An Identity-Aware Proxy Architecture for Integrating Keycloak IAM with External Providers and Services

Bridging National Identity Platforms (amagovpt) and High-Performance Computing (Slurm/Kubernetes)

Speaker: **Samuel Bernardo**

Team: **LIP and CNCA**

The Integration Gap: External IDPs vs. Operational HPC

Protocol Impedance Mismatches Across Upstream Government IDPs and Downstream Compute

OAuth 2.1 Security Constraints

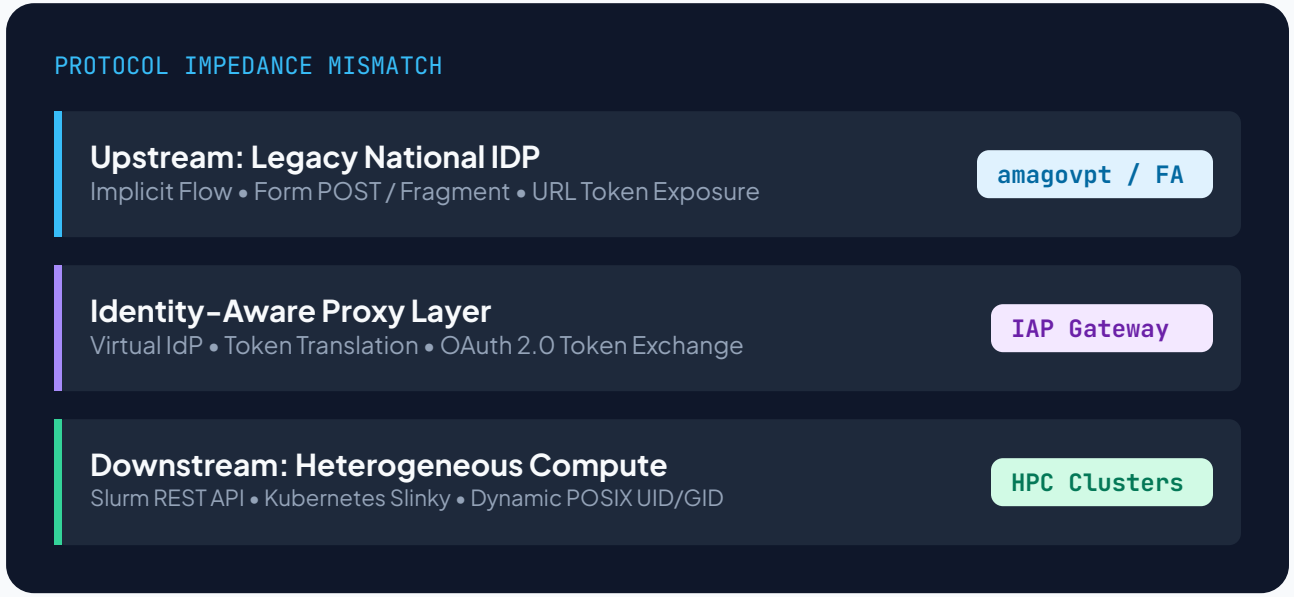
Deprecation of Implicit Grant (response_type=token) due to URI query string leakage in server logs, referrer headers, and browser history.

National Provider Limitations

External government services (Fornecedor de Atributos / FA, amagovpt) still rely on implicit flows and fixed callback domains.

HPC & Compute Demands

Slurm REST API over TLS and Kubernetes require short-lived, scoped tokens bound to valid POSIX user contexts without exposing admin keys.



GATEWAY ARCHITECTURE

The IAP Gateway: Virtual IdP & Protocol Broker

1. **1. Client Browser** — Authenticates to IAP
2. **2. IAP Proxy** — Isolates implicit flows
3. **3. Keycloak STS** — Token exchange (RFC 8693)
4. **4. Target Service** — Scoped token delivery

Intermediate Gateway Layer

`Node.js / paseto-ts`

Developed using Node.js, Express, openid-client, Passport, and paseto-ts. Acts as a high-performance architectural buffer shielding downstream services from identity provider specifics.

