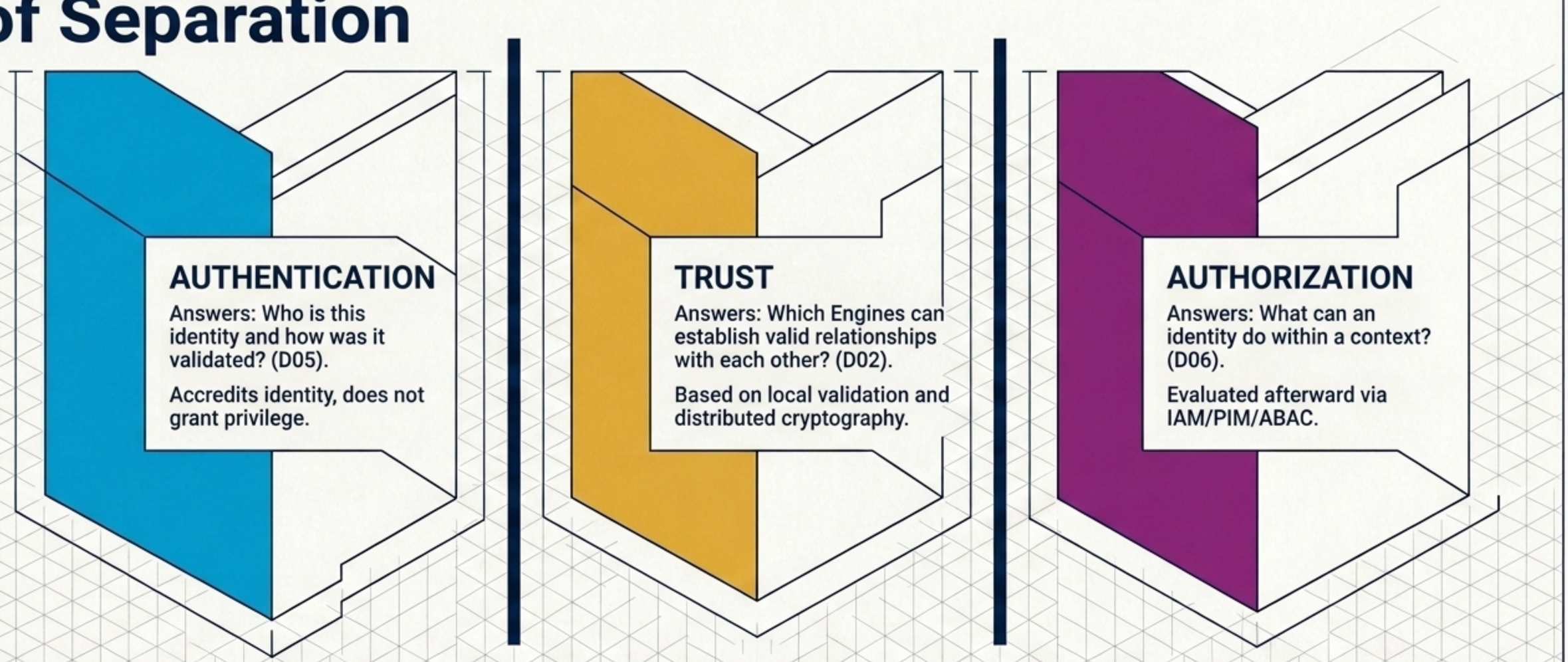
NEXOCYBER NETWORKS
NCN
NETWORKING, SEGURIDAD Y SISTEMAS

Distributed Authentication and Federation Model

Multi-Plane Zero Trust Architecture (D05)

Canonical Architectural Document for
SkyDefended InfraApp v1.0.

The Fundamental Principle of Separation



No identity gains privilege simply by authenticating.

Platform Zero Trust DNA

Approved Foundations

- ✓ NIST SP 800-207 (Zero Trust Architecture)
- ✓ Identity-Centric Security & Explicit Verification
- ✓ Just-In-Time (JIT) Privilege Elevation
- ✓ Decentralized Validation

We do not base authentication on:

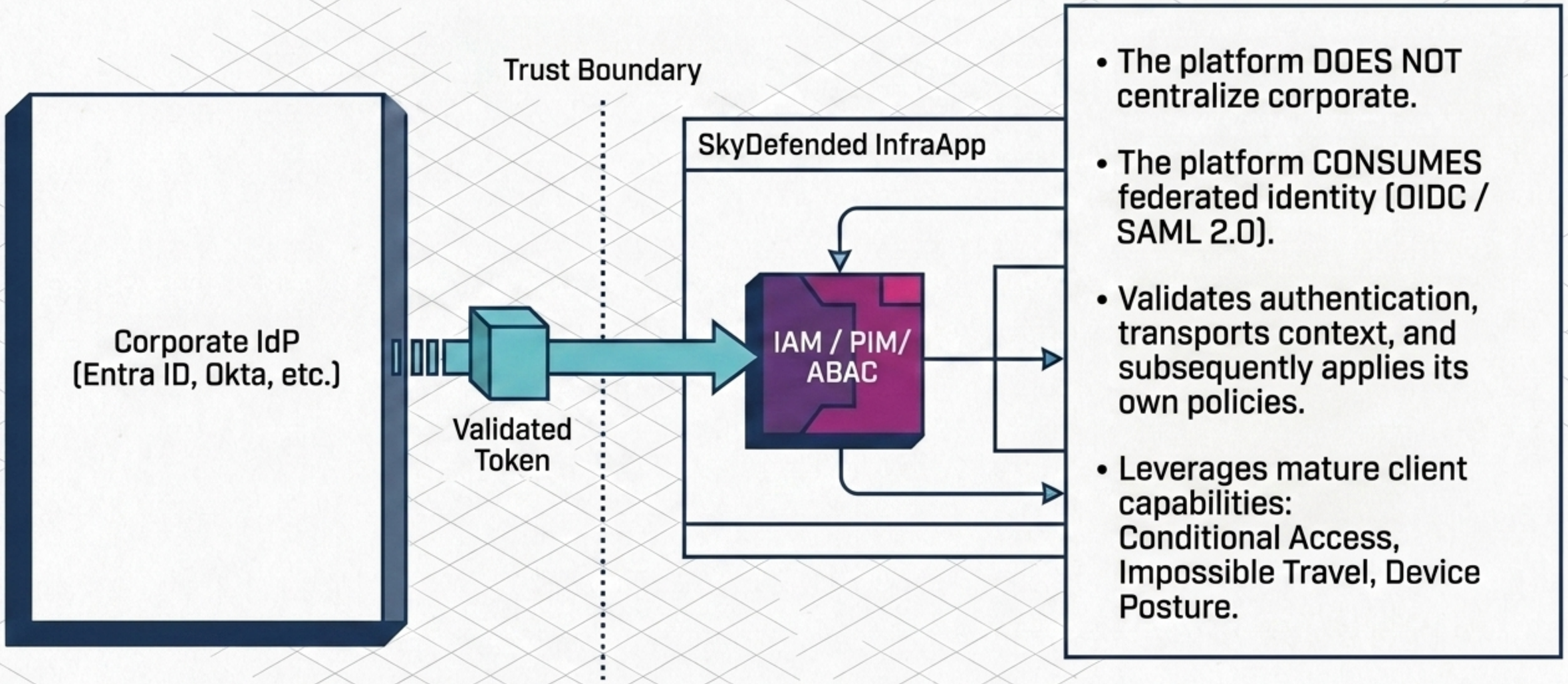
- ✗ Private networks or topological proximity
- ✗ Membership in a cluster or IPs
- ✗ Shared infrastructure or physical location

Aligned with NIST SP 800-63-3 (Digital Identity) and ISO/IEC 27001:2022.

Authentication Domain Boundaries

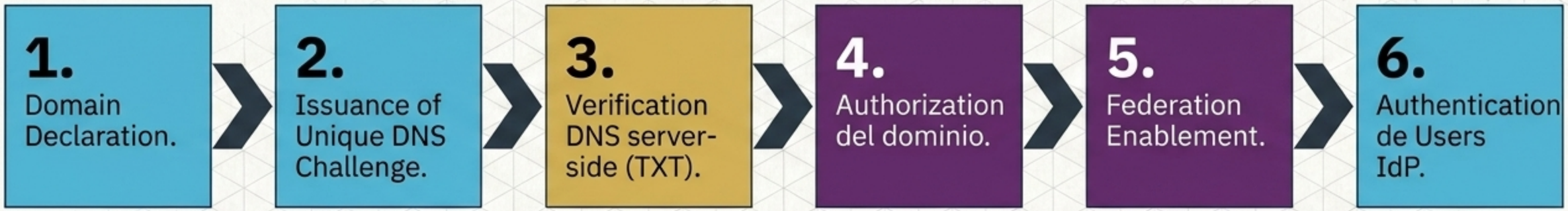
	Control Plane	Access Plane
Purpose	Governance of root structure and global administrative lifecycle.	Sovereign operational domain of the tenant.
Owner / Authority	SkyDefended InfraApp (NCN).	The Tenant (Client).
Daily Identity	NCN Corporate Federation (Entra ID).	Client Corporate Federation (OIDC/SAML).
Local Users	5 Sovereign Local Owners.	5 Local Owners of the tenant.
Isolation Rule	Does NOT participate in the functional operation of the tenant.	Does NOT have visibility over the root structure.

