
KubeCon
CloudNativeCon
Europe 2023
TiKV


# The Compliance Business Case for Kubernetes in the EU: Get Ready for EUCS

**Anders Eknert,** Styra
**Robert Ficcaglia,** SunStone Secure

# Speaker Introduction

KubeCon CloudNativeCon Europe 2023

anderseknert@hachyderm.io

anderseknert

anderseknert

anderseknert

**Anders Eknert**

Developer Advocate

*Styra*

**Robert Ficcaglia**

Co-Chair, wg-policy

K8s SIG-security 3rd Party Audit

*Sunstone Secure*

# EUCS Trust and Transparency



- Article 48.2 Cybersecurity Act (EUCSA), ENISA Ad Hoc WG
- Reference set of **security requirements** — high-level (i.e, not specific to any particular technology)
- Requirements based on previous standards and national schemes, such as ISO/IEC 270xx, C5 🇩🇪, SecNumCloud 🇫🇷
- **Applies to any CSP** (Cloud Service Provider) — including IaaS, PaaS, SaaS, i.e. most of you!

# EUCS Trust and Transparency



- Requirements grouped in **19 categories**
- Each category divided in a number of **themes**
- **3-year certification** across the EU Member States
- **“Viral”**, as sub-services are included in the assessment and likely will need to be certified too
- CSP **self-assessment, reviewed by accredited auditor**

# EUCS Assurance Levels



## Basic

Minimize the **known basic** risks of incidents and cyber attacks — **low risk profile**

- Limited assurance
- Self-assessment reviewed by a third-party
- Focus on the definition and existence of procedures and mechanisms

## Substantial

Minimize **known** cybersecurity risks, and the risk of incidents and cyber attacks carried out by actors with limited skills and resources — **medium risk profile**

- Reasonable assurance
- Design and operating effectiveness
- Functional testing

## High

Minimize the risk of **state-of-the-art** cyber attacks carried out by actors with **significant skills and resources — elevated risk profile**

- Reasonable assurance
- Design and operating effectiveness
- **Continuous (automated) monitoring of compliance**

# Example EUCS Control

KubeCon CloudNativeCon Europe 2023

## IAM-05 REGULAR REVIEW OF ACCESS RIGHTS

### Objective

- The fitness for purpose of the user accounts of all types and their associated access rights are reviewed regularly.

### Requirements

| Ref | Description | Ass. Level | |
|---|---|---|---|
| IAM-05.1 | The CSP shall review the access rights of all the user accounts under its responsibility at least once a year to ensure that they still correspond to the current needs | Basic | From C5 Basic |
| IAM-05.2 | The review defined in IAM-05.1 shall be performed by authorised persons under the responsibility of the authorised body that has approved the access rights policies. | Substantial | |
| IAM-05.3 | The CSP handles identified deviations timely, but no later than 7 days after their detection, by appropriately revoking or updating access rights. | Substantial | |
| IAM-05.4 | The CSP shall provide CSCs with a tool that facilitates the review of the access rights of user accounts under their responsibility | Substantial | From SecNumCloud |
| IAM-05.5 | The CSP shall perform the review defined in IAM-05.1 at least every six (6) months | High | From C5 Additional |

# MEDINA



- **EU funded-research project**
- Goal: **to create a Security framework** for achieving a **continuous audit-based certification** in compliance with the EU-wide cloud security certification scheme
- The main objective of the project is to provide:
  - A **holistic framework** supporting CSPs (IaaS, PaaS and SaaS providers) towards the successful achievement of a continuous certification aligned to the EU Cybersecurity Act (EU CSA).
  - Provide **tools, techniques, and processes** supporting the continuous auditing and certification of cloud services where security and accountability are measurable by design.
  - Support **continuously assessing the efficiency and efficacy of security measures** to ultimately achieve and maintain a certification.


