Model for distributed authorization policy sharing

IETF 125 - Hackaton

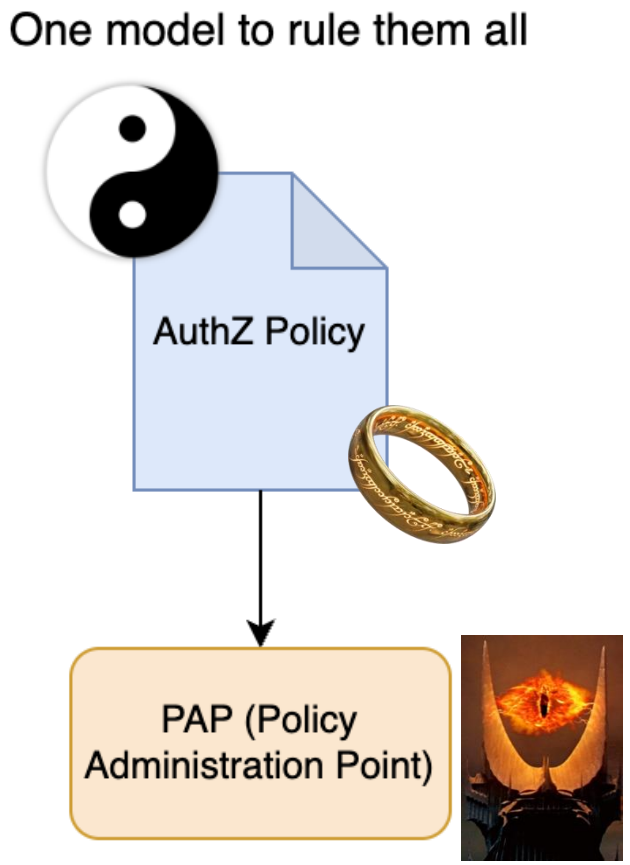
https://datatracker.ietf.org/doc/draft-cabanillas-nmop-authz-policy-sharing-model/01/

Lucía Cabanillas Rodríguez(lucia.cabanillasrodriguez@telefonica.com)
Diego López(diego.r.lopez@telefonica.com)
Ana Méndez Pérez(ana.mendezperez@telefonica.com)

YANG-based framework for policy sharing

Goal: Define a canonical way to manage and share authorization policies

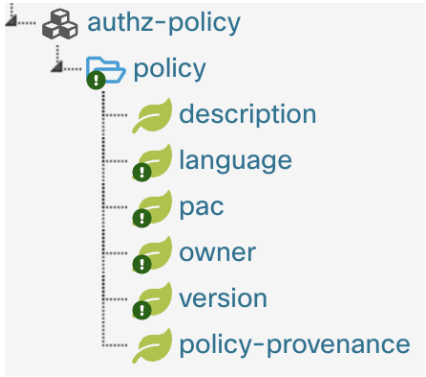
- YANG-based model for **machine-readable authorization policies**
- Enables **Policy-as-Code (PaC)**: policies as structured artifacts
- Supports the **full policy lifecycle**
  • creation • validation • versioning • distribution
- Designed for **interoperability across systems and domains**
- Policy engines (typically PDPs) consume and enforce the policies