Tenant Sovereignty: InfraApp is NOT the IdP



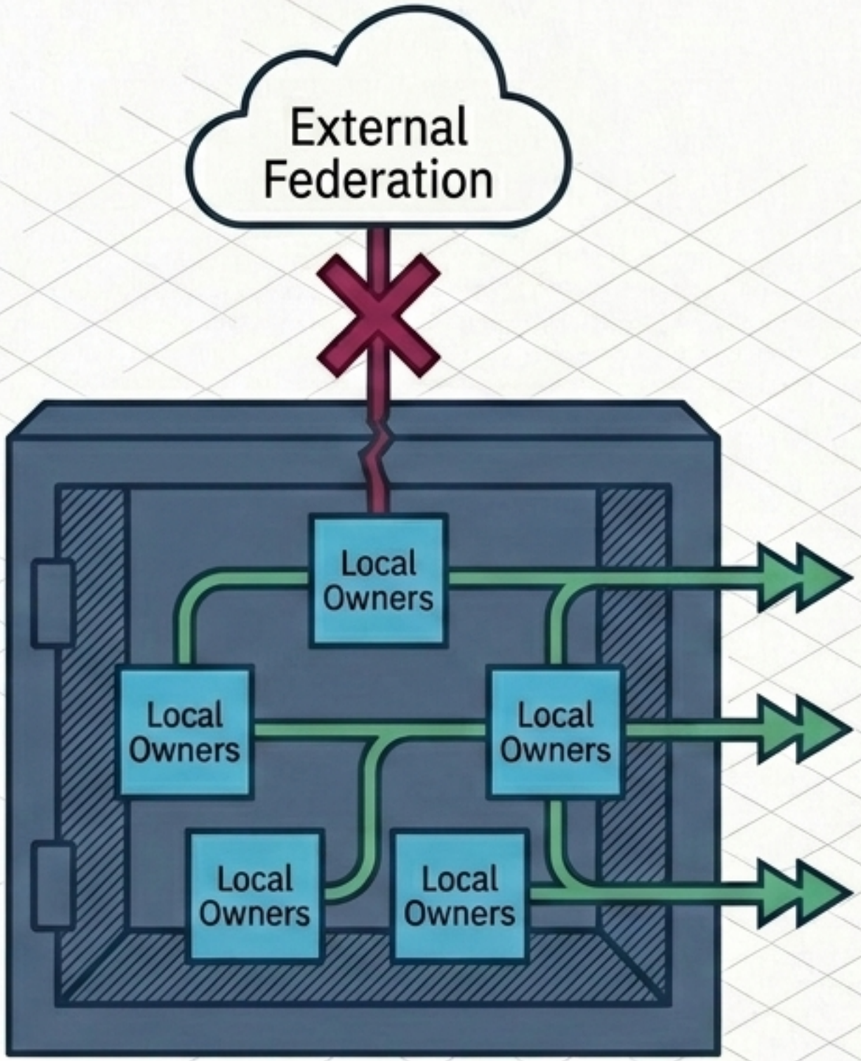
- The platform DOES NOT centralize corporate.
- The platform CONSUMES federated identity (OIDC / SAML 2.0).
- Validates authentication, transports context, and subsequently applies its own policies.
- Leverages mature client capabilities: Conditional Access, Impossible Travel, Device Posture.

Strict Validation of Federated Domains



Tronjanza es no se basa en ‘un **login Microsoft**’.
Exige validación explícita para evitar suplantación.

