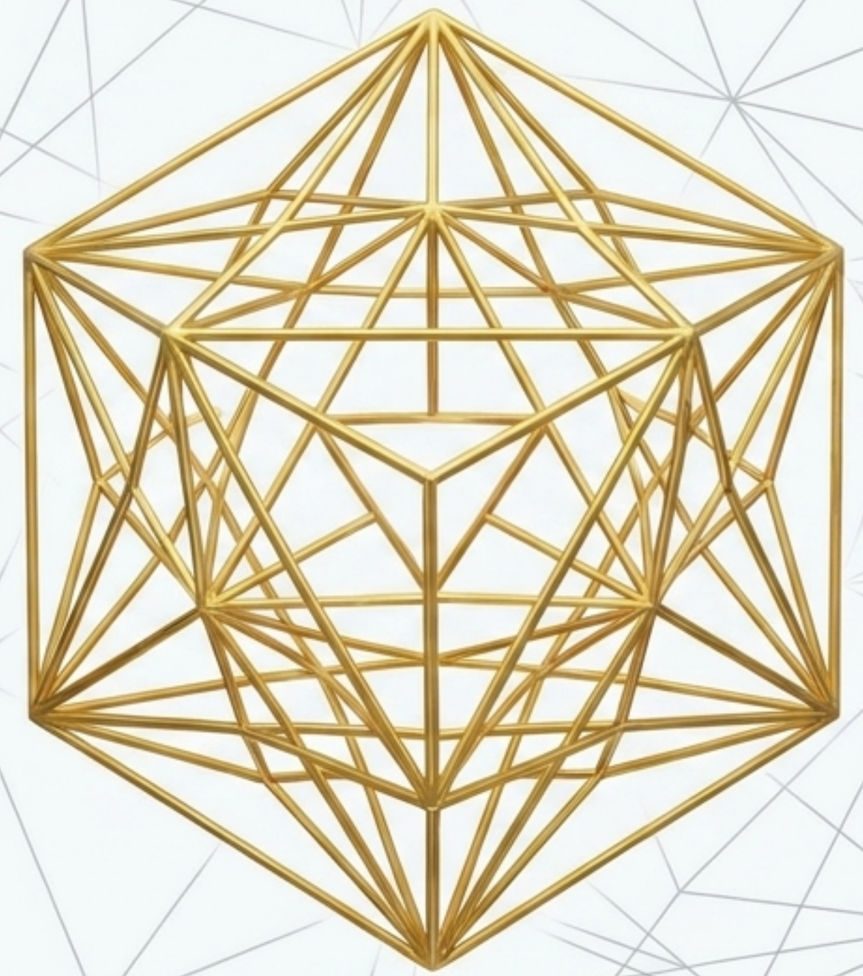
NEXOCYBER NETWORKS
ncn
NETWORKING, SEGURIDAD Y SISTEMAS

ADVANCED ZERO TRUST ARCHITECTURE

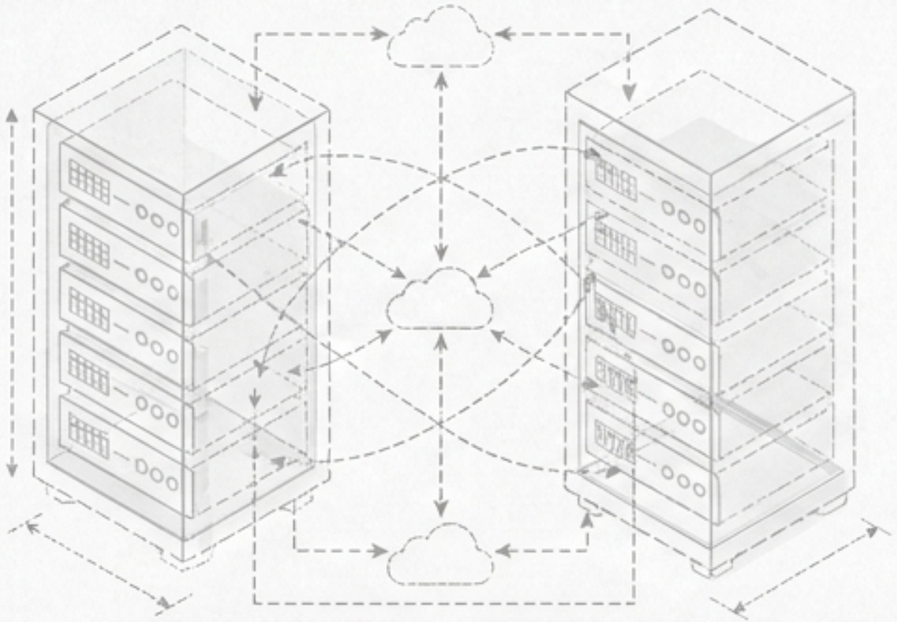
DISTRIBUTED CRYPTOGRAPHIC TRUST MODEL

SkyDefended InfraApp v1.2:
Establishment, autonomous validation, and trust continuity in ephemeral runtimes.