KubeCon
CloudNativeCon
Europe 2023
Open Policy Agent

# Open Policy Agent (OPA)

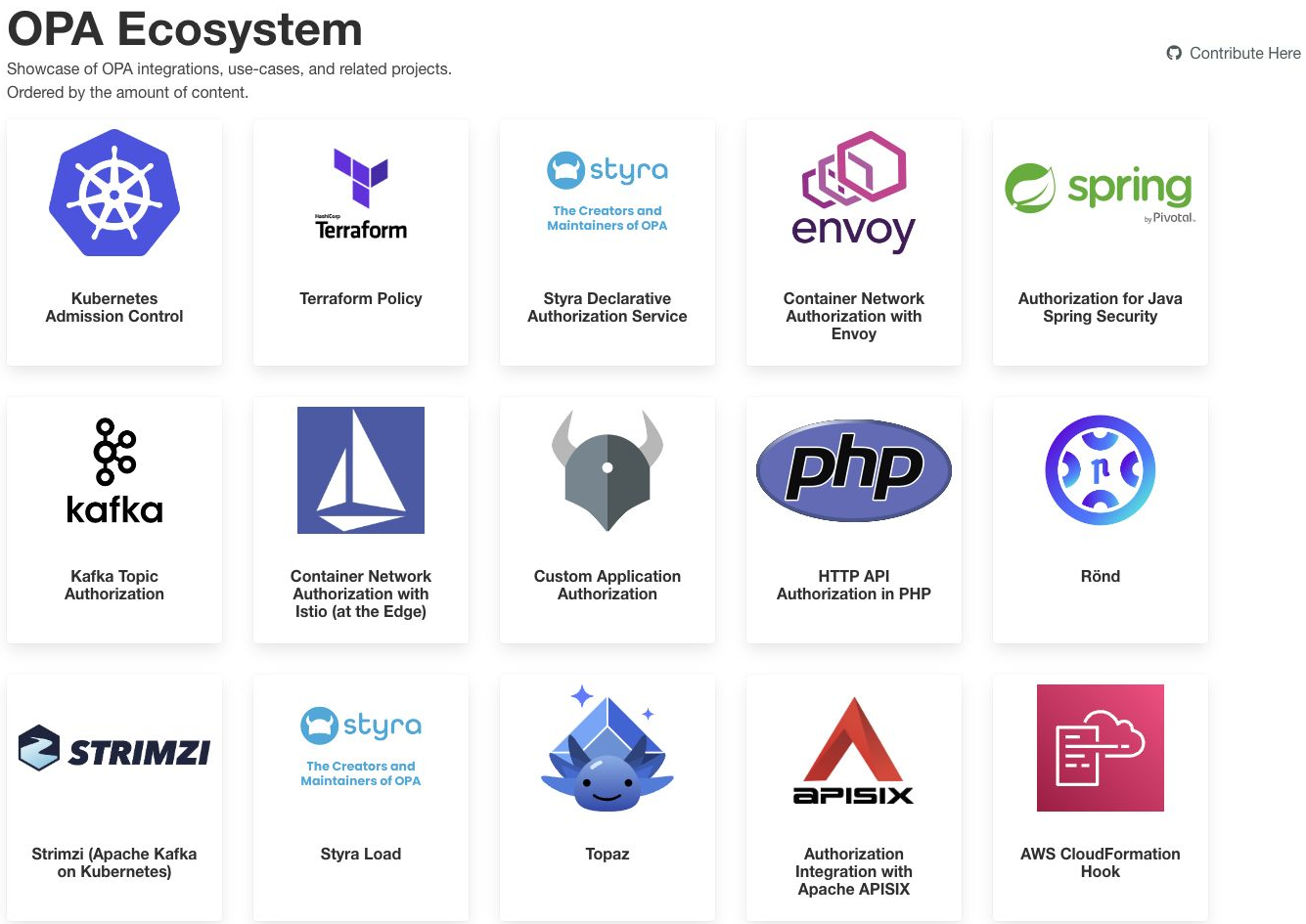


- **General purpose** policy engine
- Graduated CNCF project (2021)
- **Unified** framework for policy-as-code across **all** layers of the stack
- **Decouples** policy from application logic
- Policy written in **declarative** Rego language

# OPA: Community



- **350+** Contributors
- **100+** Integrations
- **8K+** GitHub Stars
- **7K+** Slack Users
- **OPA Gatekeeper**
- **Conftest**
- **Editor plugins**