Local Owners and Sovereign Resilience

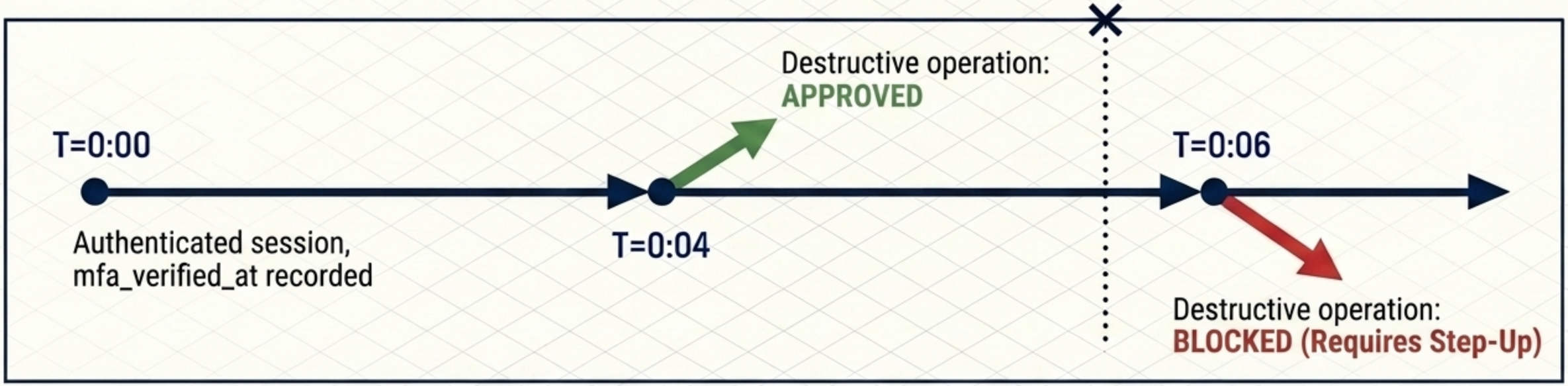


Purpose: Operational continuity, recovery from federation loss (Break-glass), and sovereign bootstrap.

Design: 5 owner administrators per tenant (and 5 in the Control Plane).

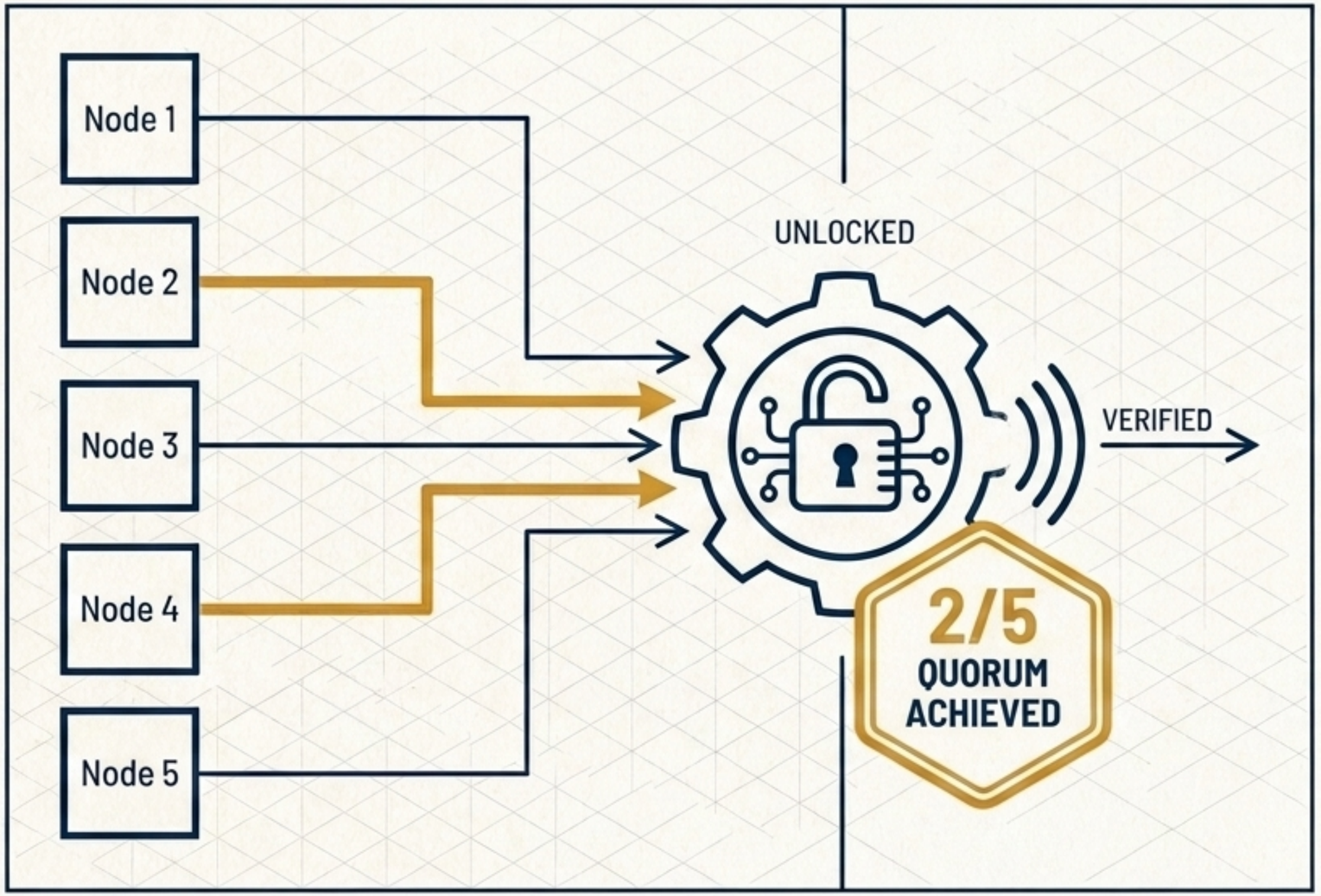
Independence: Use any domain, require email untiqueness,
DO NOT depend on corporate federation.
Not intended for daily operation.