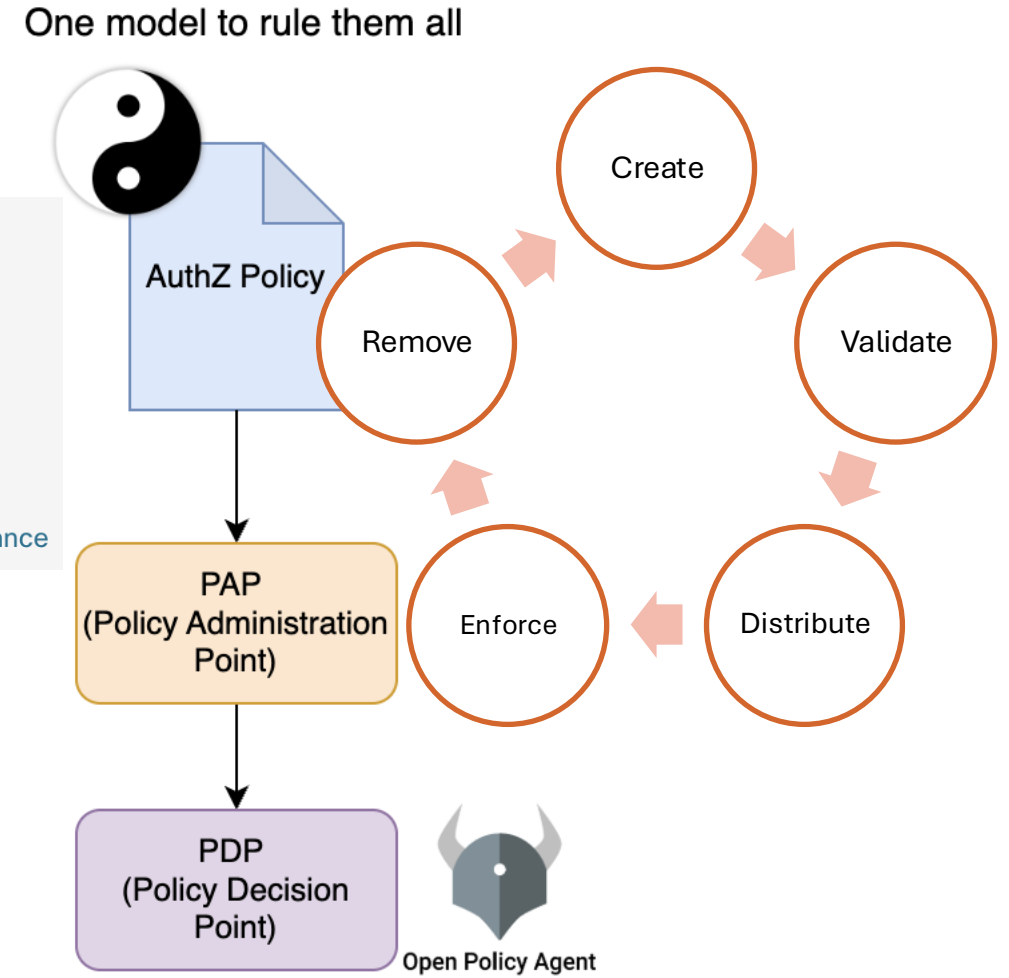
What we brought

A **policy artifact** modeled in YANG including:

- **Description** – human-readable explanation
- **Language** – policy language used
- **Policy-as-Code** – declarative policy content
- **Owner** – authority responsible
- **Version** – policy version for lifecycle management
- **Provenance (optional)** – signature



In the demo, the **policy artifact is processed by the PAP and executed in Open Policy Agent (OPA)** acting as the **PDP**, demonstrating how YANG-based policies can be validated, managed, and enforced in a real system



What we demonstrated

Scenario

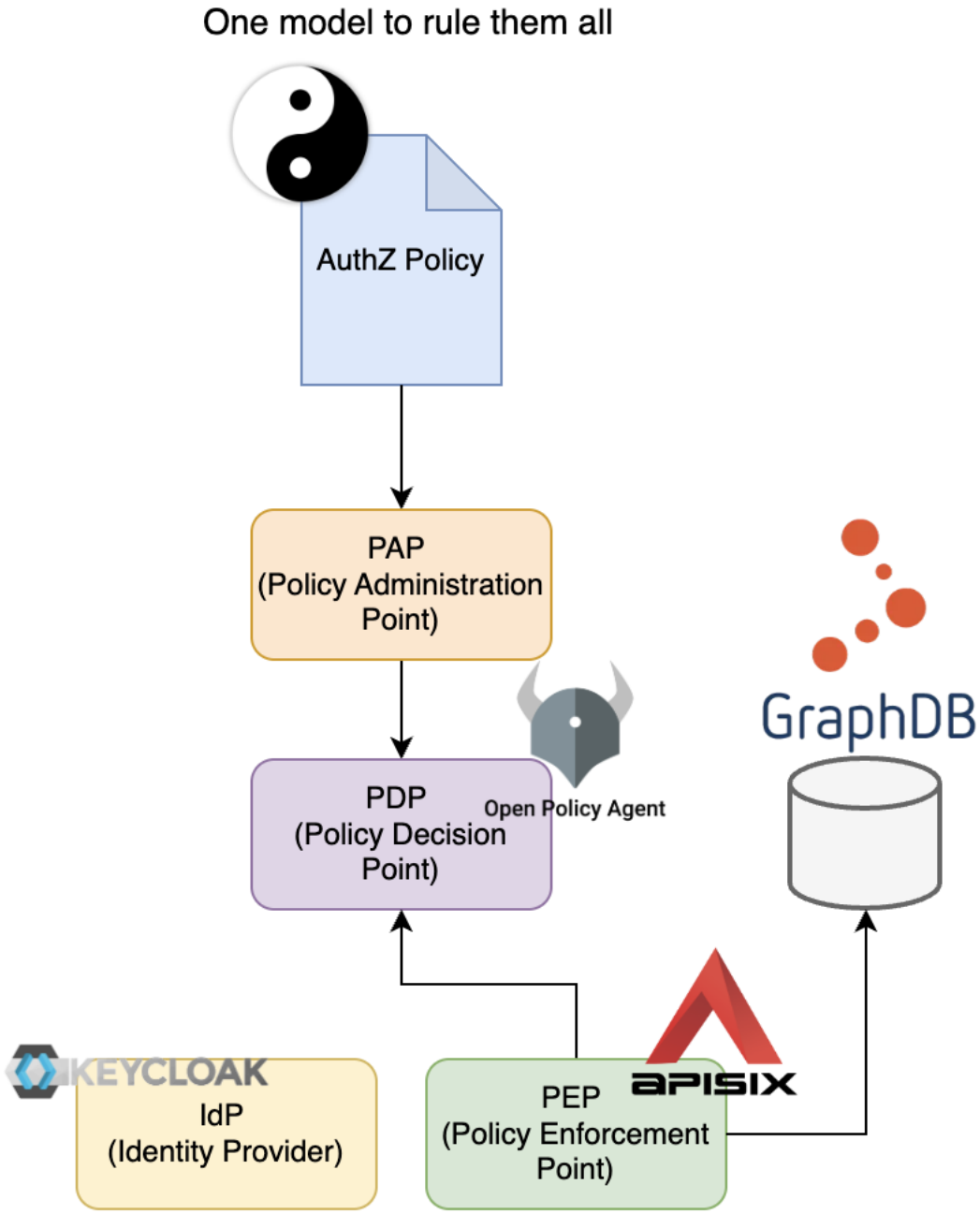
- A **YANG policy artifact** is submitted to the **PAP**
- PAP validates and distributes the policy to **OPA (PDP)**
- Policy logic written in **Rego**
- Protect data stored in **GraphDB**
- Policy denies queries requesting the field **vendorName**