# OPA: Use Cases

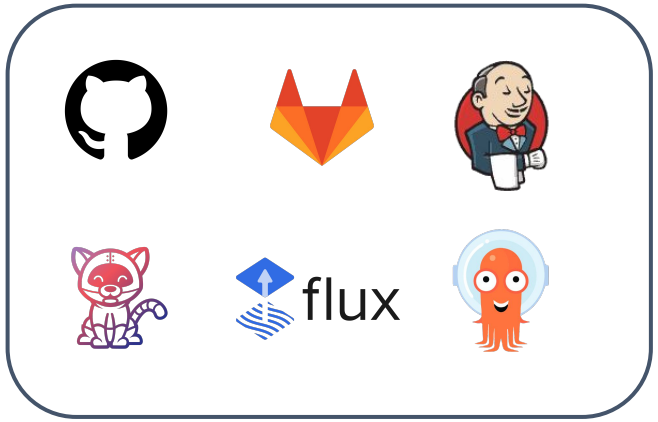


## Application Authorization


## Infrastructure


## Cloud

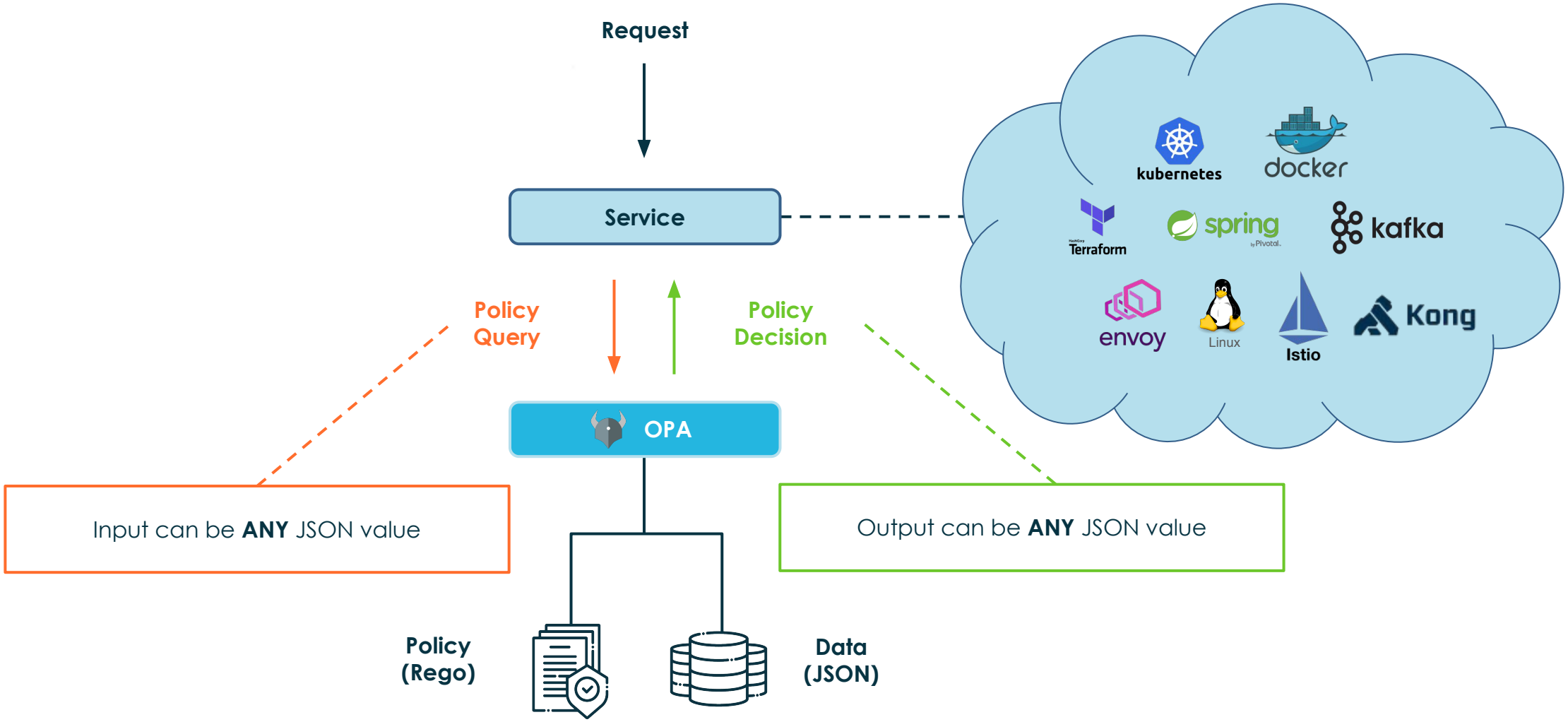

## CI / CD / GitOps




## Data

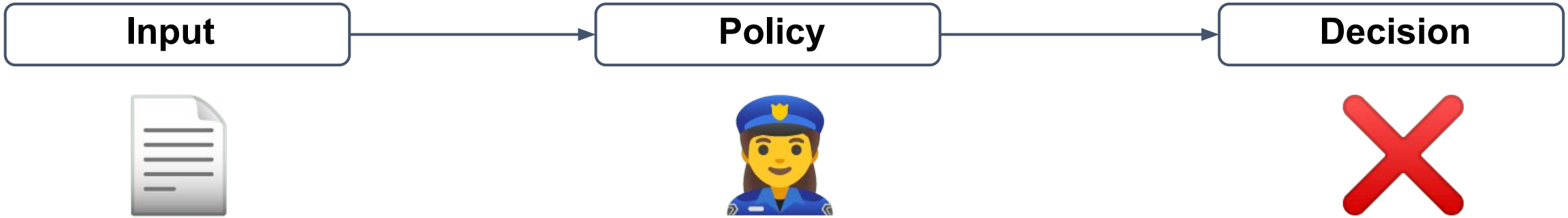
# OPA: Policy Decision Model





# OPA: Rego






```
{
    "user": {
        "name": "anders",
        "roles": [
            "devops",
            "dba"
        ]
    }
}
```

```
package policy

import future.keywords

default allow := false

allow := true if {
    "admin" in input.user.roles
}
```

```
{
    "allow": false
}
```