Cryptographic Custody and Step-Up Authentication



Custody	Step-Up
Custody: TOTP (RFC 6238). SMS explicitly excluded (NIST AAL2). Seed never in plaintext. **Encryption:** Vault Transit, AES-256-GCM, non-exportable custody.	**Step-Up:** Destructive operations require recent MFA (maximum window: 5 minutes). **Grace Period:** Configurable (0-5 days) to balance onboarding and mandatory security.

Distributed Administrative Quorum



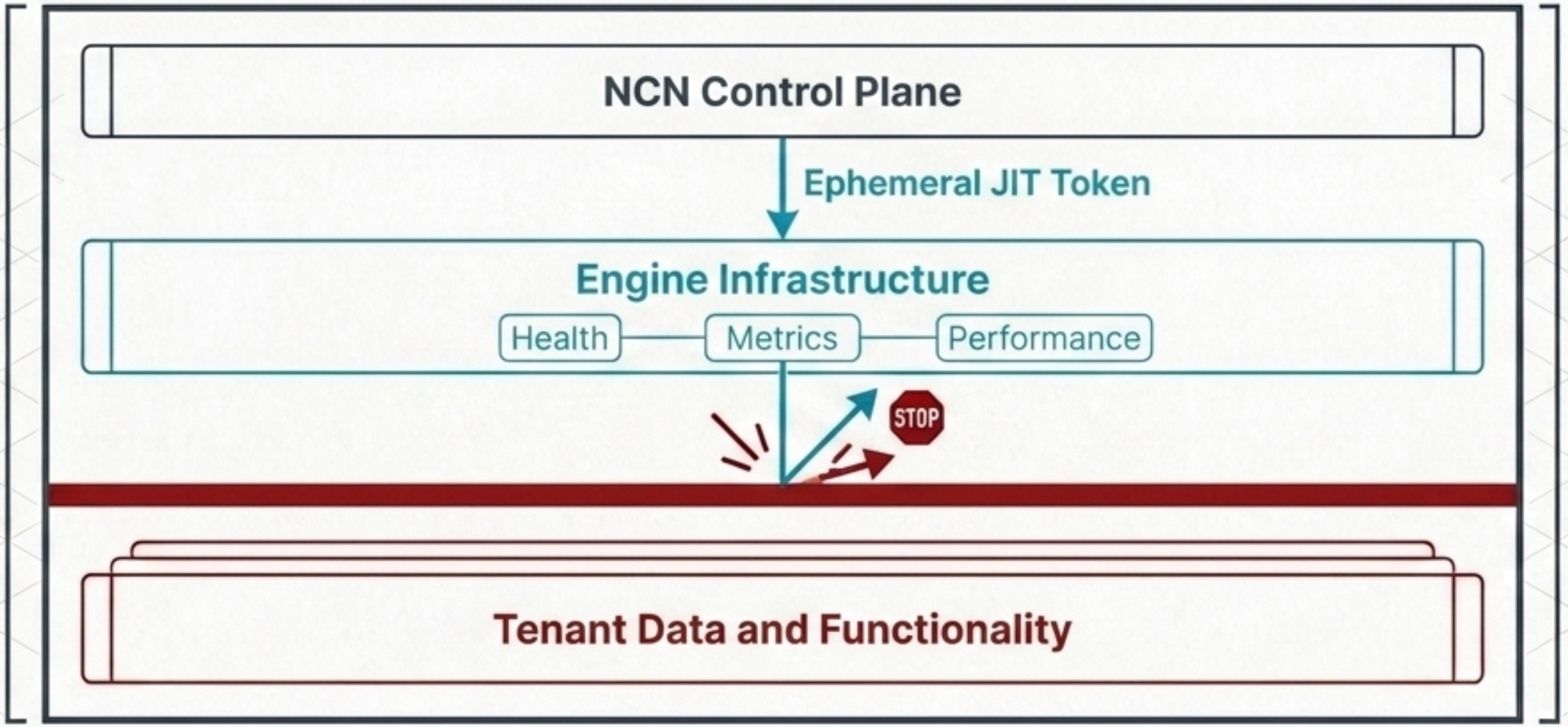
Concept: Dual-control and ‘two-person integrity’ (permanent privilege reduction).