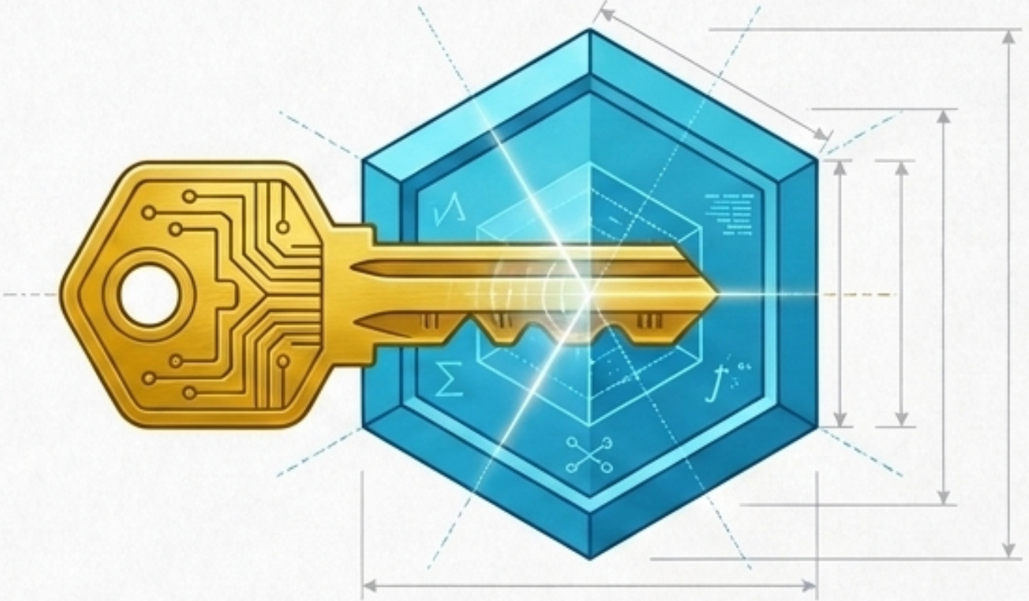
Structural trust is not inferred; it is demonstrated mathematically

The Where and The How



Topological Transport (Ephemeral)

The With Whom



Mathematical Identity (Immutable)

Explicit and Prior
Established before the first functional byte.

Cryptographic
Based on persistent identities, not topology.

Mediated
Defined exclusively by the Control Plane.

Local
Validated mathematically at the receiving node.

Decoupling Ephemeral Transport from Immutable Authority

Transport and Exposure

DO NOT constitute trust

- ✗ IP Addresses and Private Networks
- ✗ Proxies and Web Frontends
- ✗ Execution Environments and Physical Instances
- ✗ HTTP Sessions

Participate in operational connectivity, never in cryptographic authority.

Cryptographic Authority

DO constitute trust

- ✓ Isolated RSA Keys (2048+ bits)
- ✓ JWKS Distribution and RS256 Signatures
- ✓ Cryptographic Identifiers (kid)
- ✓ JWT Tokens for Operational Identity

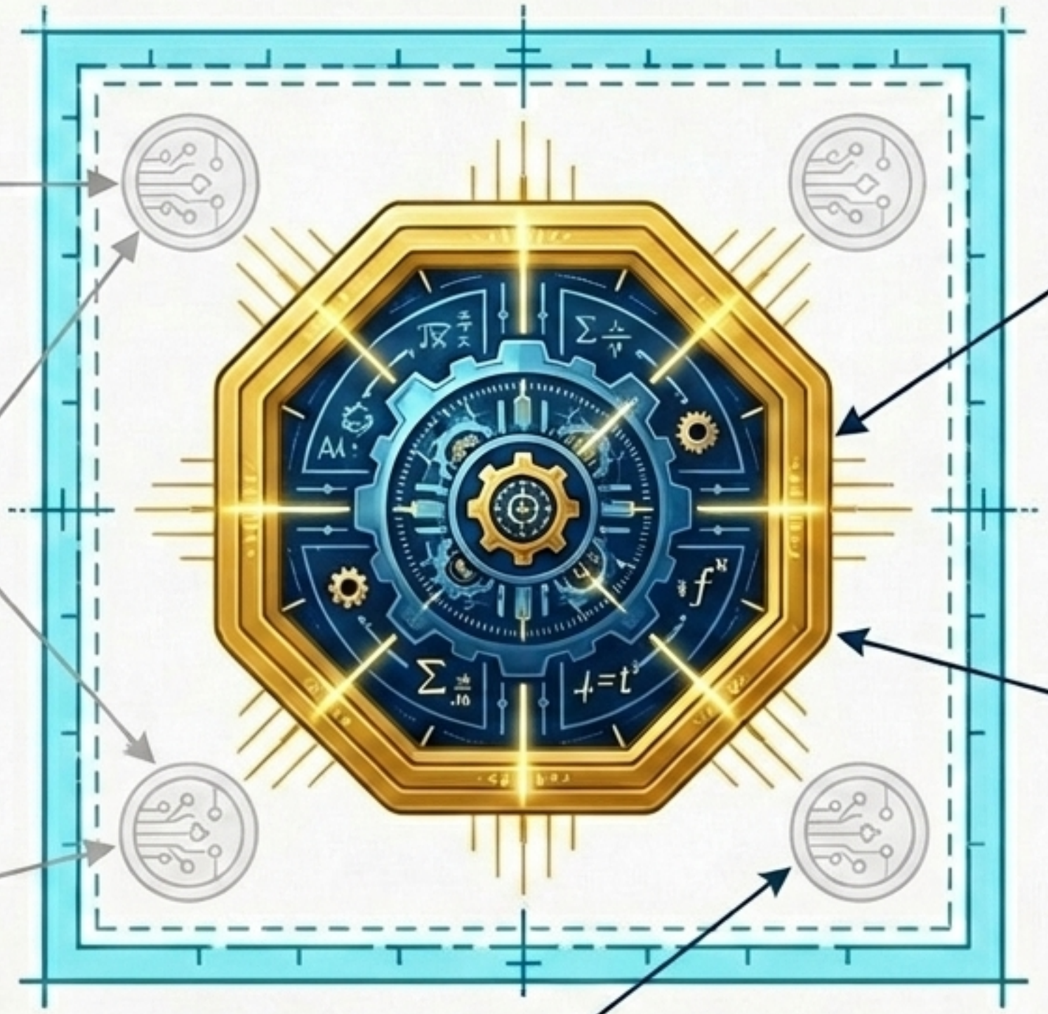
Immutable, auditable, and mathematically verifiable elements.

