Model for distributed authorization policy sharing

IETF 125 - NMOP

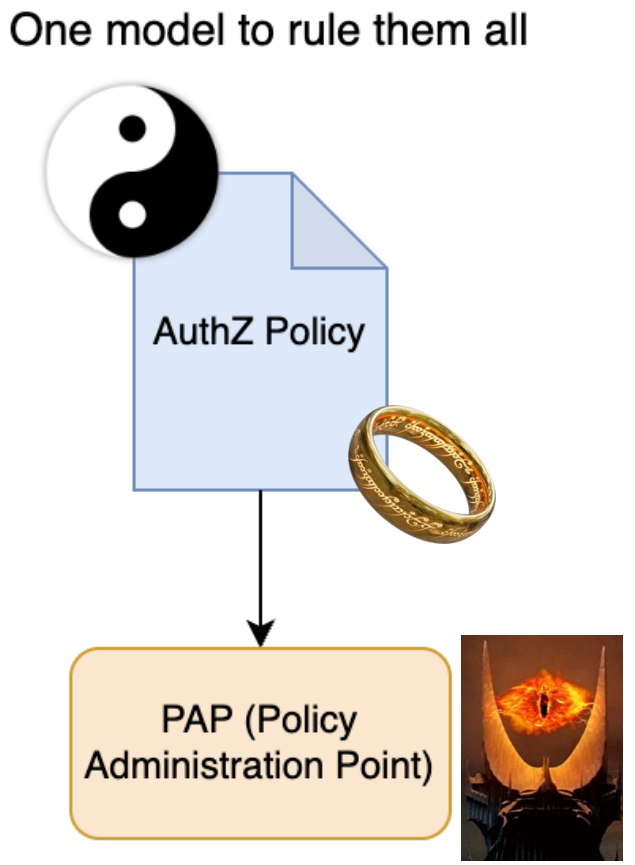
https://datatracker.ietf.org/doc/draft-cabanillas-nmop-authz-policy-sharing-model/01/

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 apply the policies



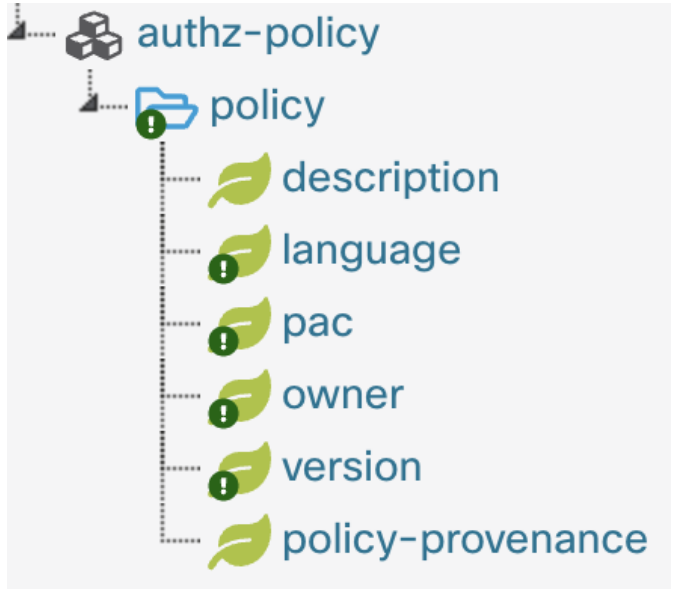
Updates

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

- **Description** – human-readable explanation
- **Language** – policy language used (Rego, Cedar, ALFA…)
- **Policy-as-Code** – declarative rule content
- Added **Owner** – authority responsible (URI)
  - PAP **may query PDP** to check authorization
- Added **Version** – policy version for management
- Added **Provenance (optional)** – verifiable signature providing proof of origin and integrity
  - Address verifiability and multi-domain trust

- **Complementary role** with existing YANG-based approaches
  - For example, OpenConfig gNSI authorization model

- Emphasis on **policy distribution and management**
- Lower focus on **policy semantics**



