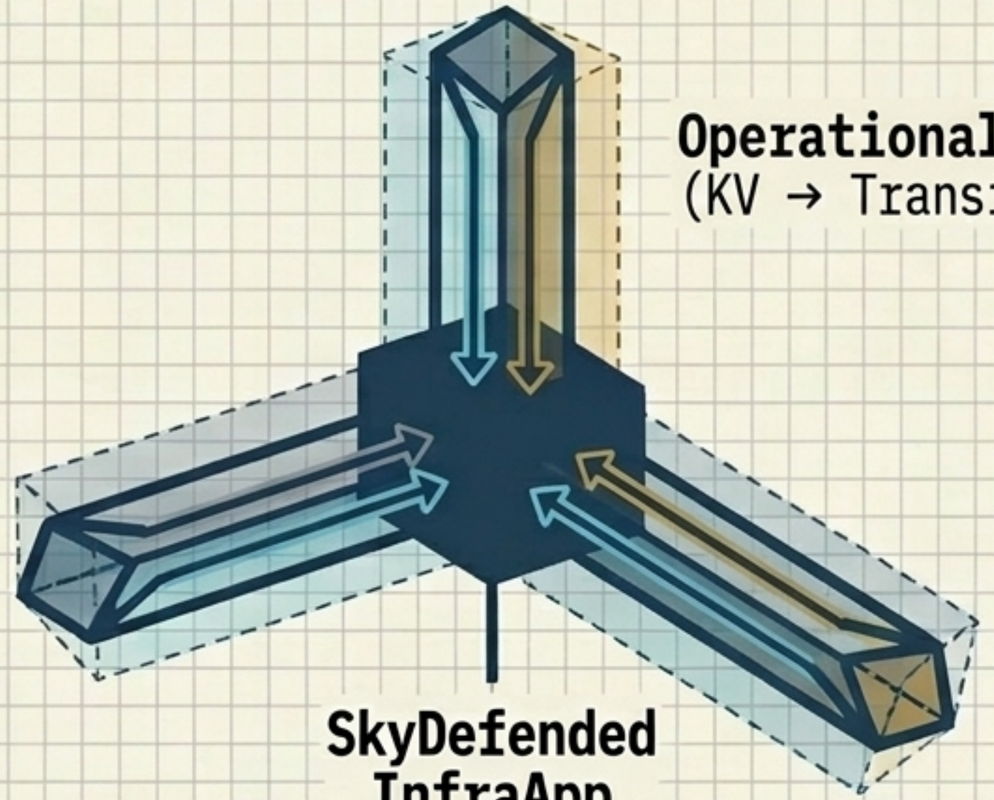
- HashiCorp Vault Raft (isolated external VM)
- Kubernetes Auth v2.0

Workload Integrity

- Cosign keyless & Sigstore
- Kyverno verify-image-signatures (Digest pinning)

Current State:
KV level generalized, partial Transit, HSM projected.

Conclusion: The Architecture of Continuity



Operational Resilience
(KV → Transit → HSM)

Trust Continuity
(Persistent identity)

SkyDefended InfraApp

Doep Governance
(Blast radius reduction)

The platform does not pursue maximum isolated theoretical protetion. It pursues the perfect architectural balance between tween trust continuity, operational resilitence, and distributed cryptographic governance.