Capsules scale operation; Engines custody trust

Frontends
(Operational Periphery)

Intrinsic structural relationship by deployment. DO NOT sign, DO NOT validate, DO NOT hold cryptographic authority.

Functional Persistence



Sole entity with **cryptographic identity** (Private Key, Public Key, kid).

Private keys NEVER leave this perimeter.

The Engine
(Authoritative Core)

Strict separation of business data from cryptographic persistence.

Architectural Singularity vs. Operational Scalability

Level 1: Control Plane (The Cryptographic Arbiter)

Singularity: Single main capsule (Root of Trust).

Function: Defines identities, builds relationships, distributes signed artifacts. Never consumes business operations.

Level 2: Access Plane (Operational Identity)

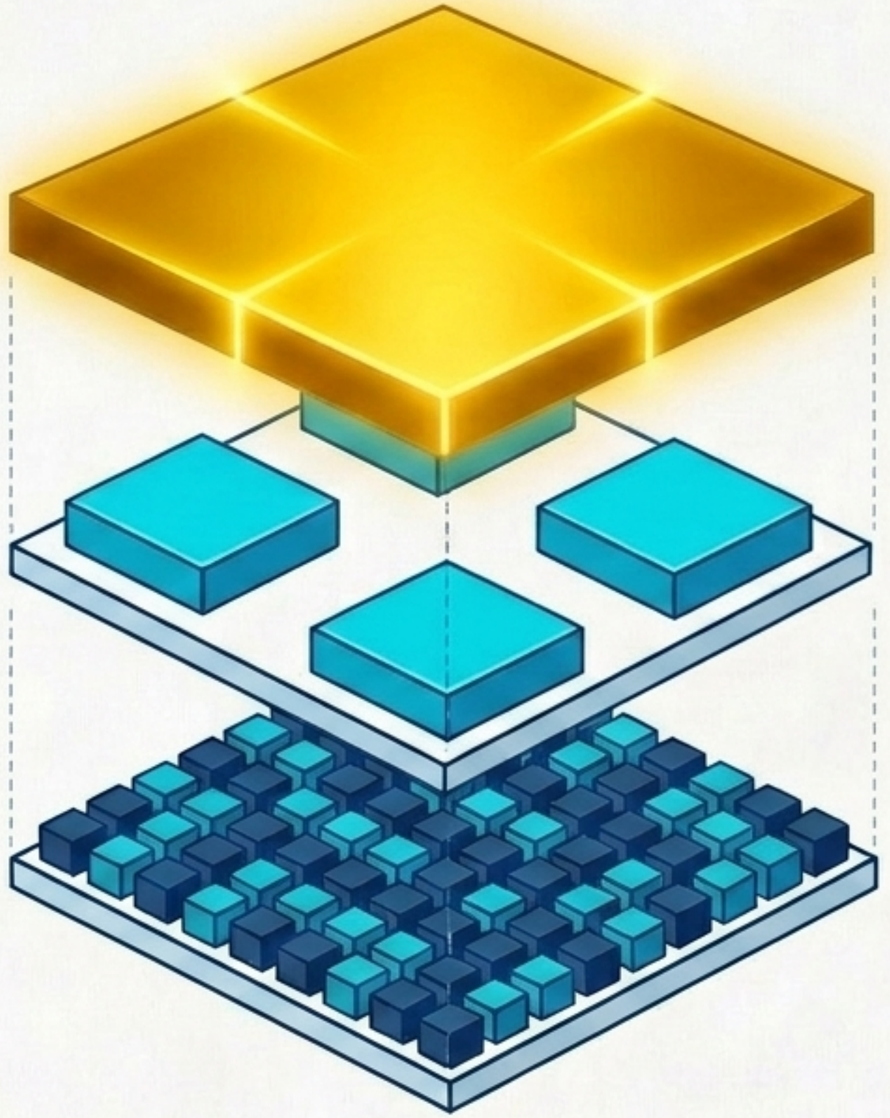
Scalability: Engines distributed by region or tenant.