# EUCS Policy to Policy as Code

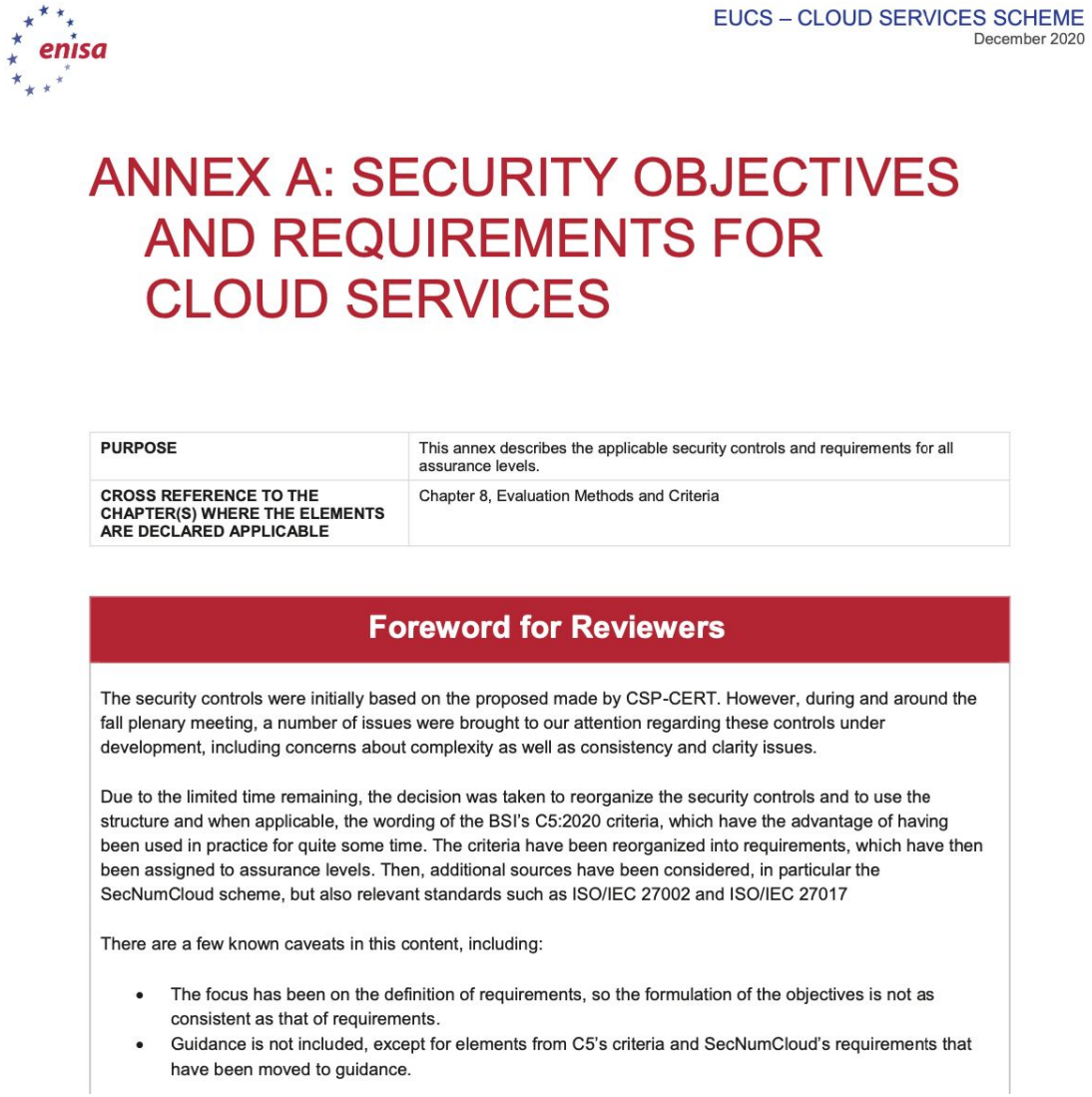


- Annex A lists all **requirements**, along with their assurance level

- 19 categories, including:
  - **Organization of information security**
  - **Information security policies**
  - **Risk & asset management**
  - **Operational security**
  - **Identity, authentication and access control**
  - **Development of information systems**

- **Continuous, automated monitoring, a central theme**

- **This is policy!** Can it be codified?



enisa

EUCS – CLOUD SERVICES SCHEME
December 2020

ANNEX A: SECURITY OBJECTIVES AND REQUIREMENTS FOR CLOUD SERVICES

| | |
|---|---|
| **PURPOSE** | This annex describes the applicable security controls and requirements for all assurance levels. |
| **CROSS REFERENCE TO THE CHAPTER(S) WHERE THE ELEMENTS ARE DECLARED APPLICABLE** | Chapter 8, Evaluation Methods and Criteria |

**Foreword for Reviewers**

The security controls were initially based on the proposed made by CSP-CERT. However, during and around the fall plenary meeting, a number of issues were brought to our attention regarding these controls under development, including concerns about complexity as well as consistency and clarity issues.

Due to the limited time remaining, the decision was taken to reorganize the security controls and to use the structure and when applicable, the wording of the BSI's C5:2020 criteria, which have the advantage of having been used in practice for quite some time. The criteria have been reorganized into requirements, which have then been assigned to assurance levels. Then, additional sources have been considered, in particular the SecNumCloud scheme, but also relevant standards such as ISO/IEC 27002 and ISO/IEC 27017

There are a few known caveats in this content, including:

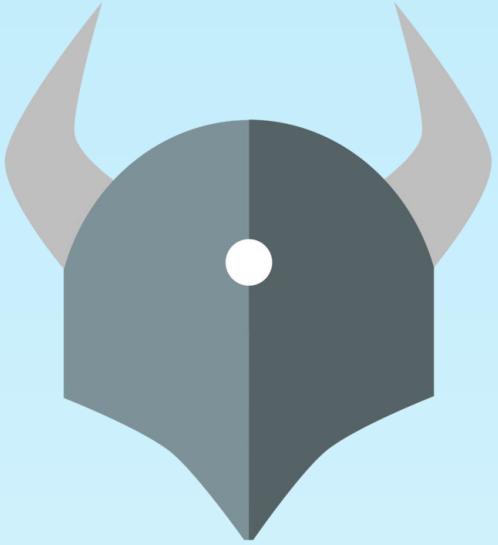
- The focus has been on the definition of requirements, so the formulation of the objectives is not as consistent as that of requirements.
- Guidance is not included, except for elements from C5's criteria and SecNumCloud's requirements that have been moved to guidance.