Hackaton

Scenario

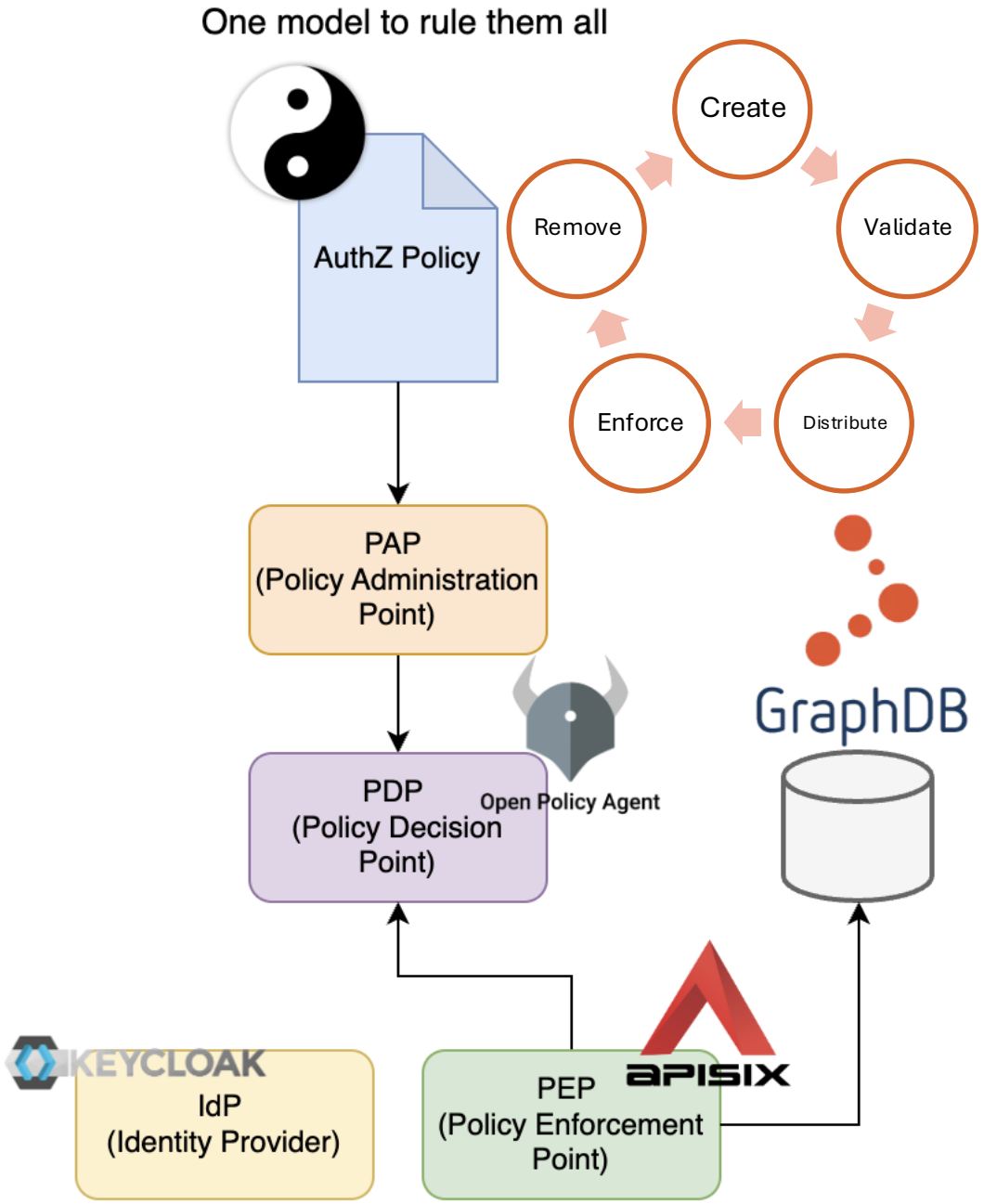
- A **YANG policy artifact** is submitted to the **PAP**
- PAP validates and distributes the policy to **OPA (PDP)**
- Policy logic written in **Rego**
- Protect data stored in **GraphDB**
- Policy denies queries requesting the field **vendorName**

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**



Open points and next steps

YANG model design

- Should policy language be an enum?
  - May be too restrictive
  - Alternatives?

- Refine YANG modules
- Explore integration with existing provenance mechanisms
- Refine the reference implementation with multiple domains, to be demonstrated at the next Hackathon
- Role of the Accounting Ledger

- Feedback welcome!