Isolating Legacy Implicit Flows

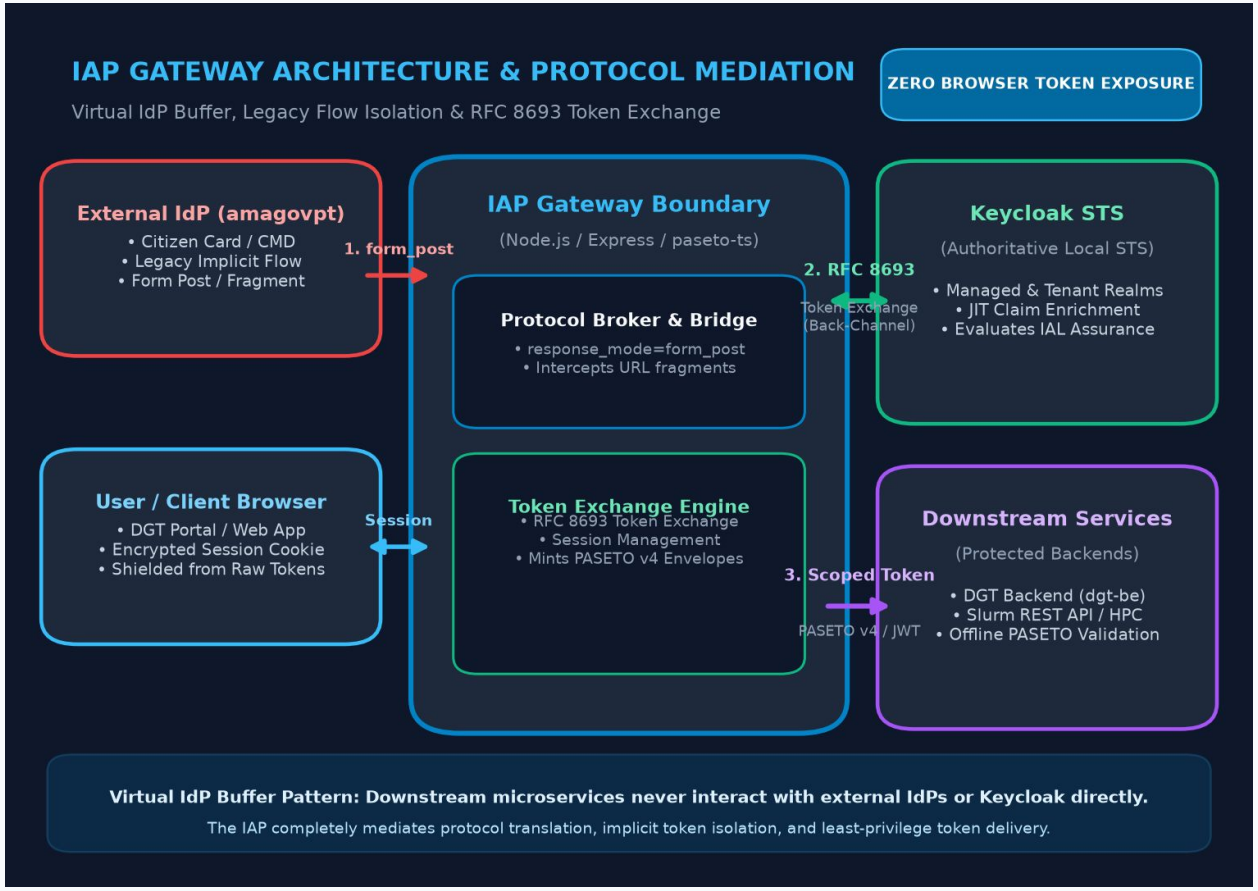
`response_mode=form_post`

Intercepts amagovpt responses at the proxy boundary via HTTP POST bindings and URL fragment bridges. Prevents direct client browser exposure of sensitive bearer tokens and fragments.

Back-Channel Token Exchange

`RFC 8693 STS`

Executes OAuth 2.0 Token Exchange (RFC 8693) against Keycloak. Keycloak acts as the authoritative local Security Token Service (STS) minting scoped downstream assertions.



DOMAIN ISOLATION & GOVERNANCE

Keycloak Multi-Realm Domain Isolation & JIT Provisioning

1. **1. amagovpt Auth** — Citizen Card / CMD
2. **2. Managed Realm** — Isolated external realm
3. **3. JIT Enrichment** — NIC / Tax ID mapped
4. **4. Tenant Realm** — Downstream access

Realm & Assurance Isolation

External IDPs (amagovpt) are isolated in a dedicated managed realm separate from the organizational tenant realm. Enforces distinct Identity Assurance Levels (Citizen Card vs CMD).

