



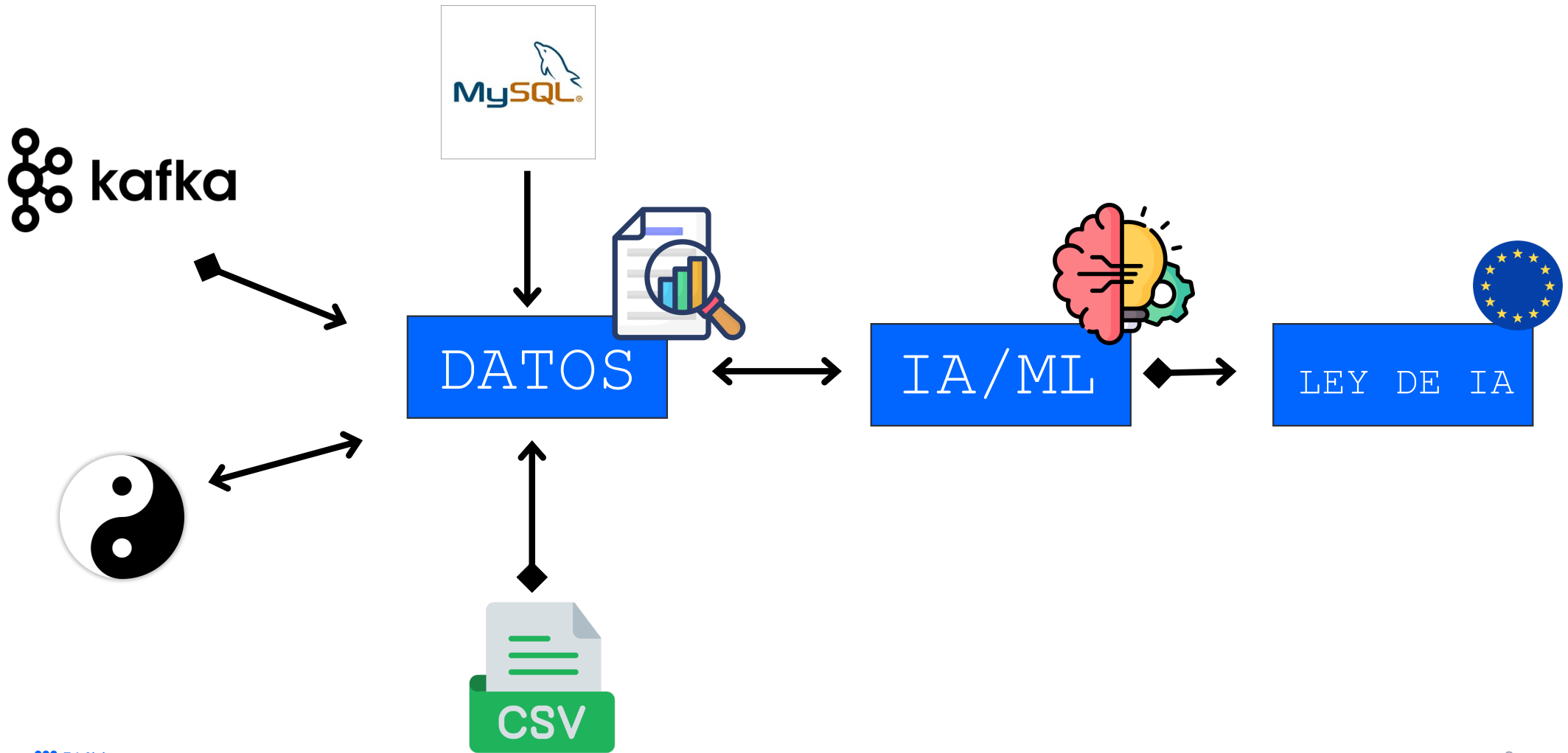
Telefónica
Innovación Digital

Reforzando la gobernanza de la infraestructura de datos

Lucía Cabanillas Rodríguez



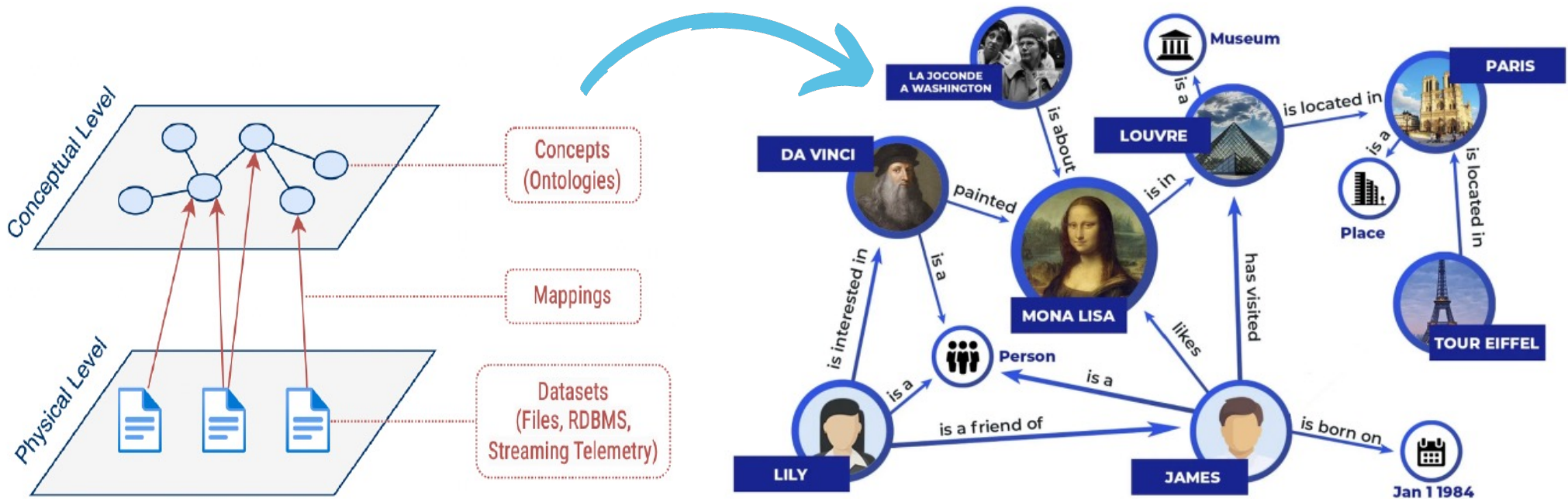
Los desafíos de la IA



Knowledges graphs

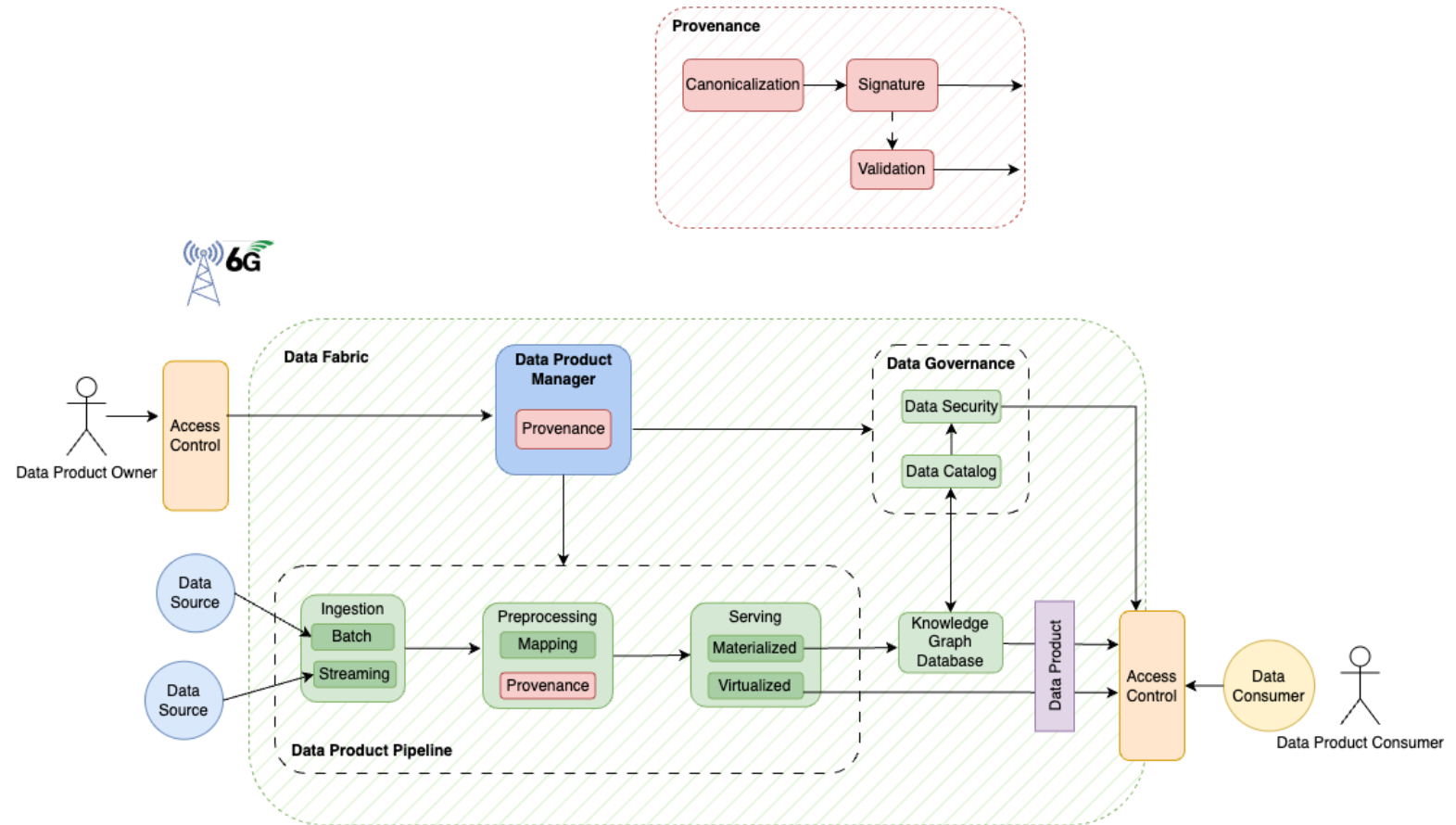
Knowledge graphs:

- Representación de conceptos relacionados con otros conceptos
- Captura explícita del conocimiento con ontologías y anotación semántica



Data Fabric

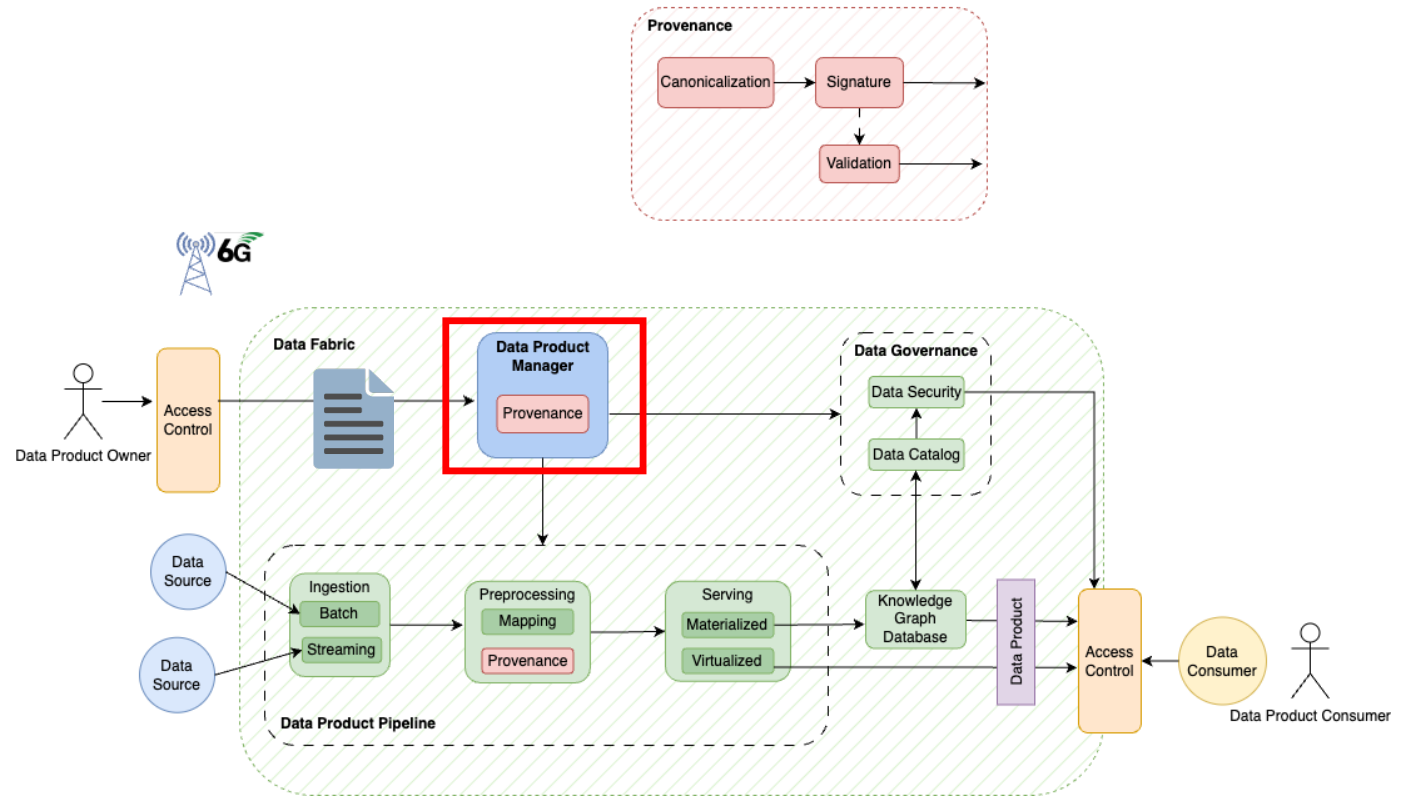
- Basado en normas acordadas para la interoperabilidad
- De los datos brutos a un producto de datos
- Diferentes flujos en función de los requisitos del producto de datos