Function: Generates operational identities based on Control policies.

Level 3: Application Plane (Business Logic)

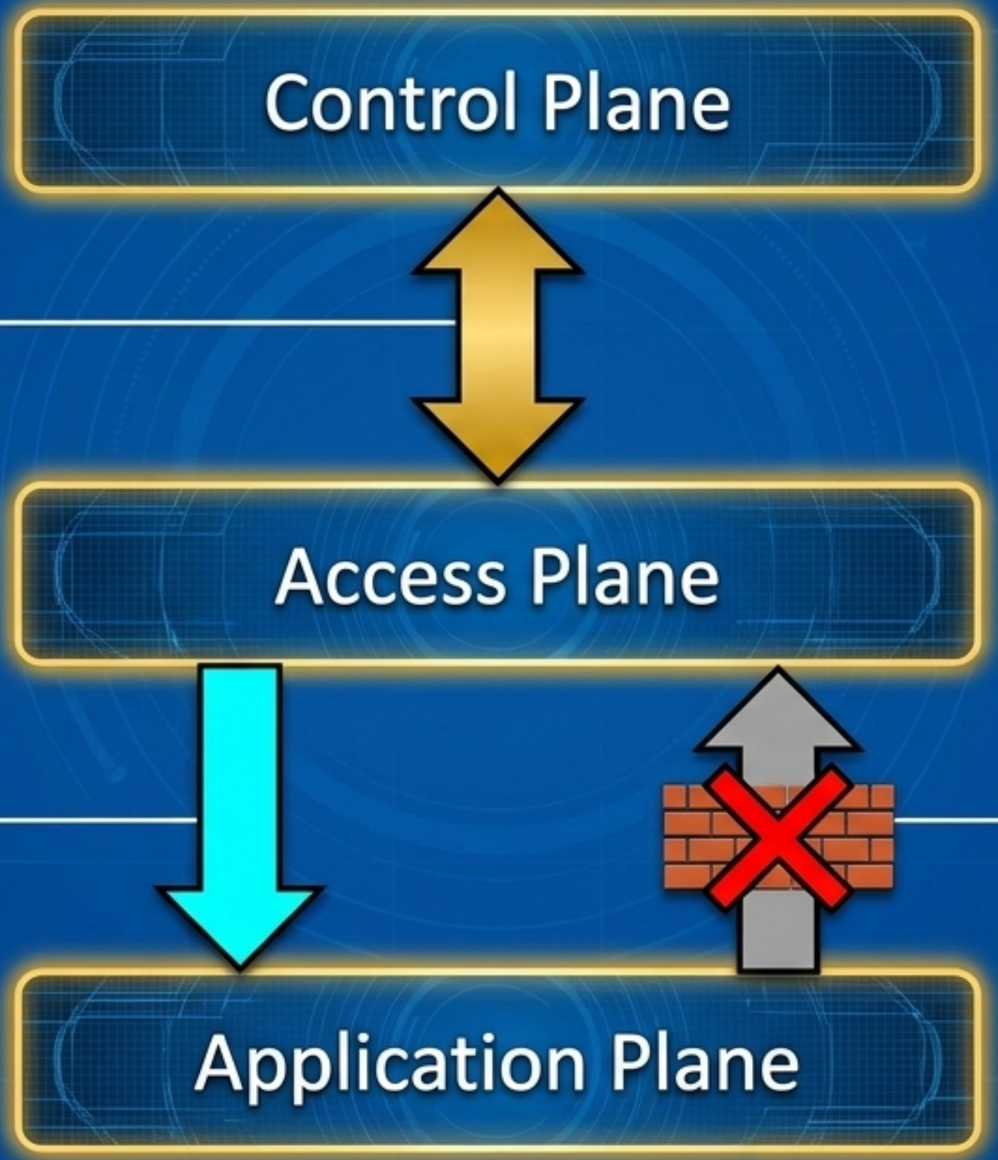
Scalability: Thousands of functional capsules.

Function: Validates input signatures and executes isolated business processes.