Rule: Minimum quorum 2/5 (2 of 5 Owners).

Mechanism: Server-side validation. The operation remains pending until explicit approval from independent sessions.

Application: Root mutations, irreversible actions, break-glass, structural platform changes.

Ephemeral NCN Access and Data Isolation



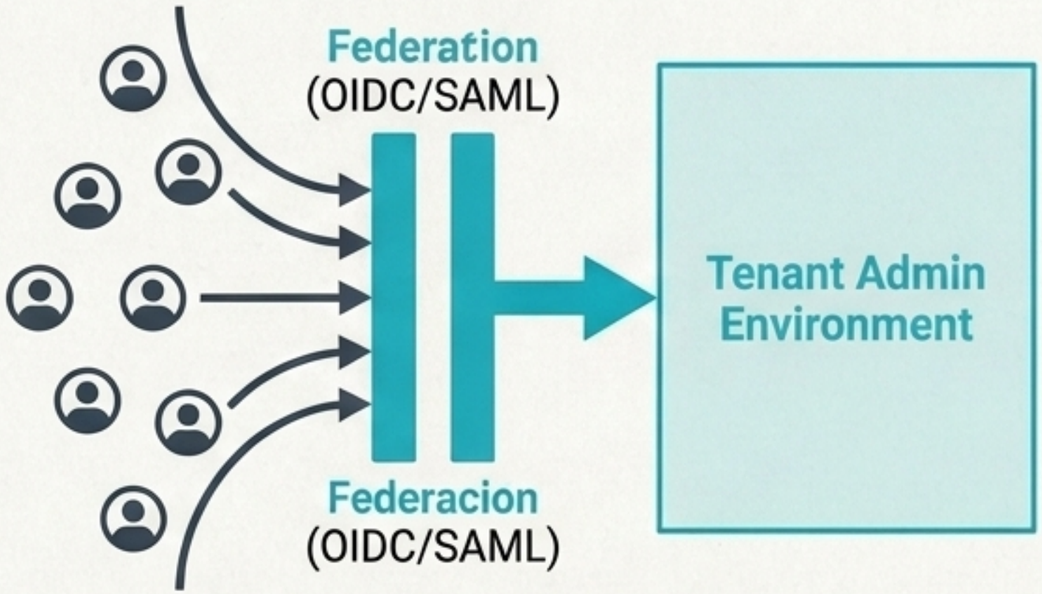
Just-In-Time (JIT):
Temporary token, limited scope, short TTL. Requires PIM and explicit justification.

Permitted Access:
Engine health, metrics, diagnostics, connectivity.

Hermetic Barrier:
The token does NOT allow access to tenant data, raw audit, or consent bypass.