Data Fabric

Data Product Manager:

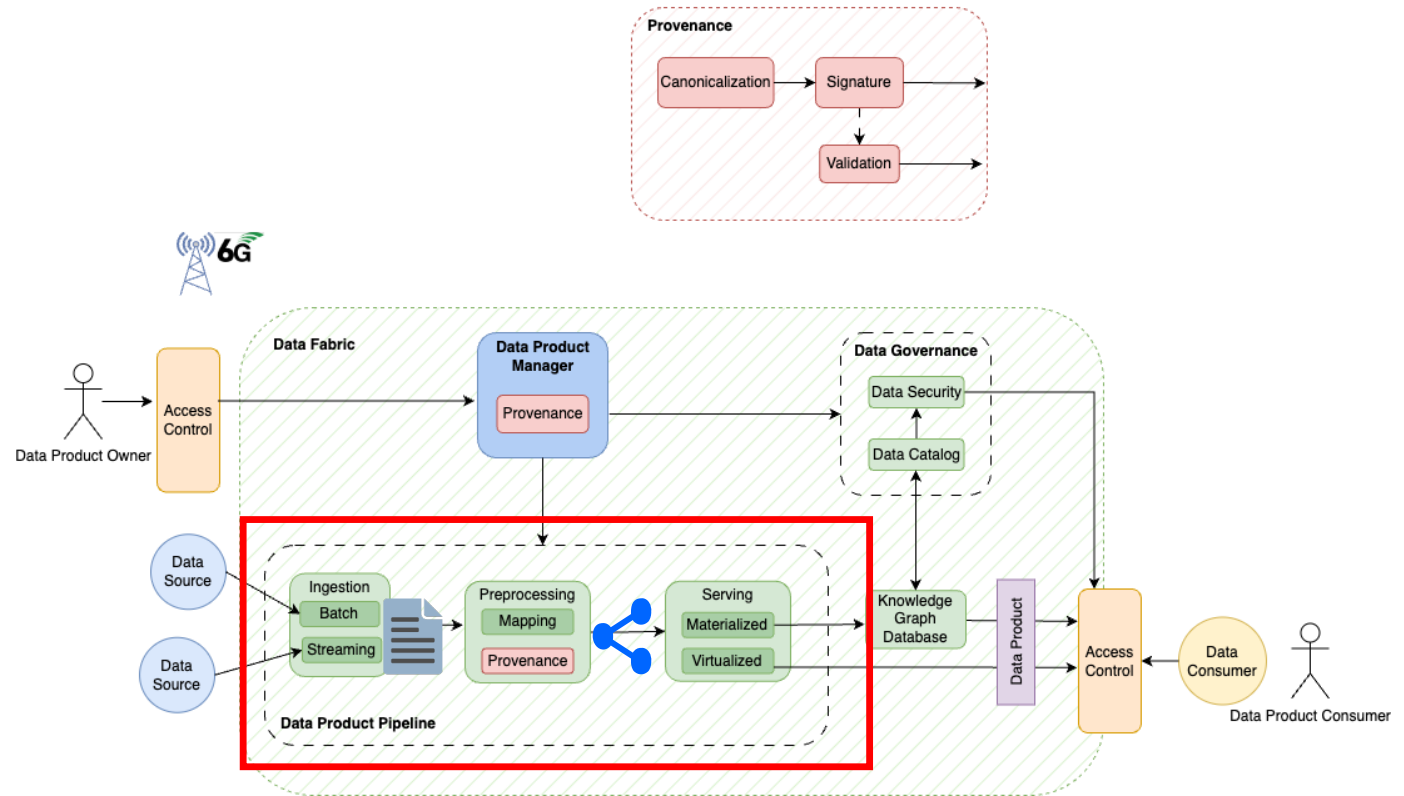
- Incorporación y registro de productos de datos
- Organiza la canalización de los productos de datos
- Se coordina con los componentes Data Catalog y Data Security para controlar los nuevos productos de datos.