# OSCAL (Open Security Controls Assessment Language)



- Compliance as “code” (JSON / YAML / XML)
- Three different “layers” (schemas)
  - **Control** layer: describes the **requirements**
  - **Implementation** layer: describes the implementation of the requirements — hardware, software, service, policy, etc..
  - **Assessment** layer: describes **how to assess compliance**, as well as a format for **assessment results**
- **No more PDFs!** Automate everything. Exchange requirements, implementations and assessments across systems.
- OSCAL + Rego = ❤️
  - Use OPA for “policy on policy” enforcement
  - Use OSCAL to build Rego rules — and OPA to generate OSCAL artifacts
  - Continuous compliance!

```yaml
- id: s2
  title: Access control
  props:
    - name: label
      value: "2"
  groups:
    - id: s2.1
      title: Business requirements of access control
      props:
        - name: label
          value: "2.1"
      parts:
        - id: s2.1_smt
          name: objective
          prose: To limit access to information and information processing facilities.
      controls:
        - id: s2.1.1
          title: Access control policy
          props:
            - name: label
              value: 2.1.1
          parts:
            - id: s2.1.1_stm
              name: statement
              prose: An access control policy should be established, documented
                and reviewed based on business and information security requirements.
            - id: s2.1.1_gdn
              name: guidance
              parts:
                - id: s2.1.1_gdn.1
                  name: item
                  prose: Asset owners should determine appropriate access control
                    rules, access rights and restrictions for specific user roles
```



KubeCon | CloudNativeCon

Europe 2023

# Asset Management

# EUCS Policy to OPA Policy



## AM-05 ASSET CLASSIFICATION AND LABELLING

**Objective:** Assets are classified and, if possible, labelled. Classification and labelling of an asset reflect the protection needs of the information it processes, stores, or transmits.

| Ref | Description | Assurance Level |
|---|---|---|
| **AM-05.1** | The CSP shall define an asset classification schema that reflects for each asset the protection needs of the information it processes, stores, or transmits | **Basic** |
| **AM-05.2** | The asset classification schema shall provide levels of protection for the confidentiality, integrity, availability, and authenticity protection objectives | **Substantial** |
| **AM-05.3** | When applicable, the CSP shall label all assets according to their classification in the asset classification schema | **Basic** |
| **AM-05.4** | The need for protection shall be determined by the individuals or groups responsible for the assets | **Substantial** |

# EUCS Policy to OPA Policy



| Ref | Description | Assurance Level |
|---|---|---|
| **AM-05.1** | **The CSP shall define an asset classification schema** that reflects for each asset the protection needs of the information it processes, stores, or transmits | **Basic** |
| **AM-05.2** | The asset classification schema shall provide levels of protection for the **confidentiality, integrity, availability, and authenticity protection objectives** | **Substantial** |

```
{
    "classification": {
        "availability": {
            "options": [
                "critical",
                "high",
                "low"
            ]
        },
        "confidentility": {
            "options": [
                "internal",
                "private",
                "public"
            ]
        }
    }
}
```

# EUCS Policy to OPA Policy



| Ref | Description | Assurance Level |
|---|---|---|
| **AM-05.3** | When applicable, the CSP shall **label all assets according to their classification** in the asset classification schema | **Basic** |

**Kubernetes Admission Control**

https://play.openpolicyagent.org/p/YruadzkMNP

**AWS CloudFormation**

https://play.openpolicyagent.org/p/iSfpj2rdZZ

# EUCS Policy to OPA Policy



| Ref | Description | Assurance Level |
|---|---|---|
| AM-05.4 | The need for protection shall be determined by the individuals or groups responsible for the assets | Substantial |

```
curl -L \
  -H "Accept: application/vnd.github+json" \
  -H "Authorization: Bearer $GITHUB_TOKEN"\
  -H "X-GitHub-Api-Version: 2022-11-28" \
  "https://api.github.com/repos/acmecorp/infrastructure/pulls/123"
```

```
"teams": {
    "platform": {
        "members": [
            "anderseknert",
            "johanfylling",
            "charlieegan3"
        ]
    },
    "dev-1": {
        "members": [
```

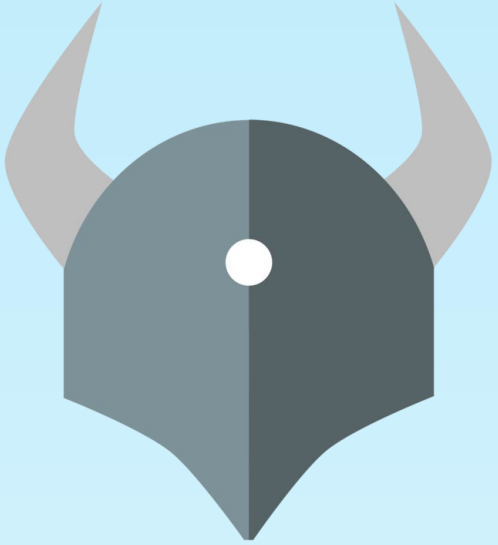
What team are they in?