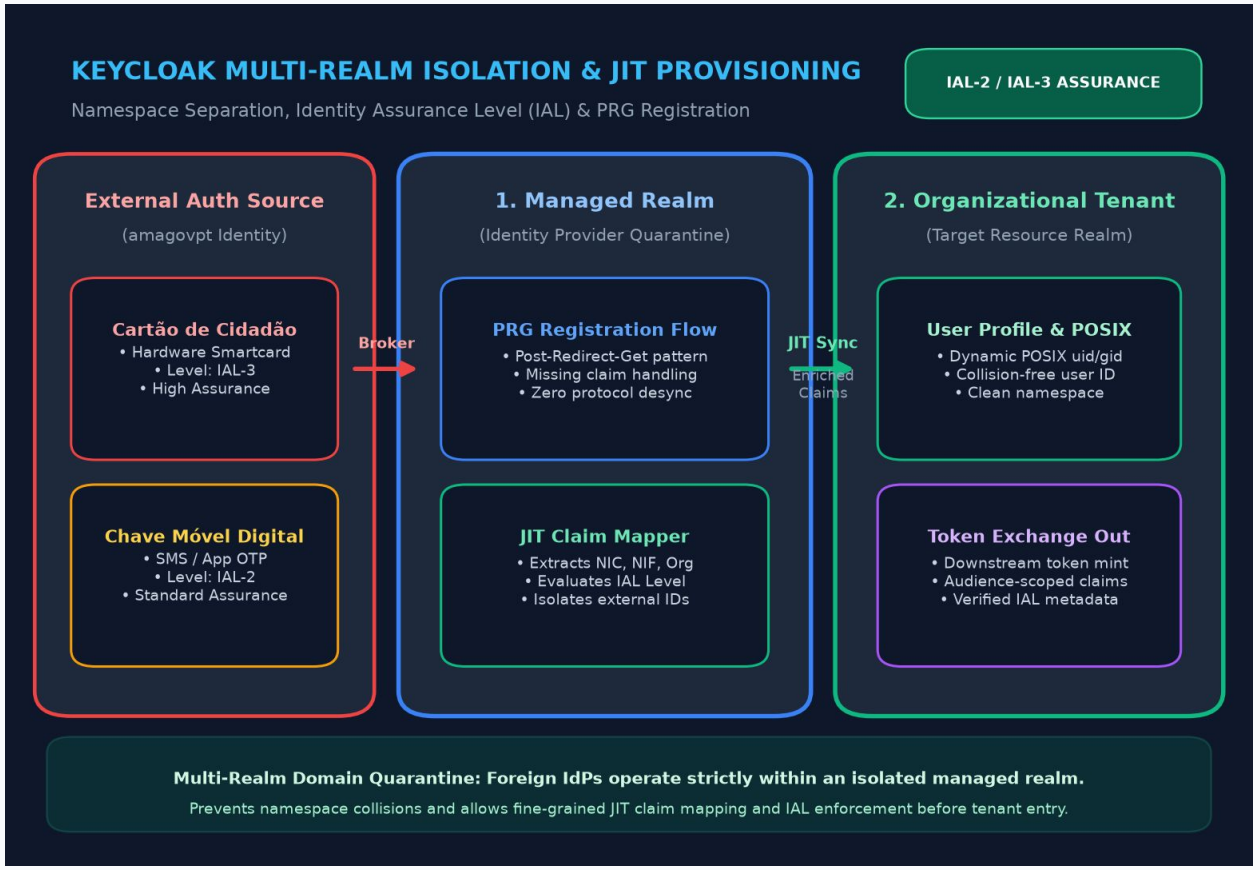
`IAL-2/3`

Just-In-Time (JIT) Provisioning

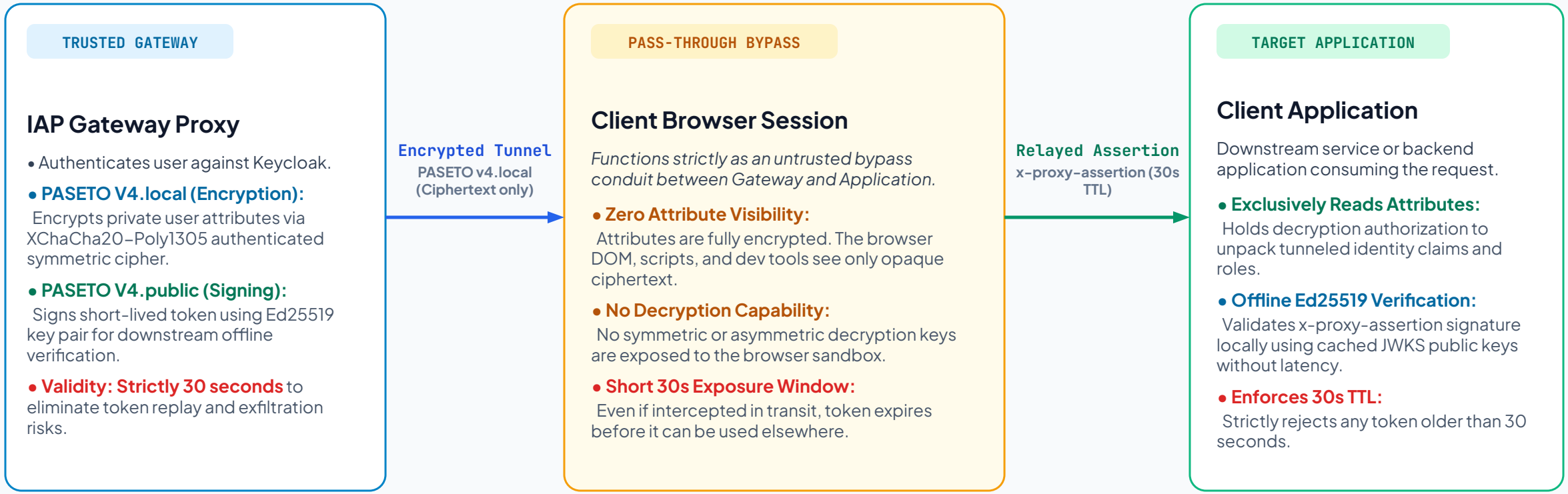
Validated citizen attributes (NIC, tax ID, professional credentials) dynamically populate local user accounts upon first login without manual intervention.