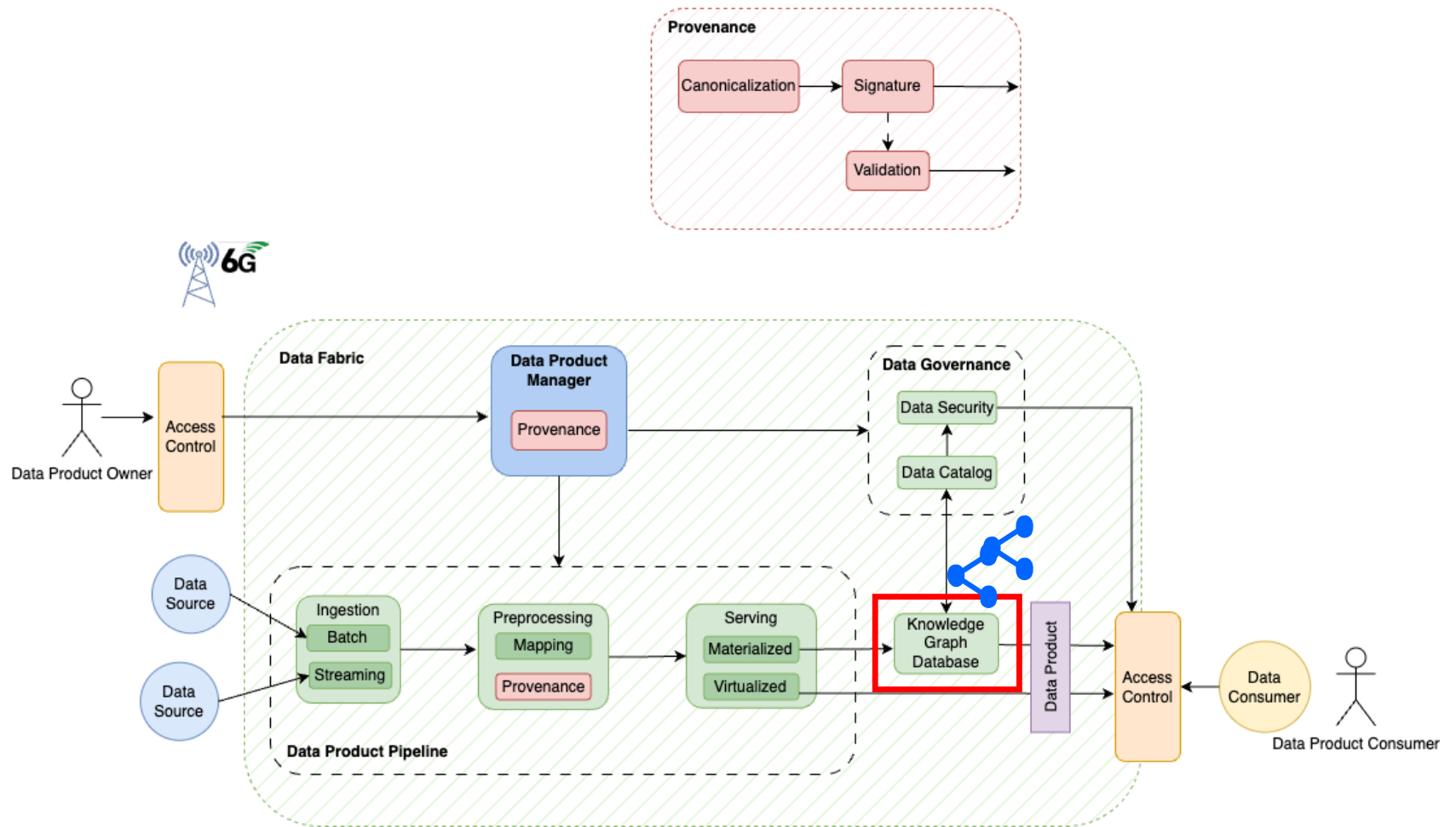
Data Fabric

Data Product Pipeline:

Canal de datos que transforma conjuntos de datos brutos en productos de datos semánticos interoperables que pasan a formar parte del grafo de conocimiento



Data Fabric



Data Fabric

Data Catalog:

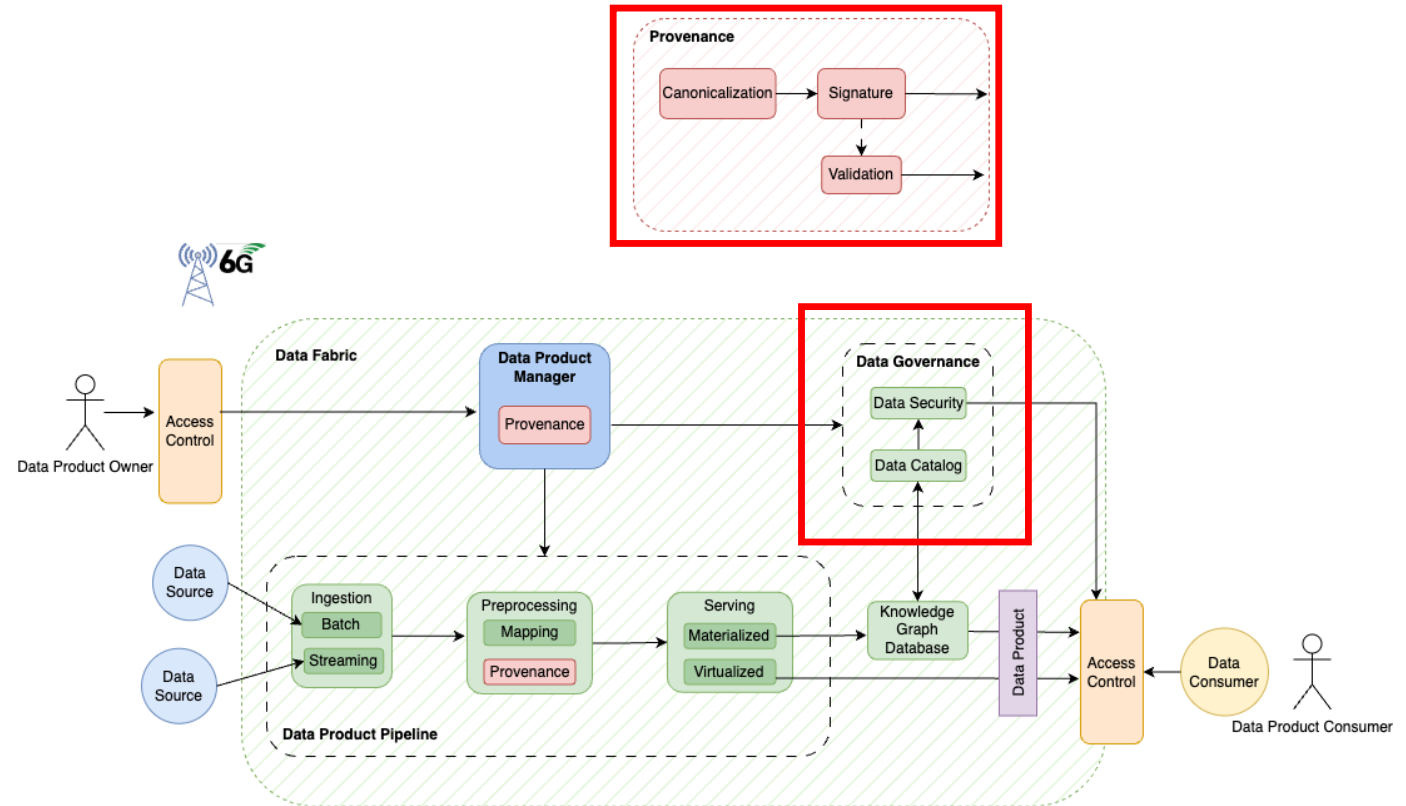
- Herramienta para organizar y encontrar los datos disponibles

Data Security:

- Aplica políticas de control de acceso para nuevos productos de datos basadas en los requisitos de seguridad indicados por el propietario

Provenance:

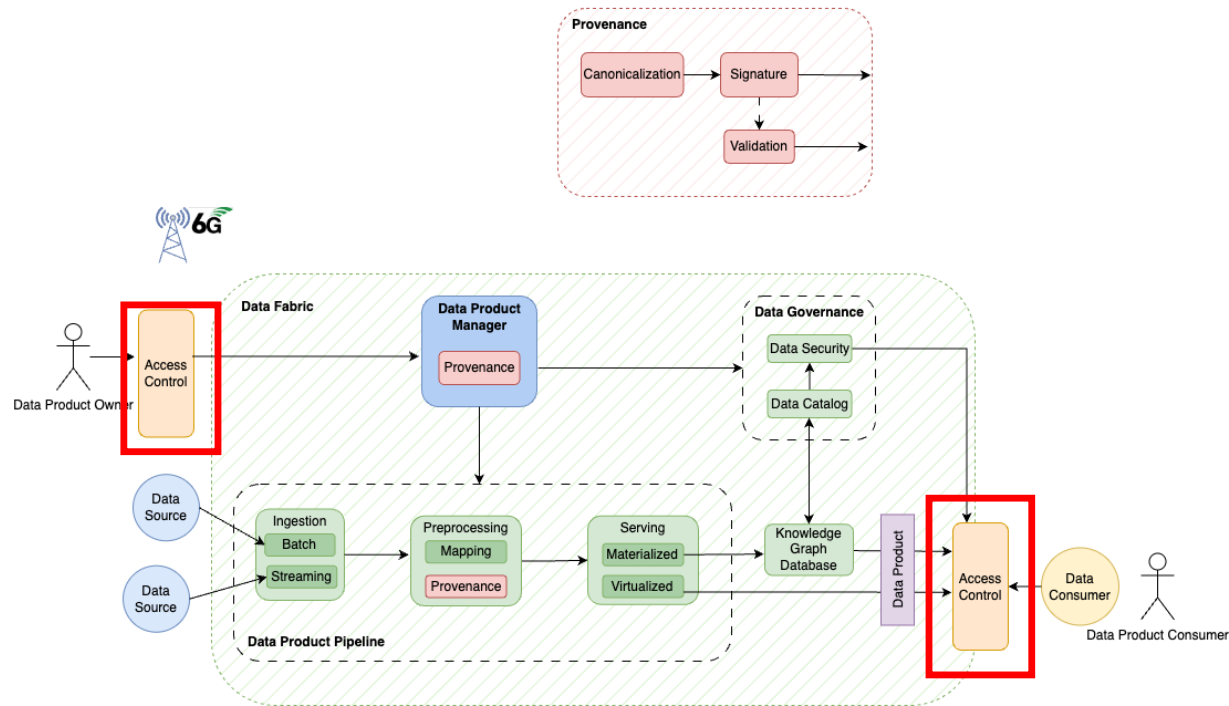
- Aplica una firma para asegurar el origen y la integridad de los datos



Data Fabric



Acceso no autorizado: Un fallo en los mecanismos de control de acceso podría permitir a un atacante hacerse pasar por un usuario con privilegios elevados, lo que daría lugar a la ingestión de datos contaminados u obtener acceso no autorizado a los datos almacenados

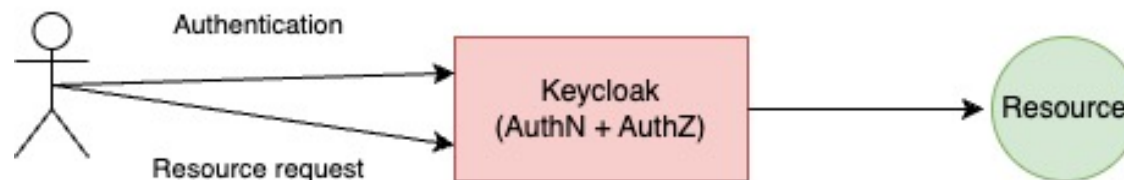


Access Control



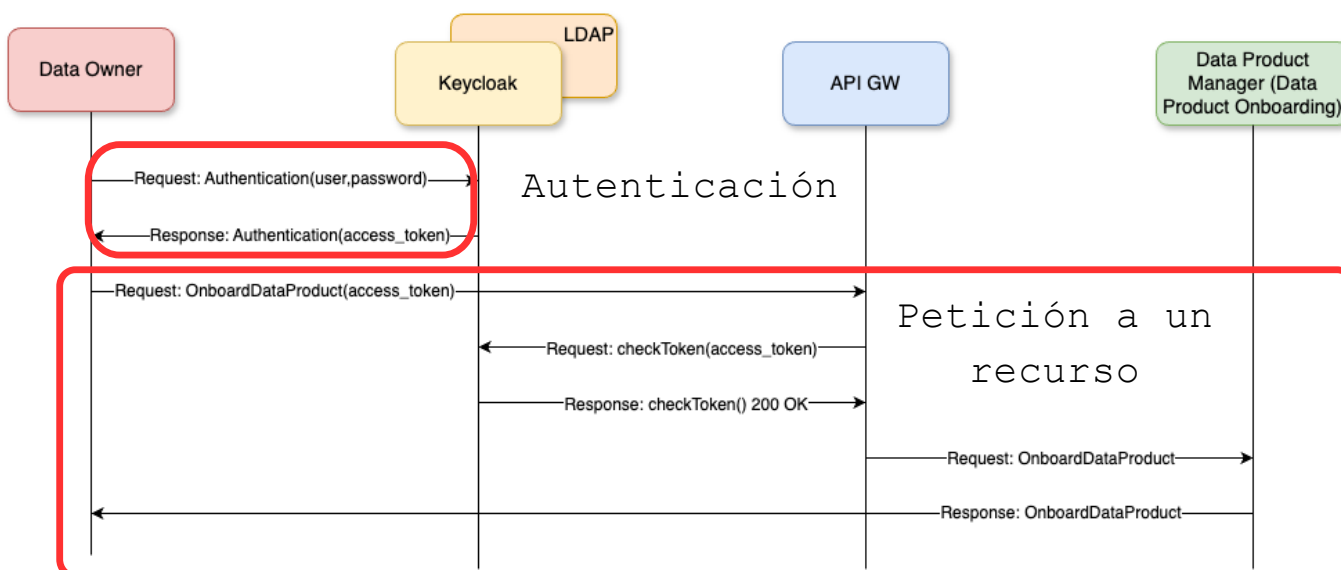
Keycloak es un gestor de acceso e identidad de código abierto

- Basado en OAuth 2.0 y OpenID Connect
- Keycloak puede conectarse a servidores LDAP y Active Directory existentes



Keycloak soporta políticas de **autorización** y es capaz de combinar diferentes mecanismos de control de acceso:

- Control de acceso basado en atributos (ABAC)
- Control de acceso basado en roles (RBAC)
- Control de acceso basado en usuarios (UBAC)
- Control de acceso basado en el contexto (CBAC)



Access Control

PEP Policy Enforcement Point

- Solicita y aplica las decisiones de política

PDP Policy Decision Point

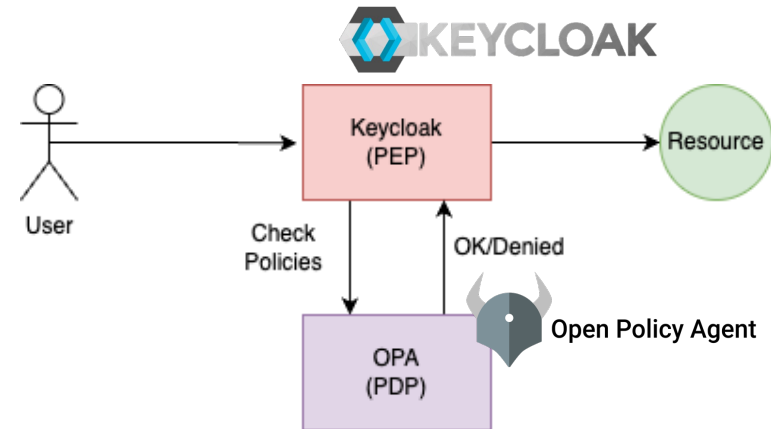
- Evalúa la política a partir de la solicitud



Open Policy Agent

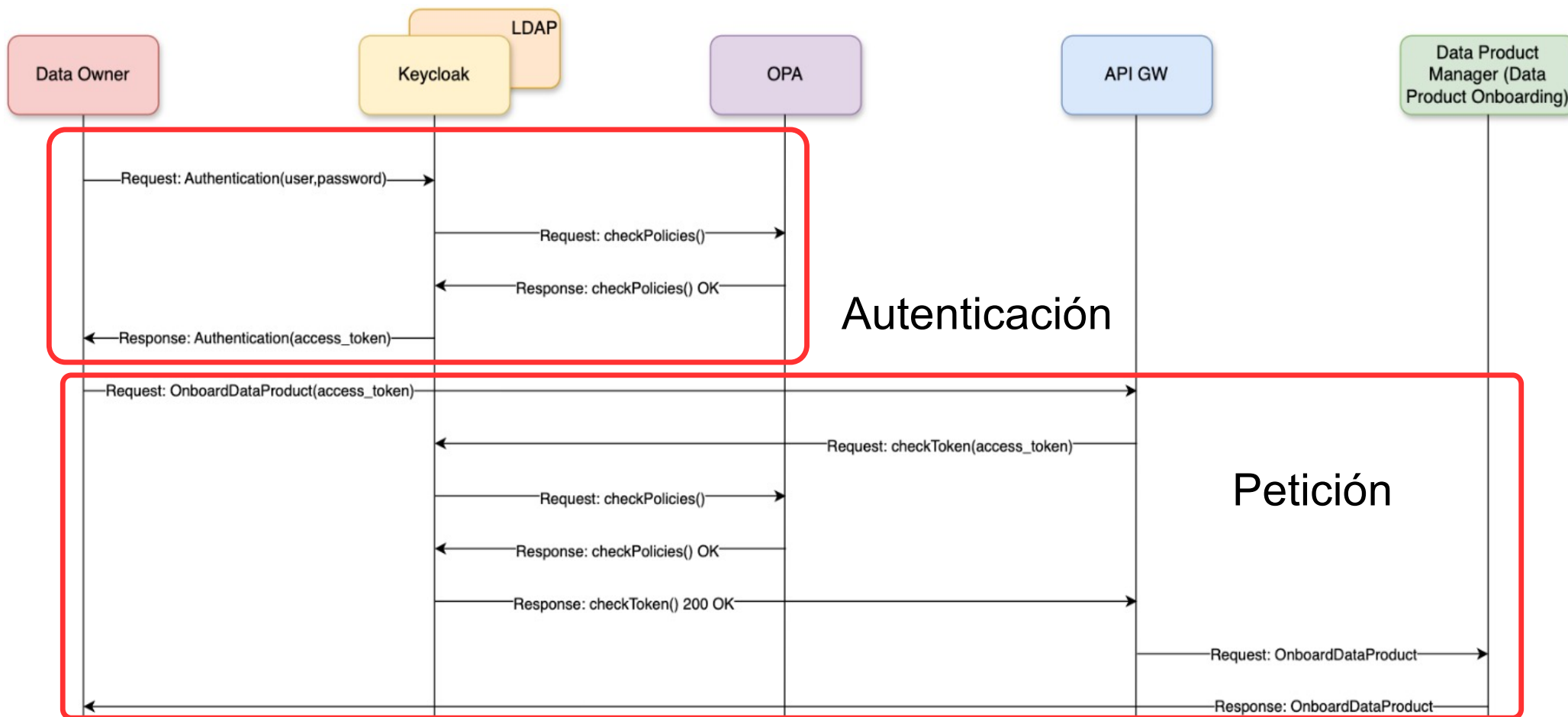
Open Policy Agent

- Evalúa políticas, valida, soporta Pull / Push
- Desarrollado bajo los auspicios del CNCF
- “Policy as Code”
- Permisos detallados

