IBERGRID 2026 | Santiago de Compostela

A Modular Cloud–Native Architecture: Unifying Bare-Metal Infrastructure & Client-Side Developer Platforms

Bridging Low-Level Hardware Efficiency with Developer-First Abstractions

Speaker: **Samuel Bernardo**

Team: **LIP and CNCA**

LIP

ARCHITECTURAL VISION

OVERVIEW & PILLARS

A Modular Cloud-Native Architecture

Unifying Bare-Metal Infrastructure & Client-Side Developer Platforms

Architectural Decoupling

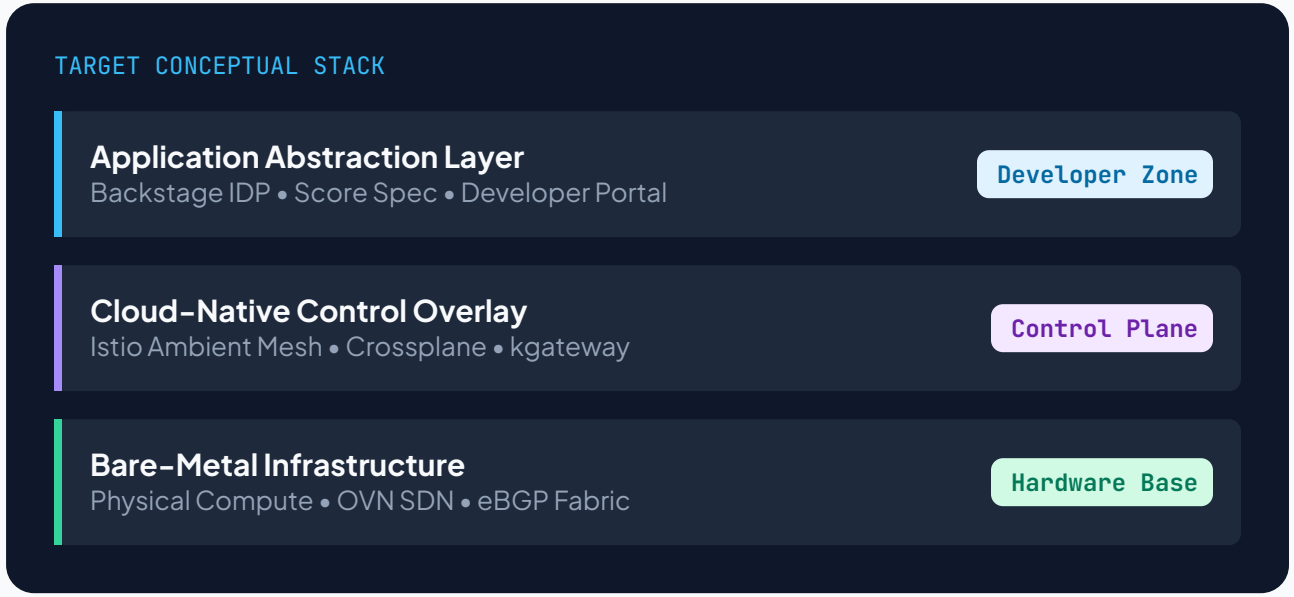
Separating bare-metal hardware operations from application delivery.

Developer Autonomy

Empowering developers with simple declarations while platform teams enforce governance.

Lightweight Mesh & Gateways

Providing ambient L4/L7 network abstractions without sidecar overhead.



DEVELOPER EXPERIENCE

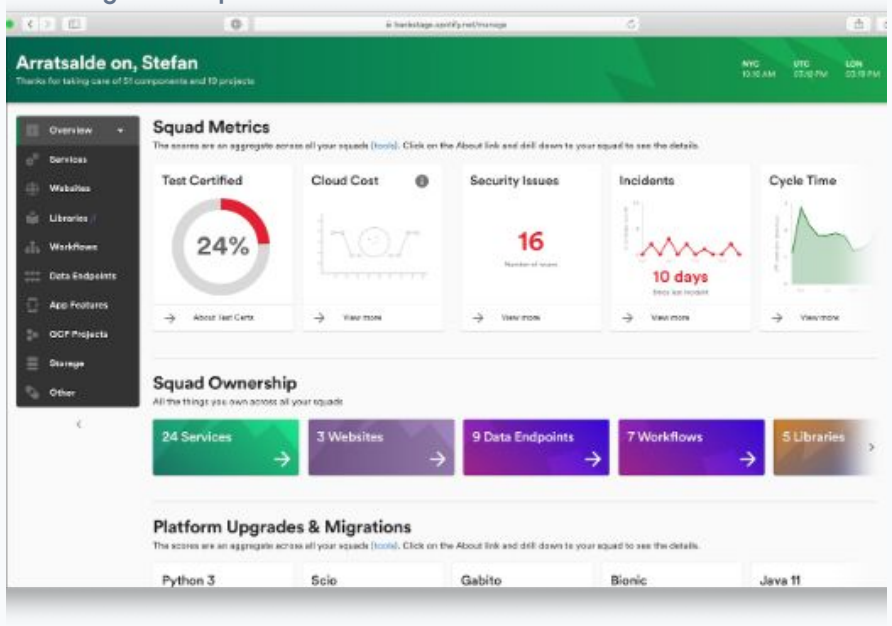
Simplifying Workload Delivery with Backstage & Score