Who's making the change?

```
{
    "url": "https://api.github.com/repos/acmecorp/infrastructure/pulls/123",
    "html_url": "https://github.com/acmecorp/infrastructure/pull/123",
    "number": 123,
    "state": "open",
    "title": "Change the owner of bucket",
    "user": {
        "login": "anderseknert",
        "html_url": "https://github.com/anderseknert"
    }
}
```

Allow if owner label matches team belonging

```
allow if input.pr.username in data.teams[labels.owner].members
```



KubeCon | CloudNativeCon

Europe 2023

# Management Capabilities

# OPA: Management



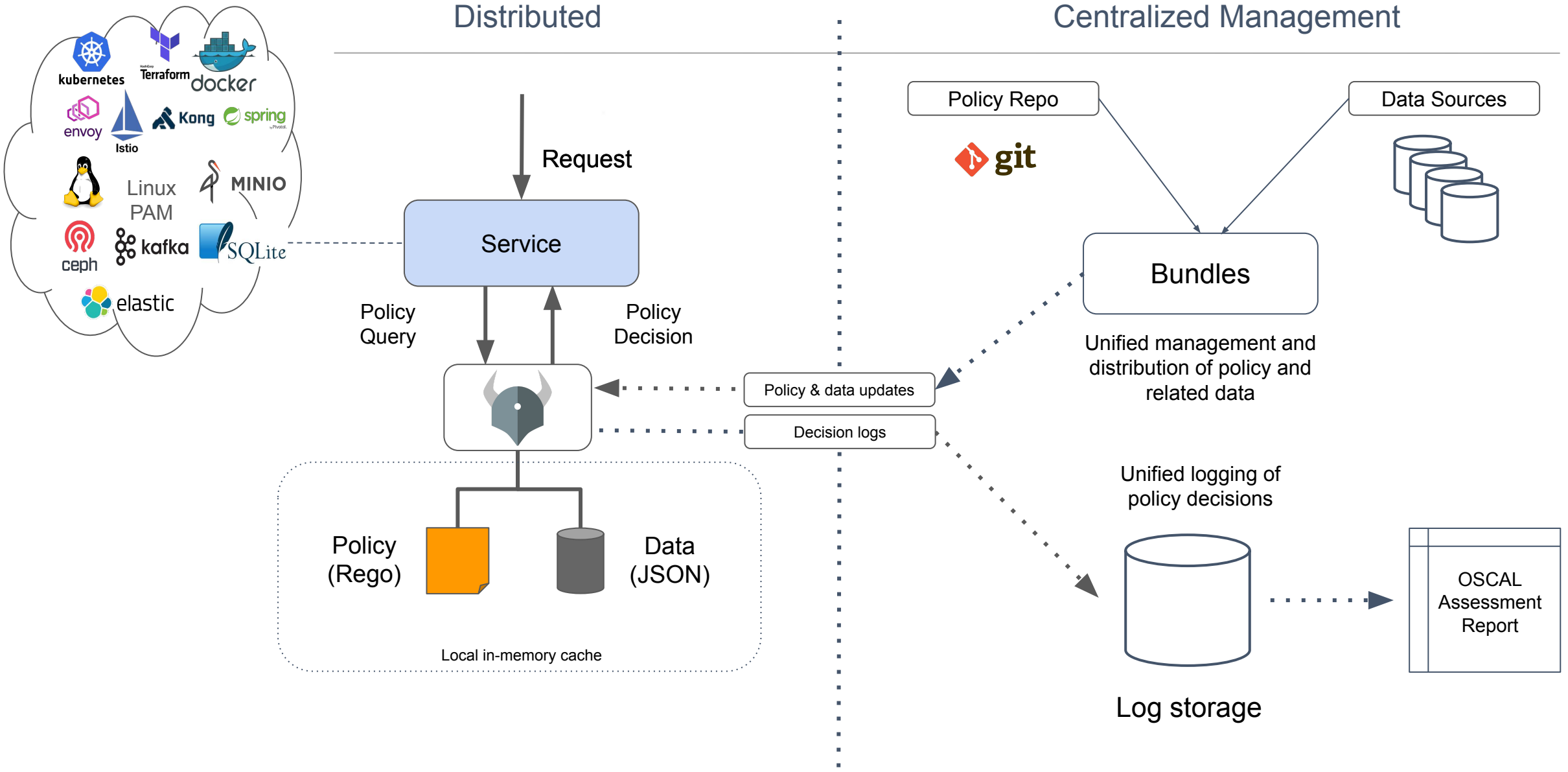
- OPA a **distributed** component, 100's or 1000's of instances