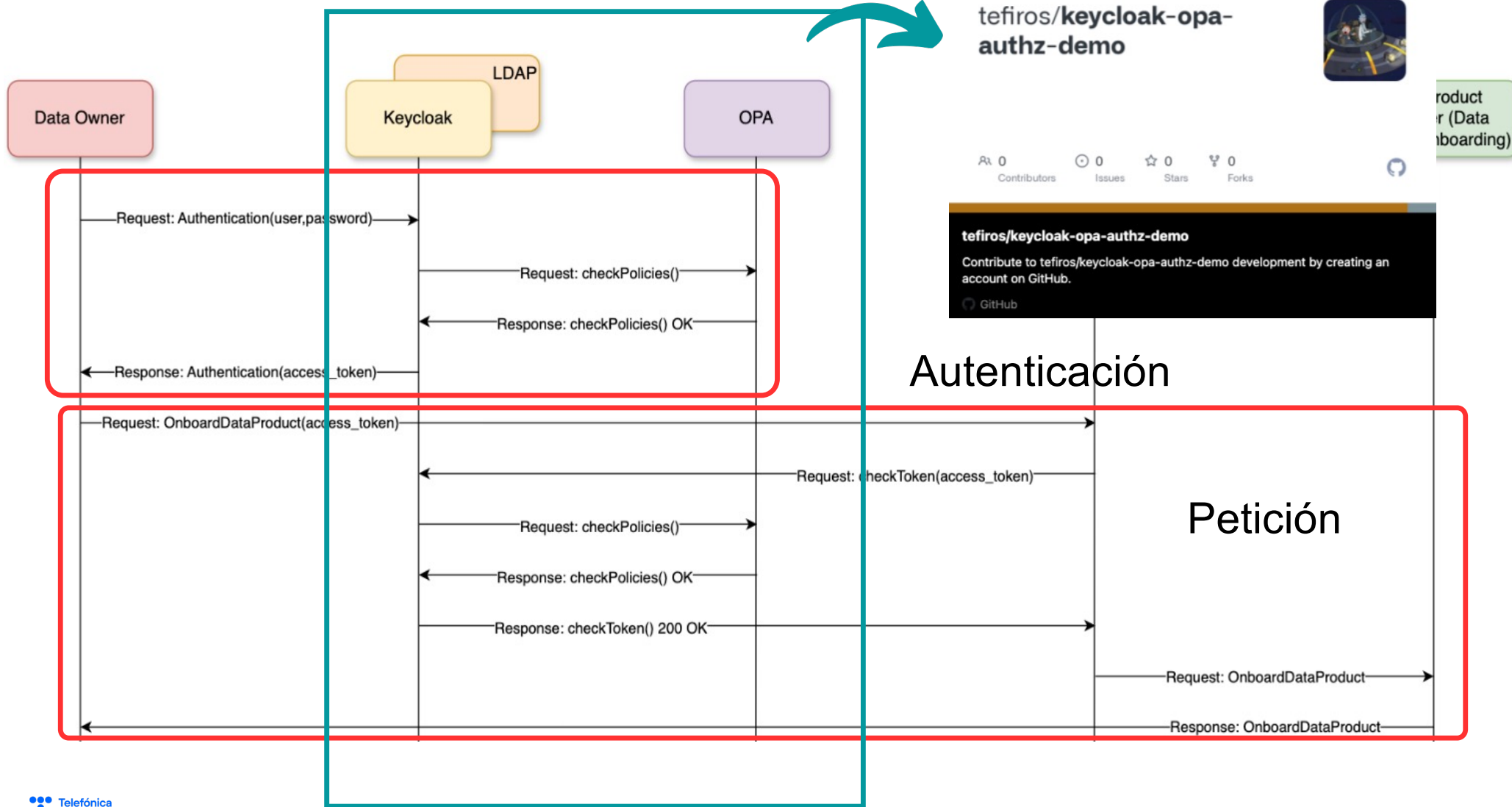


```
}
| # By default, deny requests.
| default allow := false
|
|
| # Allow admins to do anything.
| allow if user_is_admin
|
| # user_is_admin is true if "admin" is among the user's roles as per data.user_roles
| user_is_admin if "admin" in data.user_roles[input.user]
|
|
| # user_is_admin is true if "admin" is among the user's roles as per data.user_roles
```