Post-Redirect-Get (PRG) Registration

Handles missing mandatory attributes during First Broker Login cleanly without breaking protocol state or creating namespace collisions across realms.



PASETO v4: Attribute Tunneling & 30s Tokens



CORE INVARIANT: ATTRIBUTE PRIVACY & 30s TTL

- **Cryptographic Strengthening:** Combines V4.local authenticated symmetric encryption (XChaCha20–Poly1305) and V4.public asymmetric Ed25519 signing. Attributes are tunneled and only decryptable by the designated client application.
- **Browser Session as Pure Bypass:** The browser merely carries the payload without possessing the keys to inspect or tamper with sensitive claims, preventing frontend data exposure.
- **30–Second Token Validity:** Token lifespan is restricted to ~30s, minimizing attack surfaces, replay windows, and credential exfiltration through client environments.

CLIENT SPECIALIZATION // DUAL-CLIENT ARCHITECTURE

Dual-Client Federation: Web Frontend & Desktop QGIS Plugin

IN-BROWSER SESSION

Web Frontend (dgt-fe / dgt-be)

Ephemeral ECDH Agreement: Negotiates secp384r1 keys with IAP for app-scoped encryption.

Encrypted PASETO v4: Wraps user claims; browser scripts never hold bearer tokens.

LOOPBACK + PROOF-OF-POSSESSION

Desktop QGIS Plugin (dgt-plugin)

Ephemeral Browser Auth: Starts 127.0.0.1 listener for Keycloak login; browser closes after handoff.

PoP HMAC Tokens: Exchanges auth code + RSA fingerprint for Proof-of-Possession tokens.