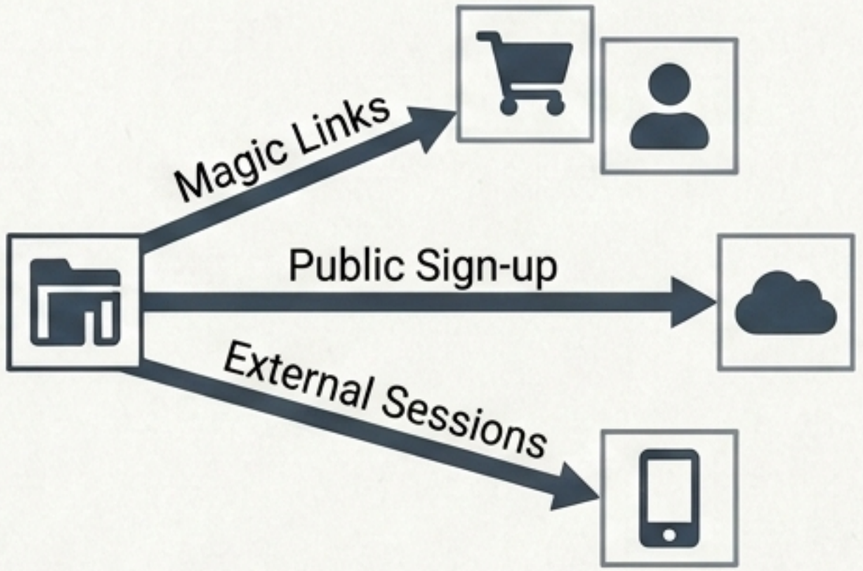
Administrative Shell vs. Application Autonomy

Administrative Authentication



Integrated applications reuse the Access Plane as a unified administrative shell.

Applications with External Users



Maintain total autonomy over login, sign-up, and session management of their final and external clients.

Principle: Administration centralizes identity in the platform; the final application runtime belongs to its own business model.