Demo flow

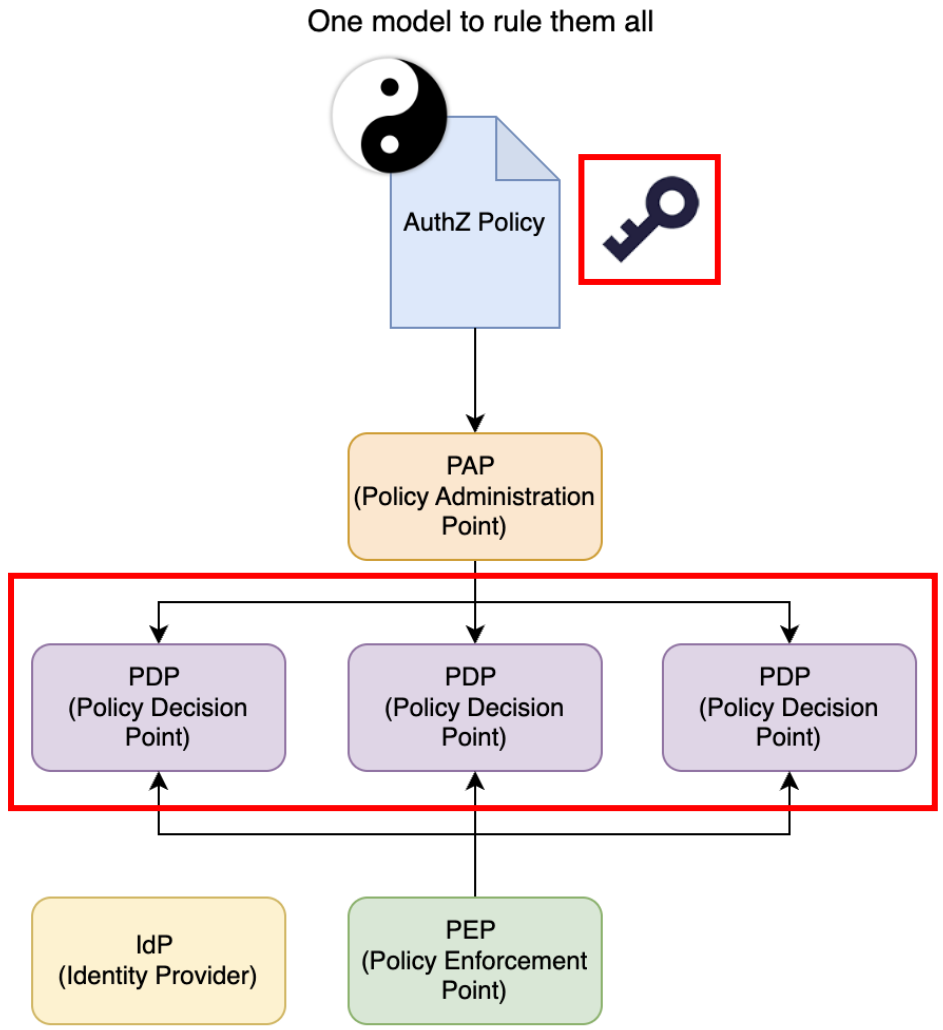
- User authenticates with **Keycloak (IdP)** → obtains token
- Request sent to **APISIX (PEP)**
- APISIX queries **OPA (PDP)** for authorization
- OPA evaluates the request using the **Rego policy**

- Allowed queries → **data returned**
- Queries requesting **vendorName** → **access denied**

Demonstrates **policy creation, distribution, and enforcement using the YANG-based model**



What we achieved and next steps

- YANG-based policy sharing implemented
- Demonstrated policy distribution from PAP to a PDP
- Validated interoperability and automation potential

- Policy provenance: COSE signatures
- Explore cross-domain
- Gather community feedback