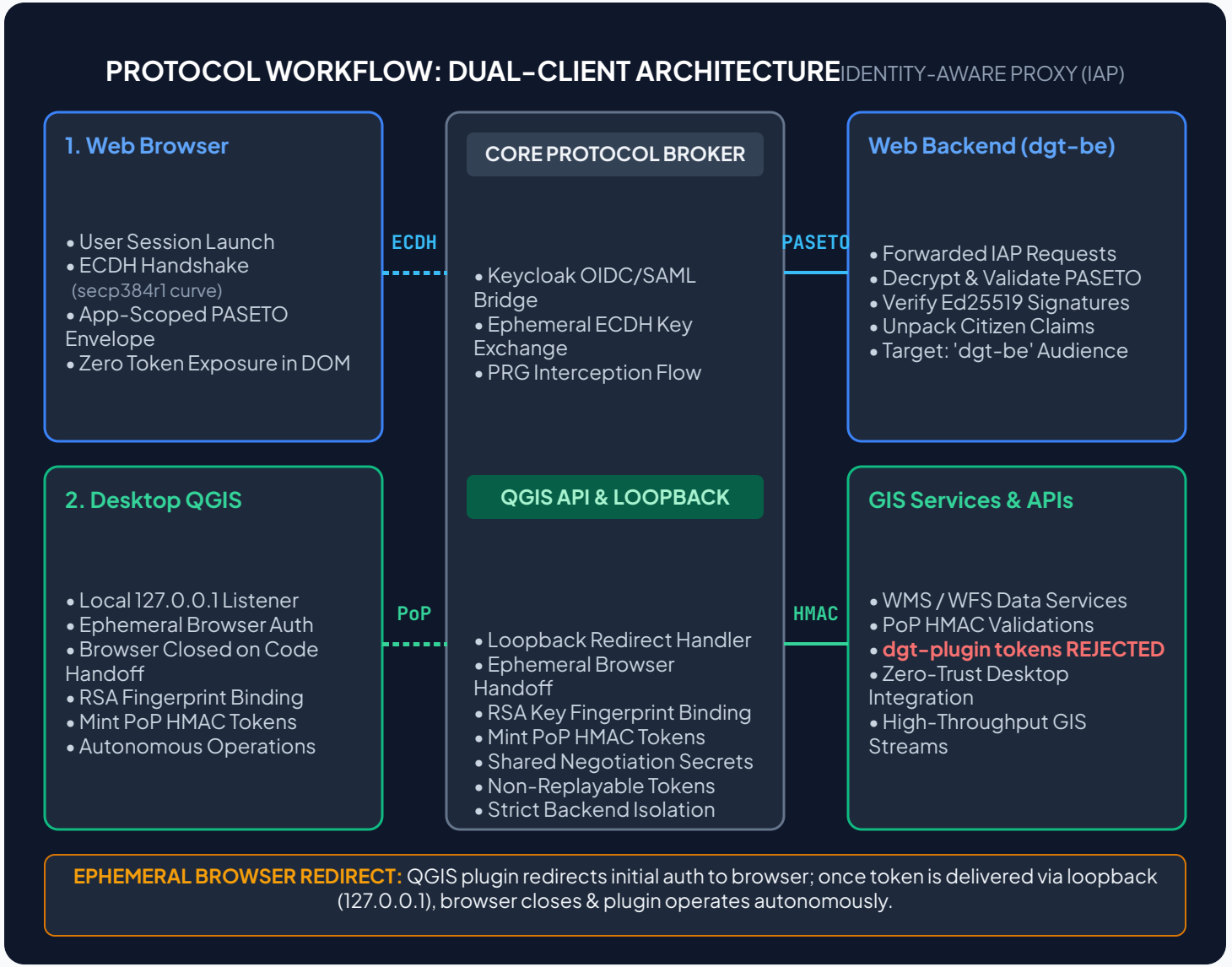
Autonomous Operation: Runs headlessly without persistent sessions or re-prompts.

AUDIENCE ISOLATION

Cryptographic Isolation & Replay Prevention

Non-Replayable Credentials: Tokens issued for dgt-plugin are strictly rejected by dgt-be.

Zero Cross-Contamination: Clients cannot spoof or impersonate each other's session context.



USE CASE 2 — HIGH-PERFORMANCE COMPUTING

Kubernetes slurm-bridge (SchedMD Slinky) & External Slurm

OBO BROKERAGE

Kubernetes Slinky (slurm-bridge)

On-Behalf-Of (OBO) token brokerage enables Kubernetes operators to dispatch jobs without storing administrative root keys or long-lived static tokens.

✓ Eliminates cluster-to-HPC privilege escalation.

Role: Kubernetes Slinky Dispatcher

POSIX & RBAC

External Slurm HPC Cluster

Dynamic POSIX mapping binds user uid/gid to short-lived RS256 JWTs or scontrol tokens. Path-level RBAC blocks administrative changes while allowing job submissions.

⚡ Single-flight caching protects slurmctld from token storms.

Role: POSIX-Mapped Slurm REST API Execution

Workflow → 1. K8s Pod / Slinky → 2. IAP OBO Translation → 3. slurmctld REST Execution

SUMMARY & TAKEAWAYS

Architectural Impact: Keycloak IAP Gateway

Enhanced Security Posture

Eliminates URL query string token leakage (OAuth 2.1 compliance) and mitigates JWT algorithm confusion risks via PASETO v4.

Multi-Provider Governance

Unifies rigid national identity flows (amagovpt) and enterprise OIDC within Keycloak multi-realm boundaries with dynamic JIT attributes.

Zero-Trust Compute Orchestration

Delivers fine-grained, short-lived credentials to specialized computational backends (Slurm REST API, Kubernetes, QGIS).

Automated Token Lifecycle

Offloads background token refreshes, back-channel single sign-out, and session maintenance from application backends.

A robust, scalable bridge connecting national identity infrastructure with enterprise IAM and HPC.

Enterprise IAM

Thank You

An Identity-Aware Proxy Architecture for Integrating Keycloak IAM with External Providers and Services

Questions, Collaboration & Operational Inquiries

Contact Email: **helpdesk@lip.pt** • Conference: *IBERGRID 2026*

Conference Contribution

Scan for slides & details

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