Asymmetric Distribution Based on Cryptographic Least Privilege

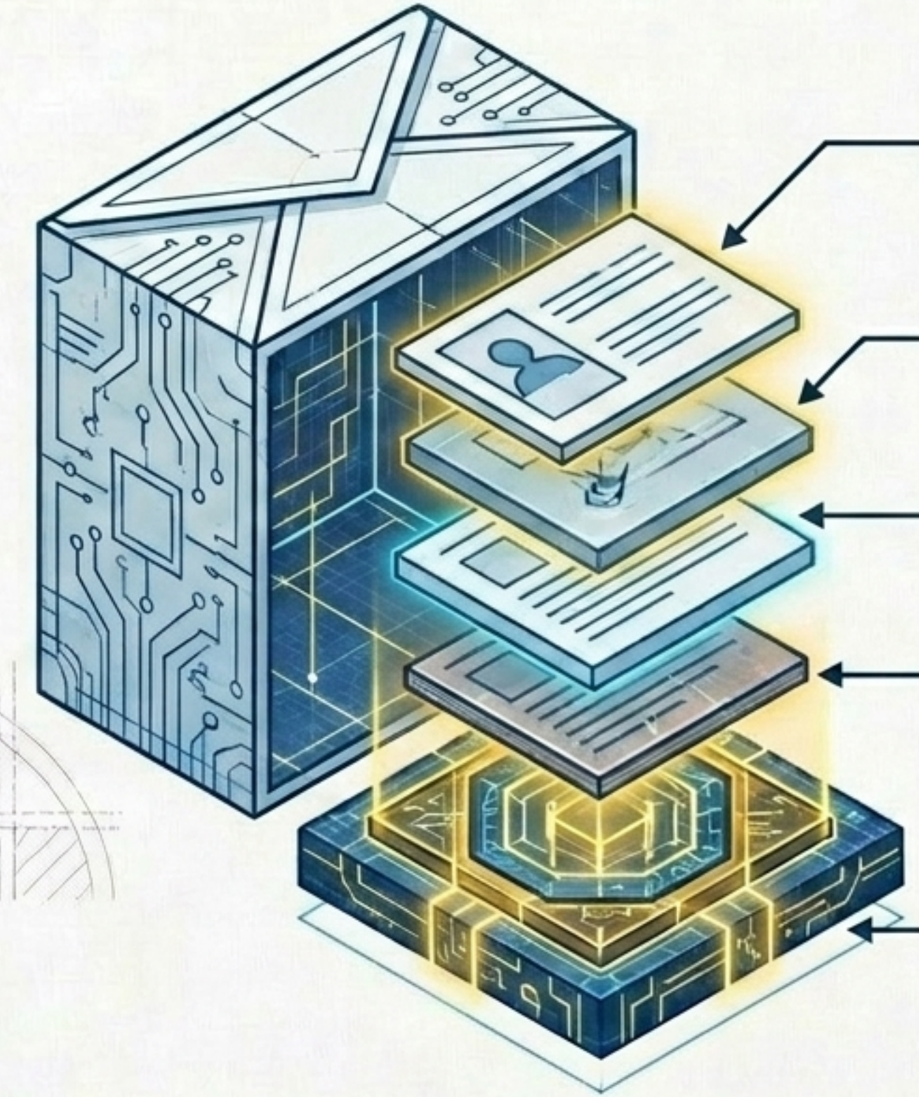
Bidirectional Distribution:
Control distributes keys and metadata. Engines register identity and demonstrate belonging.



Identity Issuance:
Access issues operational identity (JWT). Application validates and consumes.

Golden Rule:
The application does NOT issue identity to access. Strict least privilege.

Distribution Mechanics: Packaging the Cryptographic Context



Authorized Identities

JWKS (Public Keys)

Contextual Restrictions

Explicit Revocation Artifacts

Digital Signature RS256

Acceptance Flow

1. Reception

Engine receives Policy Bundle.

2. Origin Validation

Receiver verifies RS256 signature using the known Control Plane public key. No unsigned bundle is processed.