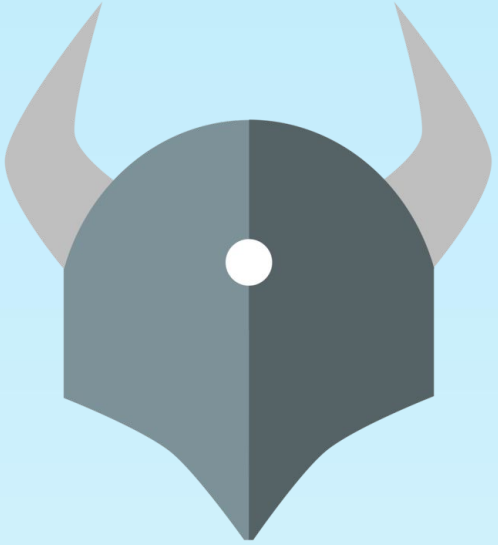
- OPA's management capabilities allow **centralized** control
  - Bundle (policy and data) **distribution**
  - Decision **logging**
  - Configuration
  - Status and health reports

- **Less places to look = simplified auditing!**

# OPA: Distributed vs Centralized







KubeCon | CloudNativeCon

Europe 2023

# Access Control

# EUCS Access Control



## Access control an important aspect of EUCS

- IAM-04 MANAGEMENT OF ACCESS RIGHTS
- IAM-05 REGULAR REVIEW OF ACCESS RIGHTS
- IAM-06 PRIVILEGED ACCESS RIGHTS
- IAM-09 GENERAL ACCESS RESTRICTIONS

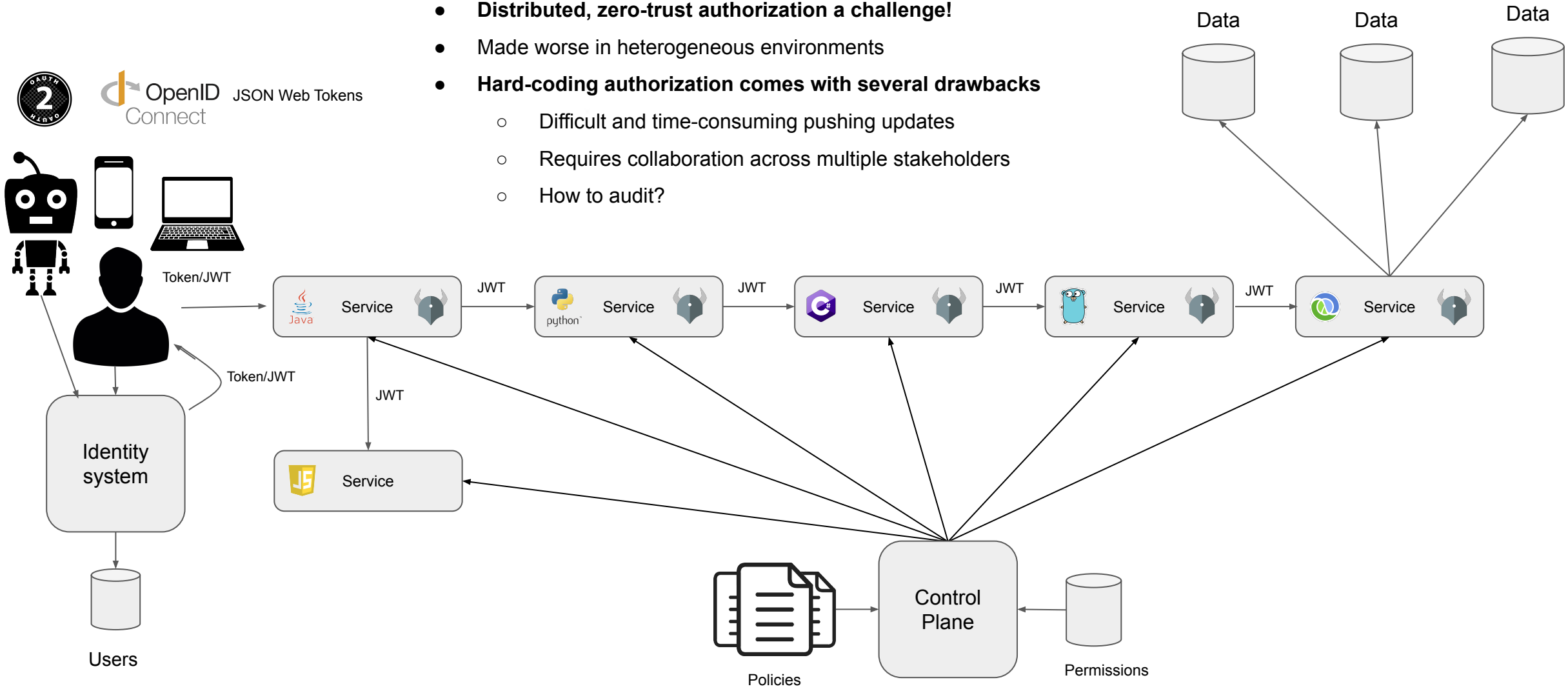
## The decoupled model of OPA provides much of this for “free”