1. **Backstage Portal** — Fills template form
2. **score.yaml Spec** — Declares intent
3. **CI Automation** — Renders manifests
4. **GitOps Sync** — Deploys to cluster

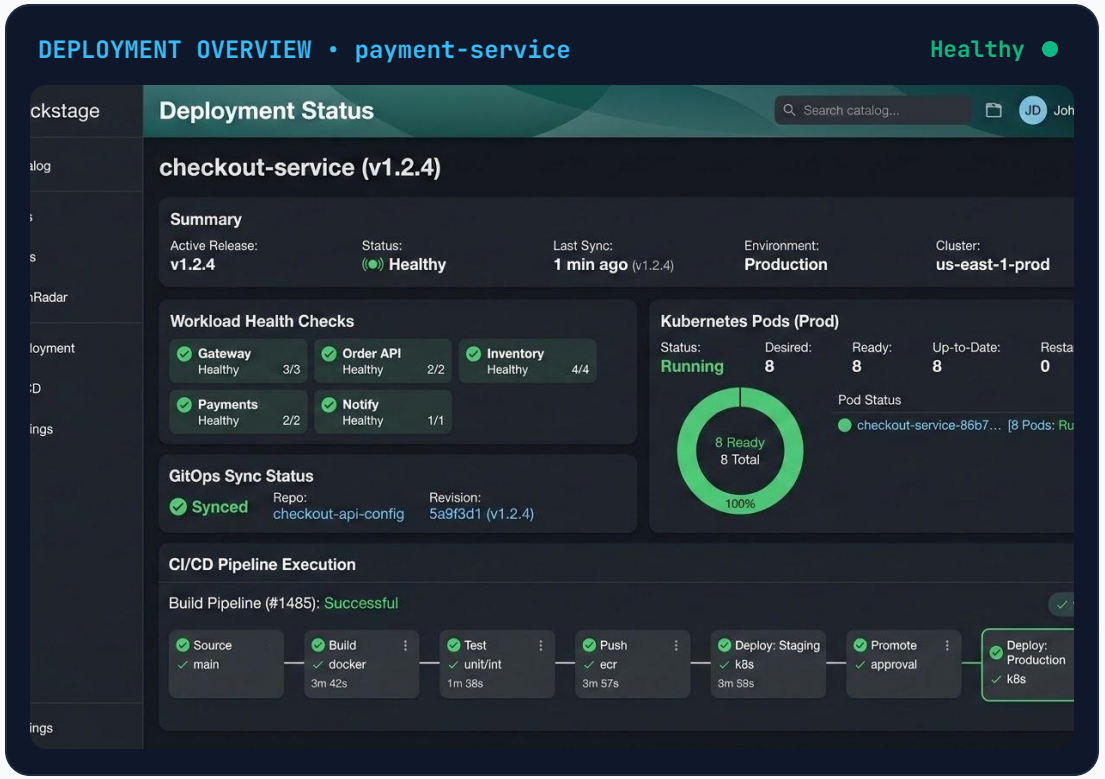
Backstage Portal Integration

Centralized software catalog and debugging dashboard. Developers inspect workload health without holding cluster-admin credentials or learning `kubectl`.

Backstage Developer Portal



Developer Intent



DEVELOPER EXPERIENCE

Simplifying Workload Delivery with Backstage & Score

1. **Backstage Portal** — Fills template form
2. **score.yaml Spec** — Declares intent
3. **CI Automation** — Renders manifests
4. **GitOps Sync** — Deploys to cluster

Backstage Portal Integration

Centralized software catalog and debugging dashboard. Developers inspect workload health without holding cluster-admin credentials or learning `kubectl`.

Score Spec (`score.yaml`)

Abstract, developer-centric workload specification. Developers declare high-level application dependencies (CPU, memory, database) in simple terms.