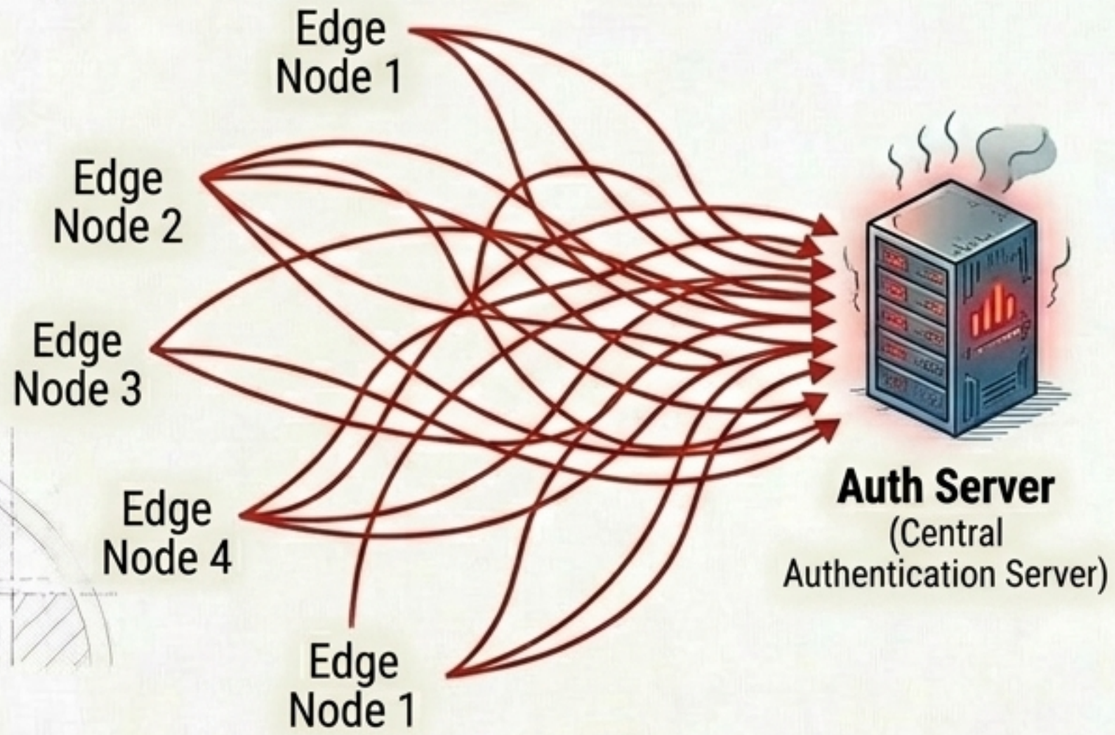
3. Local Application

The distributed policies are applied. No implicit horizontal trust exists.

Autonomous In-Memory Validation: Decoupling Runtime from Control

Centralized Model

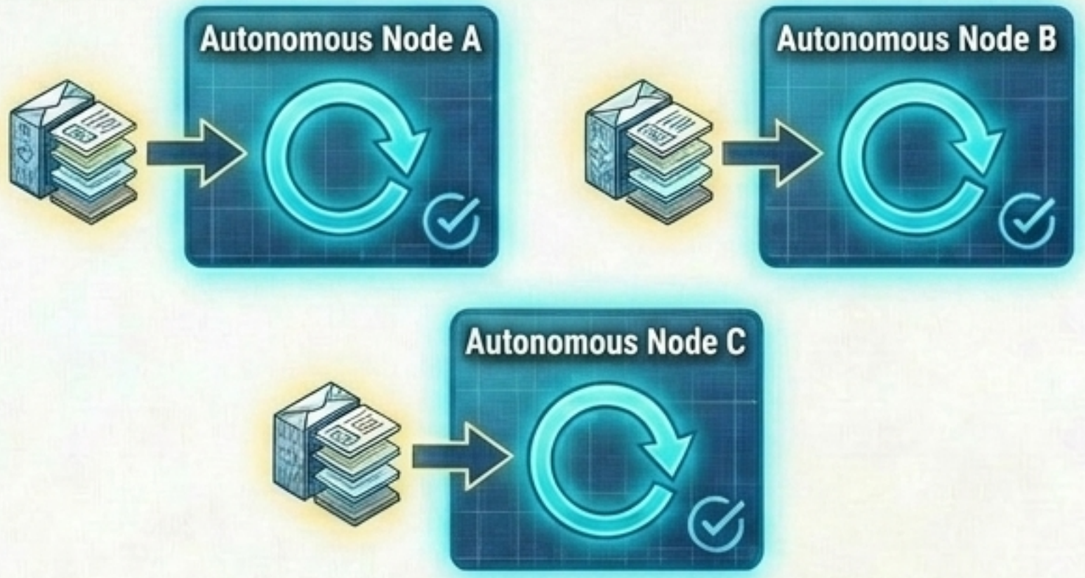
Latency + Fragility



- Every interaction requires a synchronous query.
- If the Control Plane fails, the platform is paralyzed.

SkyDefended Model

Operational Resilience



1. Issuer signs the payload locally with its private key.
2. Receiver validates the RS256 signature in-memory using preloaded JWKS.
3. Functional runtime continues without interruption even if the Control Plane is temporarily unreachable.

Cryptographic Continuity: Identity survives the infrastructure

The Problem:
Containers die and networks change.

Ephemeral Runtime Lifecycle

Container Destroyed

IP Modified

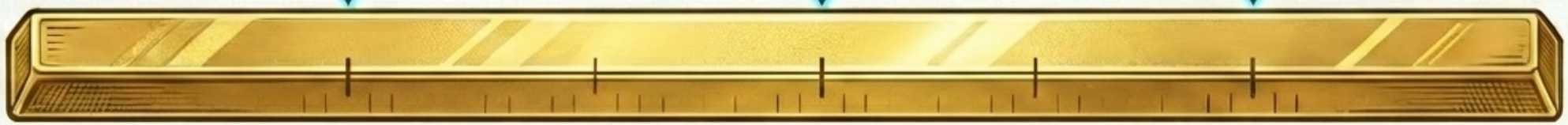
Node Restarted

Challenge-Response Authentication
(Runtime re-association)

Challenge-Response Authentication
(Runtime re-association)

Challenge-Response Authentication
(Runtime re-association)

Cryptographic Identity - RSA Keypair



Multi-kid Rotation

Multi-kid Rotation

The Solution:
Isolated mathematical identity, with continuous rotation without traffic interruption.