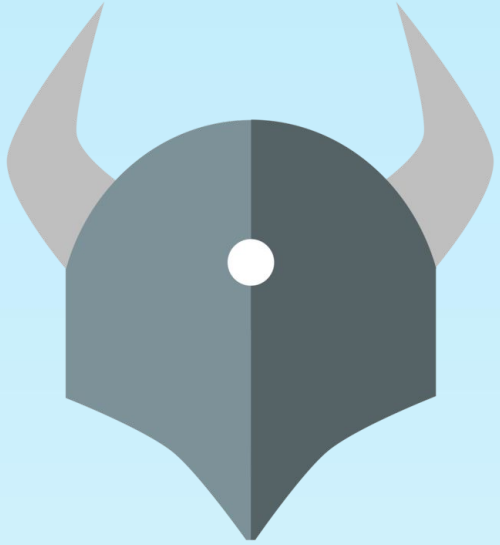
- Centralized management (policy authoring, storage, distribution)
- Review of access made easy by decoupling policy from application logic
- Unified policy language, management systems and logging simplify auditing

# EUCS Access Control and OPA



- **Distributed, zero-trust authorization a challenge!**
- Made worse in heterogeneous environments
- **Hard-coding authorization comes with several drawbacks**
  - Difficult and time-consuming pushing updates
  - Requires collaboration across multiple stakeholders
  - How to audit?





KubeCon | CloudNativeCon

Europe 2023

# Kubernetes Admission Control — Examples

# EUCS Kubernetes Admission Control



| Control ID | Name | Description (shortened) | Rego Policy |
|---|---|---|---|
| ISP-03.1 | Maintain Exception List | The CSP shall maintain a list of exceptions to the security policies and procedures. | Validate resources using allow-list of approval labels or annotations for exceptions. |
| ISP-03.2 | Time Limited Exceptions | The exceptions are limited in time. | Scheduled check of .metadata.creationTimestamp against time limit for any resource marked as exception. |
| OIS-04.2 | Risk Assessment | The CSP shall perform a risk assessment to assess and treat the risks on any project. | Allow/deny based on labels, or advanced policy to calculate risk dynamically based on multiple factors. |
| RM-02.2 | Risk Assessment Dissemination | The CSP shall make the results of the risk assessment available to relevant stakeholders. | Decision logging including provided input (i.e. the resource) and the result. |
| AM-01.2 | Support Automated Inventory | The inventory shall be performed automatically and/or by the people or teams responsible for the assets. | Validate tags on all resources. Optionally use mutating policy for automated tagging. |
| OIS-02.3 | Risk Mitigation | The CSP shall implement the mitigating measures defined in the risk assessment, privileging separation of duties. | Validating policy for creation and updates on all RBAC resources. |

# OPA and EUCS



## Applicable

- A.1 Organization of information security
- A.2 Information security policies
- A.3 Risk management
- A.5 Asset management
- A.7 Operational security
- A.8 Identity, authentication and access control management
- A.12 Change and configuration management
- A.13 Development of information systems
- A.20 Product safety and security

## Not (Directly) Applicable

- A.4 Human resources
- A.6 Physical security
- A.9 Cryptography and key management
- A.10 Communication security
- A.14 Procurement management
- A.15 Incident management
- A.16 Business continuity
- A.17 Compliance (legal)
- A.18 Documentation
- A.19 Investigation requests from governments

# Summary



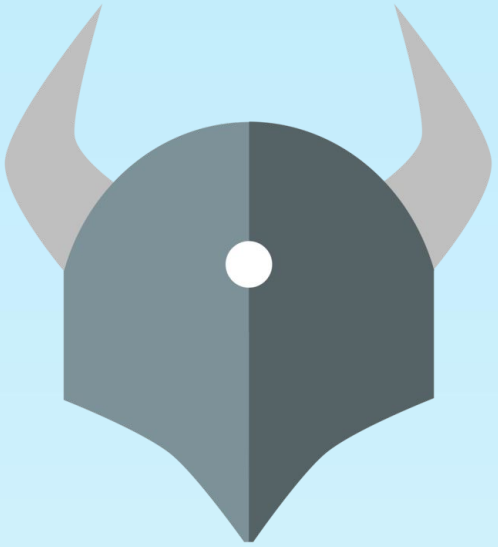
- **EUCS —** reference set of **security requirements**
- **Continuous compliance** and **automation** is key to certification
- **MEDINA** Project — tools, techniques, and processes for auditing, automation and certification
- **OSCAL** allows working with requirements, implementations & assessments as “code”
- **OPA** provides a unified way of turning requirements into enforceable policy across the entire stack

# Learn More About EUCS and OPA

KubeCon CloudNativeCon Europe 2023

| | |
|---|---|
| **EU Cybersecurity mini-site** | https://certification.enisa.europa.eu/ |
| **EUCS (with downloadable PDF)** | https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme |
| **EURACTIV articles on EUCS** | https://www.euractiv.com/topics/eucs/ |
| **MEDINA project** | https://medina-project.eu/ |
| **Open Policy Agent** | https://www.openpolicyagent.org/ |
| **Rego Playground** | https://play.openpolicyagent.org/ |
| **Styra Academy** | https://academy.styra.com/ |

Questions on EUCS, Legal, Compliance and K8s mapping - Robert Ficcaglia on Slack
CNCF #tag-security-public-sector  Kubernetes #wg-policy



KubeCon | CloudNativeCon

Europe 2023

# Thank you!