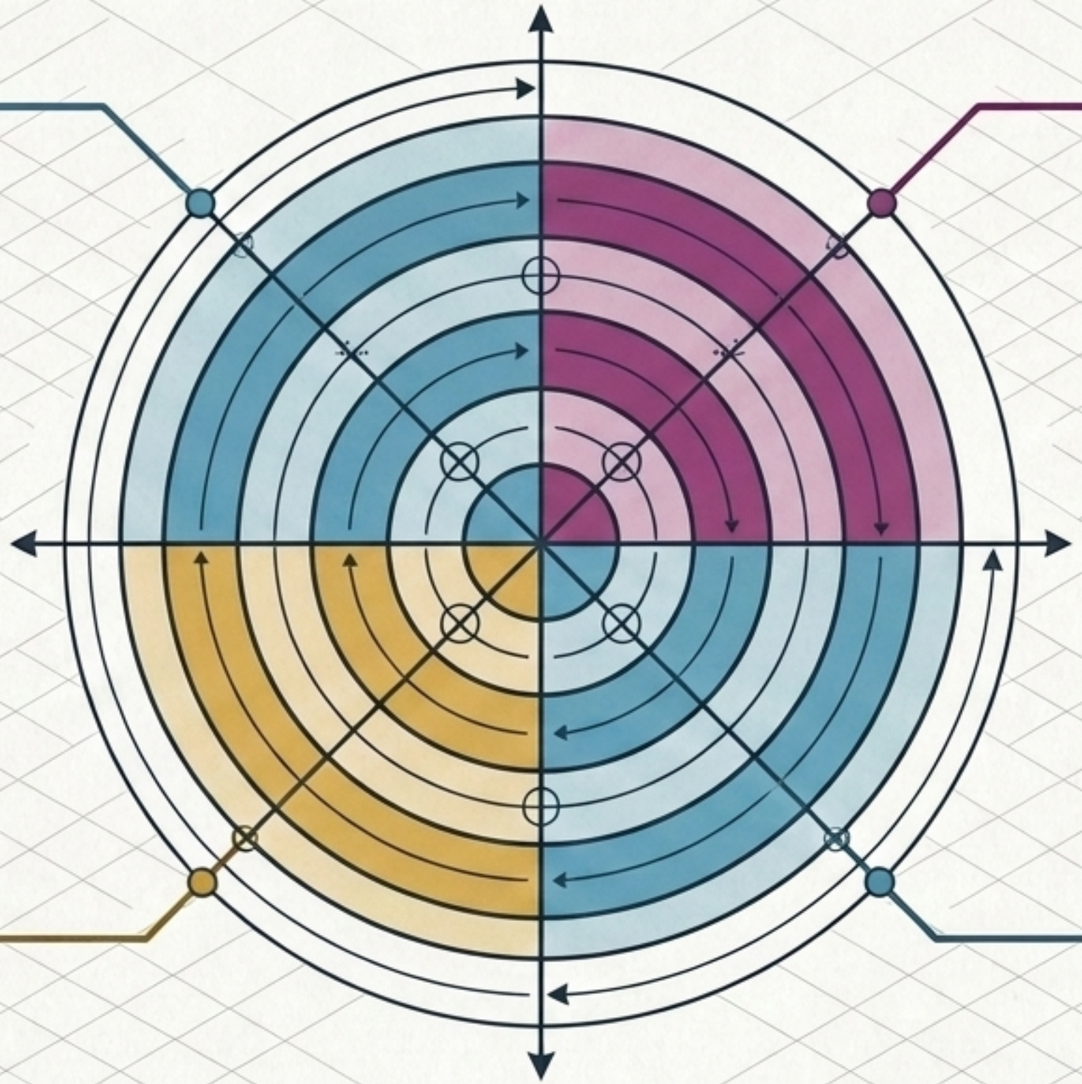
Defensive Layers and Resilience Posture

Session Protection

JWE sealed cookies, ticket+exchange tokens (out of URLs), dual-key rolling, short TTL.

Anti-Abuse

Global rate limiting, CSRF protection, anti-user enumeration, anti-bcrypt-DoS.



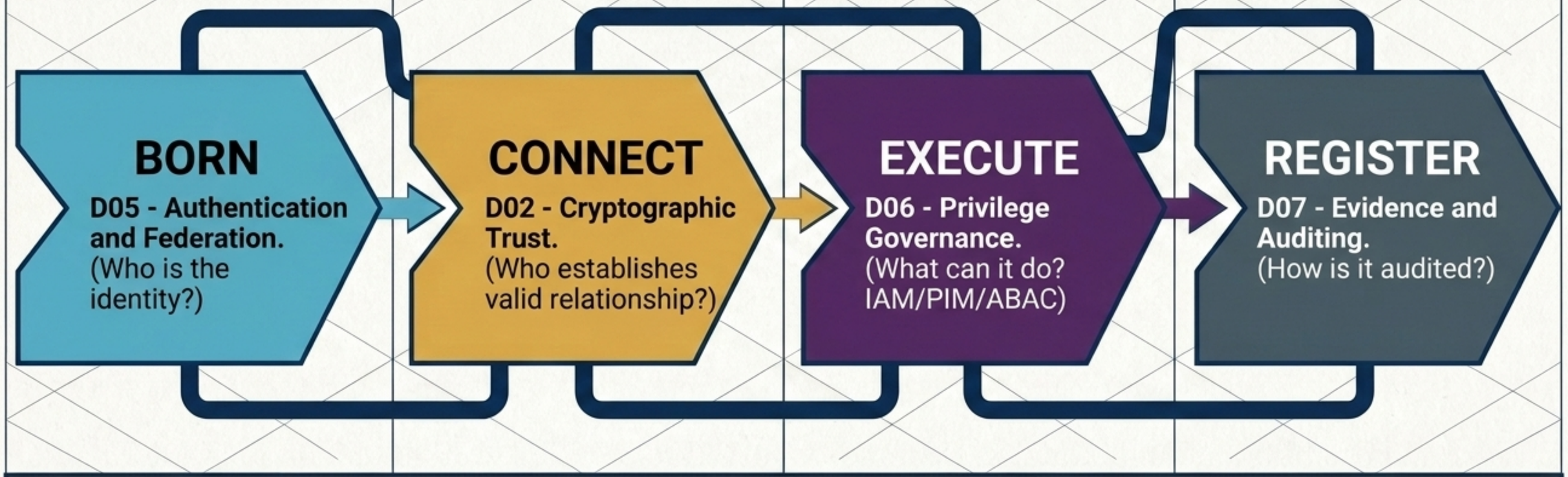
Credential Integrity

Compromised password detection (HaveIBeenPwned k-anonymity), distributed revocation.

Evolution Roadmap

FIDO2, Passkeys, WebAuthn, Risk-based & Continuous authentication, Device fingerprinting.

The Integral Security Ecosystem



Synthesis: Authentication (D05) injects identity into a system where capability is relentlessly filtered, governed, and registered.

Architectural Conclusion

SkyDefended InfraApp separates authentication, trust, and authorization: users authenticate via sovereign or federated mechanisms; Engines establish trust via distributed cryptographic identity; and all effective capacity is governed a posteriori under explicit Zero Trust principles.

NEXOCYBER NETWORKS
NCN
NETWORKING, SEGURIDAD Y SISTEMAS