Evolution of cryptographic custody by progressive isolation

1 Level 1: Operational Custody

Keys temporarily loaded into runtime memory (Vault KV). Decoupled from disk.

2 Level 2: Non-Exportable Custody

The private key never touches the Engine. Payload is sent and signed result is received (Vault Transit).

3 Level 3: Hardware-Backed

Keys sealed in cryptographic hardware. Remote direct signing operations (HSM).

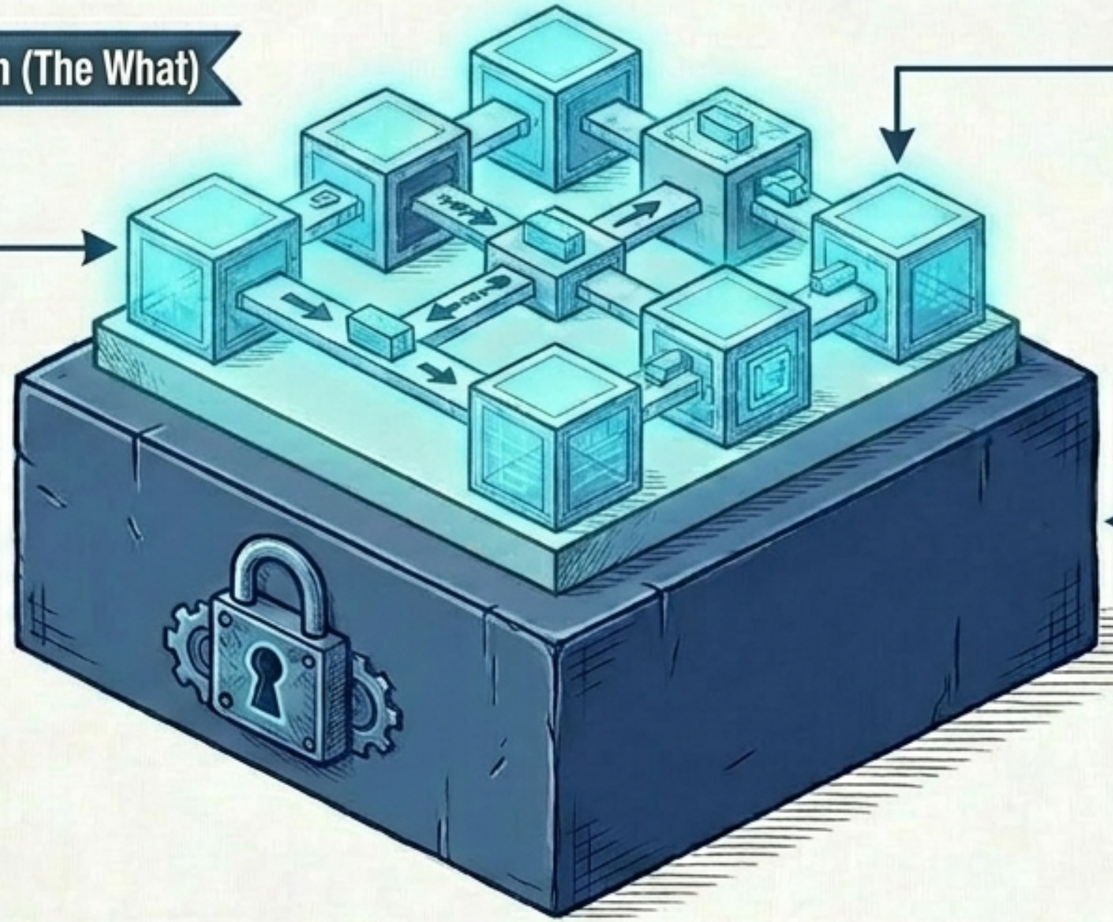
At a higher level, the total compromise of the functional host DOES NOT compromise the base cryptographic material.

Trust opens the structural channel; context defines the action

Layer 2: Contextual Authorization (The What)

Can this machine identity invoke this specific API for this Tenant?

Resolved operationally through IAM policies and context.