Zero Raw K8s Manifests

Developers never edit verbose Kubernetes manifests, Helm values, or cloud consoles—eliminating cognitive load and misconfiguration risks.

score.yaml — Developer Intent

```yaml
apiVersion: score.dev/v1b1
metadata:
      name: payment-service
containers:
      web:
            image: .
            variables:
                  PORT: "8080"
            resources:
                  limits:
                        cpu: "100m"
                        memory: "256Mi"
resources:
      db:
            type: postgres
```

CONTROL PLANE & GOVERNANCE

Behind-the-Scenes Guardrails: GitOps & Control Plane

INPUT SPEC	CONTROL PLANE	DELIVERY ENGINE	BARE-METAL CLUSTER
score.yaml	Crossplane XRD	FluxCD Pull Sync	Reconciled State

Crossplane Blueprints

Platform engineers author XRDs and Compositions, exposing pre-approved infrastructure blueprints as Kubernetes CRDs.

FluxCD Pull Engine

Continuous delivery engine syncs generated manifests into clusters without exposing cluster-admin credentials to CI.

Winning Combination

Developers gain immediate self-service autonomy while platform teams retain strict compliance, security, and budgeting guardrails.

SIDECARLESS SERVICE MESH ARCHITECTURE

Sidecarless L4/L7 Overlay with Istio Ambient

Rust-Powered ztunnel Execution Engine

TOKIO & RUSTLS RUNTIME

Built natively in Rust with the Tokio work-stealing runtime and rustls. By stripping away heavy L7 proxy parsing layers, Rust ztunnel handles up to **40 Gbits/second** in mTLS operations, slashing node memory consumption by **~4×** compared to Envoy sidecars.

40 Gbps
mTLS Throughput

4×
Memory Reduction

Node DaemonSet (L4)

ztunnel runs per node supplying zero-trust mTLS, SPIFFE identity, and L4 auth without pod proxy sidecars or restarts.

Opt-In L7 Waypoints

L7 processing (header routing, retries, policy) is decoupled into dedicated Waypoint proxies applied per namespace or service.

Gateway API Standard

Developers specify networking rules once via Kubernetes Gateway API, completely insulated from physical CNI topologies.

SPECIALIZED EDGE & MESH WAYPOINTS

Tailored Waypoints: kgateway & agentgateway

NORTH-SOUTH EDGE

kgateway (API Edge)

Consolidates enterprise API ingress, TLS termination, OAuth/JWT authentication, global rate-limiting, and Gateway API routing.

- Replaces legacy ingress controllers with unified policy.

Role: Enterprise Perimeter Ingress Gateway

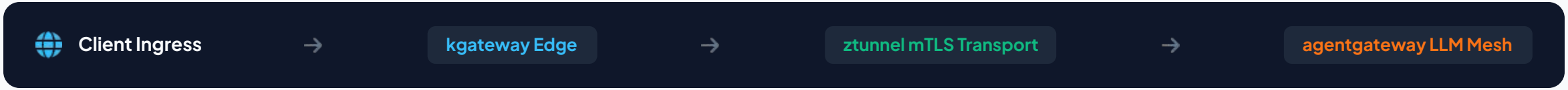
EAST-WEST AI MESH

agentgateway (AI Waypoint)

Ultra-low-latency Rust proxy designed specifically for AI/LLM workloads, handling token streaming, MCP context, and agent orchestration.

- High-throughput token streaming & multi-agent mesh.

Role: Specialized AI / LLM Traffic Waypoint



SUMMARY & TAKEAWAYS

Architectural Impact: a unifed modern cloud-native platform

Decoupled Architecture

Bare-metal hardware and OVN/eBGP network complexity are cleanly isolated from application delivery layers.

Developer Velocity

Backstage portals and Score declarative specs simplify onboarding without Kubernetes learning curves.

Control & Governance

Crossplane, FluxCD, and Istio Ambient offer fine-grained governance, policy enforcement, and auditability.

AI Pipeline Readiness

Specialized Rust agentgateways handle token streaming and agent orchestration seamlessly within the mesh.

Maximum bare-metal efficiency paired with seamless developer self-service autonomy.

Enterprise Scale

Thank You

A Modular Cloud-Native Architecture: Unifying Bare-Metal Infrastructure & Client-Side Developer Platforms

Engineering & Operations Team (LIP & CNCA)



Zacarias Benta
LIP - Minho



João Machado
CNCA



Samuel Bernardo [Speaker]
LIP



João Paulo Martins
LIP



César Ferreira
CNCA - Minho



Pedro Pinheiro
LIP



Jorge Gomes
LIP



João Pina
LIP

Conference Contribution
Scan for slides & details

Questions, Collaboration & Operational Inquiries
Contact Email: **helpdesk@lip.pt** • Conference: *IBERGRID 2026*

LIP - Laboratório de Instrumentação e Física Experimental de Partículas
Partículas e Tecnologia