Layer 1: Structural Trust

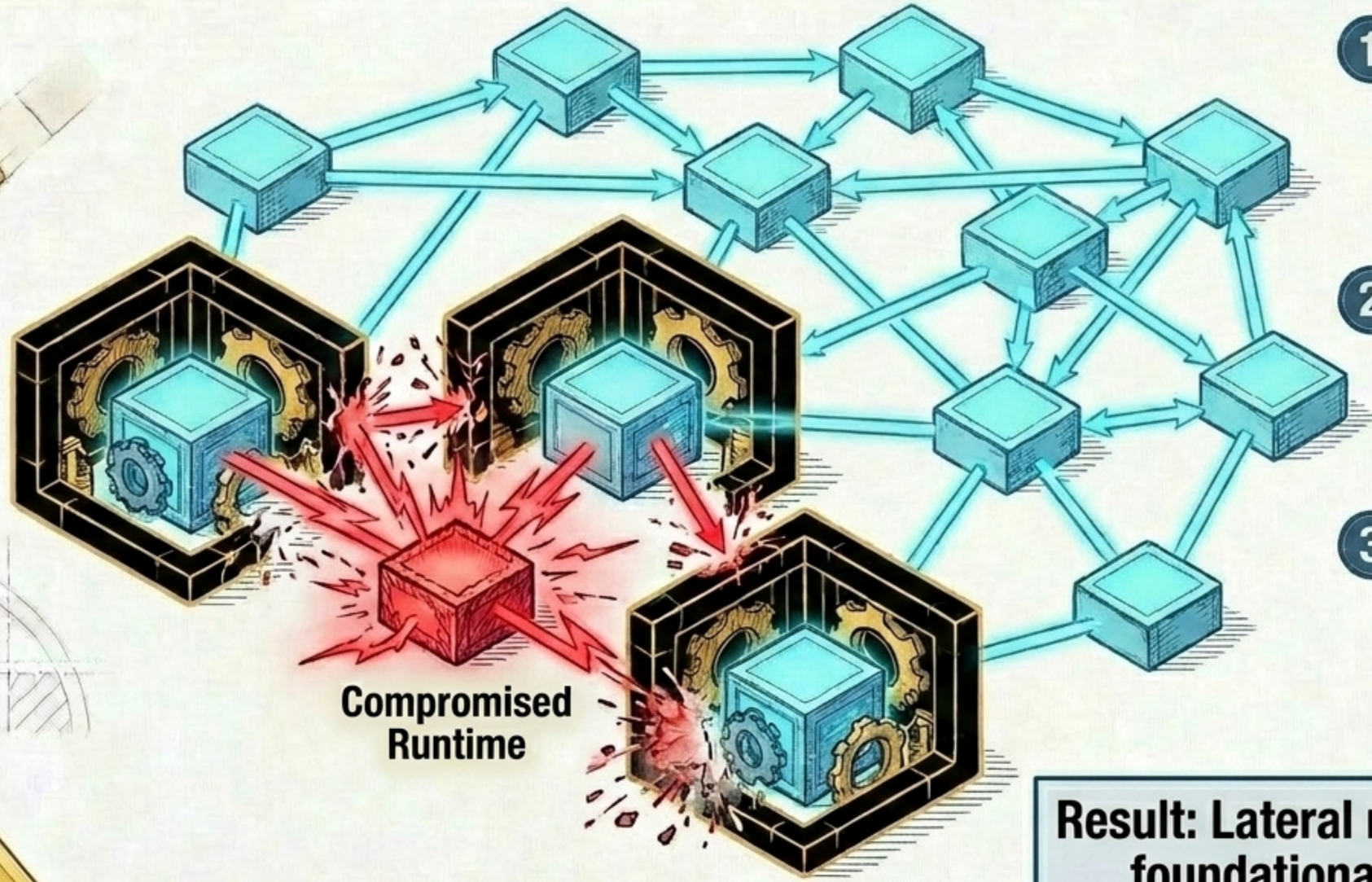
(The Who)

Can Plane A and Application B interact securely?

Resolved mathematically through signatures and JWKS distribution.

Design Principle: New horizontal cryptographic relationships (Trust) are never generated between applications to resolve context needs.

Compartmentalization Design: Containing the Blast Radius



1. Zero Horizontal Trust

A compromised Engine does not maintain “trust bundles” towards its neighbors.

2. Key Isolation

Private keys are never shared. Impossible to extract the identity of other nodes.

3. Custody Isolation

Zero lateral access in Vault/HSM systems between capsules.

Result: Lateral movement blocked at the foundational cryptographic level.

Strategic Validation: Why We Require a Distributed Model

	Traditional / Centralized	SkyDefended InfraApp
Runtime Performance	✗ Bottleneck due to synchronous latency.	✓ Zero added network latency (in-memory validation).
Functional Availability	✗ Critical dependency on the Auth server.	✓ Total resilience; the runtime operates without the Control Plane.
Scalability	✗ Vertical (Costly and limited).	✓ Horizontal, linear, and decentralized by capsules.
Security Anchor	✗ Identity tied to fallible perimeters, IPs, or VPNs.	✓ Identity tied exclusively to isolated cryptography.

The Definitive Zero Trust Status

Materialized through RSA and JWKS identities.

Survives ephemeral runtimes without latency.

“Trust in SkyDefended InfraApp is explicit, prior, mediated by the Control Plane, and validated locally.”

Never relies on networks or infrastructure.

Evolutive custody up to hardware (HSM).

NEXOCYBER NETWORKS
NCN
NETWORKING, SEGURIDAD Y SISTEMAS