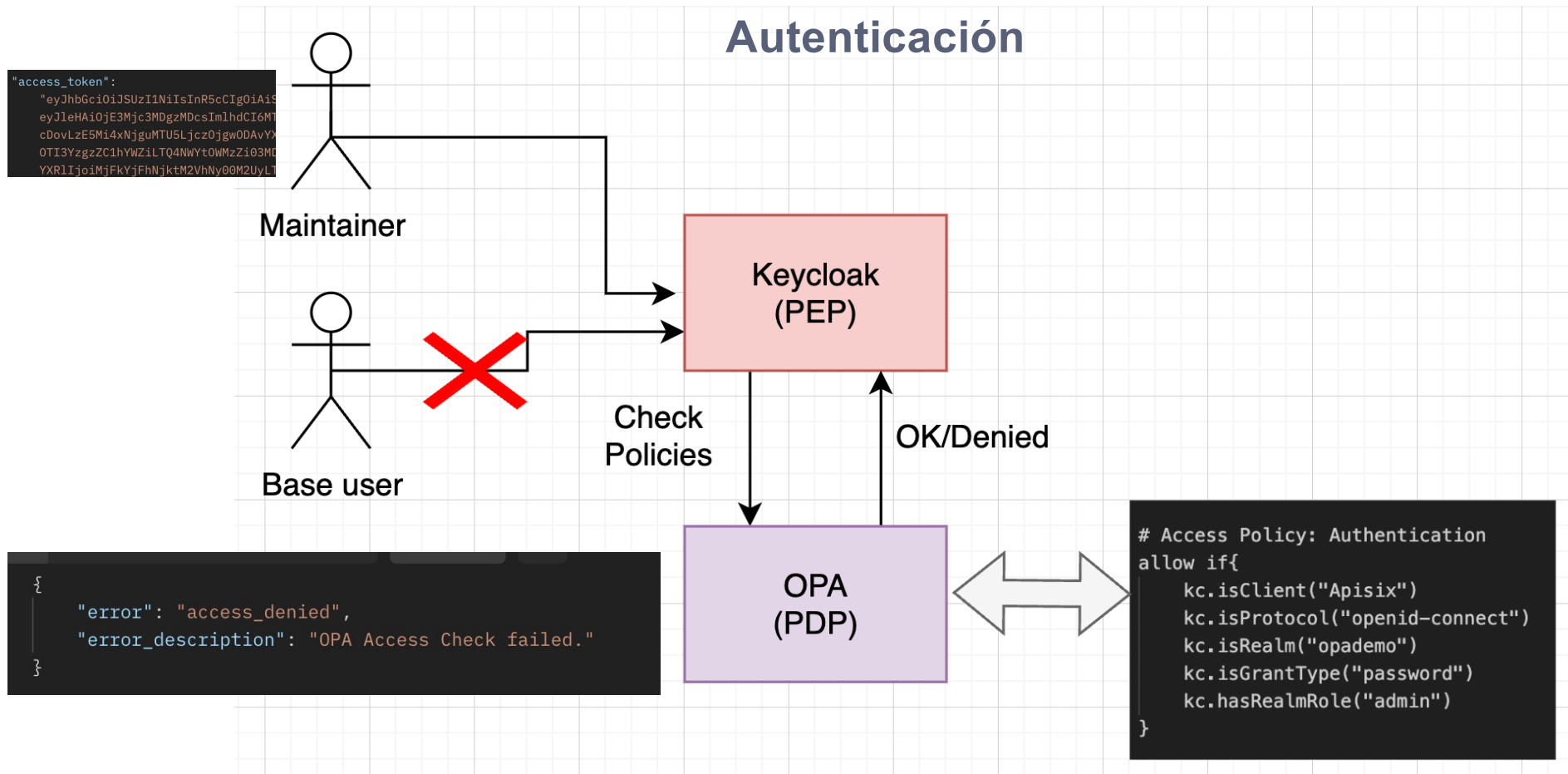
Access Control



Access Control

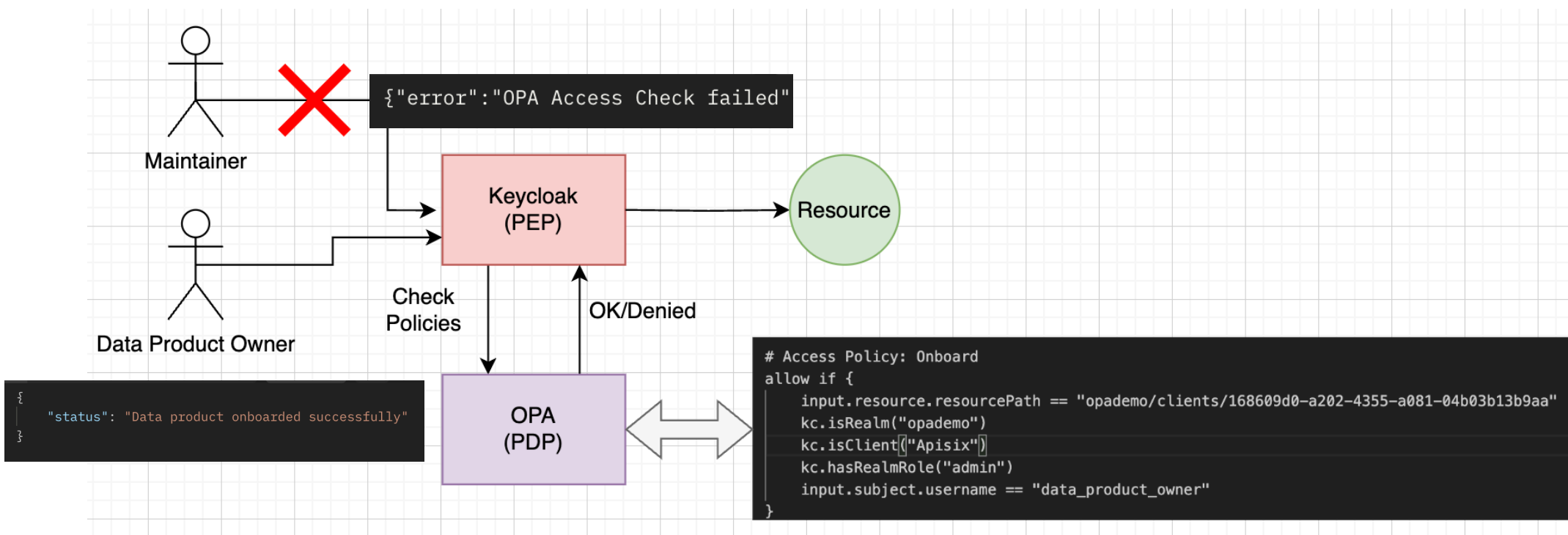


Access Control



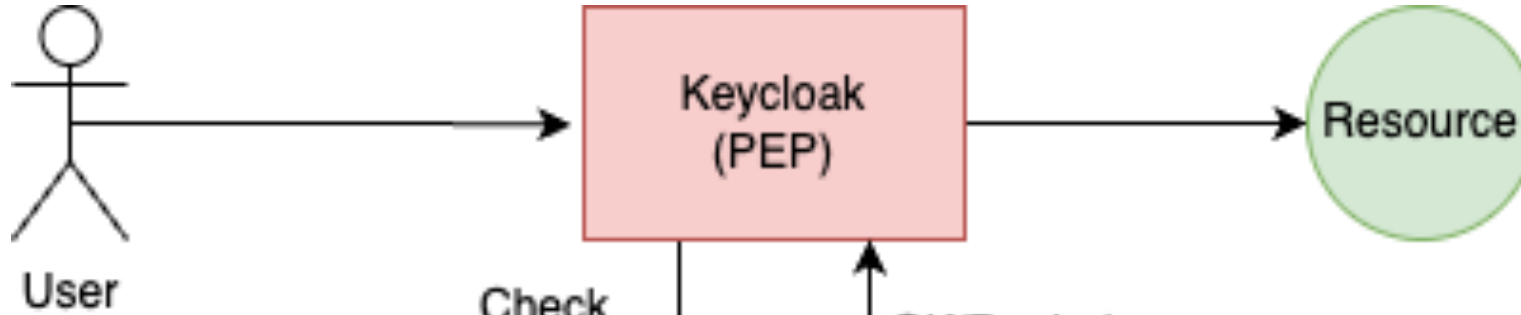
Access Control

Petición a un recurso



Access Control

Trazabilidad



```

 : {
  "subject" : {
    "id" : "789b2441-d3ce-4e9a-8043-989a9b633b24",
    "username" : "data_product_owner",
    "realmRoles" : [ "admin", "default-roles-opademo", "offline_access", "uma_authorization" ],
    "clientRoles" : [ "realm-management:view-users", "realm-management:query-users", "realm-man-
account:manage-account", "account:manage-account-links" ],
    "attributes" : {
      "emailVerified" : false
    }
  },
  "resource" : {
    "realm" : "opademo",
    "clientId" : "DataProductManager",
    "resourceId" : "06753737-7213-402b-a61d-77994335d07e",
    "resourceType" : "client",
    "resourcePath" : "opademo/clients/06753737-7213-402b-a61d-77994335d07e",
    "resourceName" : "DataProductManager"
  },
  "context" : {
    "attributes" : {
      "grantType" : "urn:ietf:params:oauth:grant-type:uma-ticket",
      "remoteAddress" : "192.168.159.228"
    },
    "headers" : {
      "Authorization" : "Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXLTZGRkMDQ0NjAwMjMlIiwiaXNjaW50UG5JQmsI
GMTcyZzQwODE4MiwianRpIjoiaHR0cDovLzE5OTY0MjY0LmVudC9kIiwiaWF0Ij0iIiwiaXNjaW50UG5JQmsIiwiaXNjaW50UG5JQmsI
E3M00Yj01LWJlYXkiOiJFMTI3IiwiaWF0Ij0iIiwiaXNjaW50UG5JQmsIiwiaXNjaW50UG5JQmsIiwiaXNjaW50UG5JQmsI
1pb1IsInVtYV9hdXR0b3JpemF0aW9uIiwiaWF0Ij0iIiwiaXNjaW50UG5JQmsIiwiaXNjaW50UG5JQmsIiwiaXNjaW50UG5JQmsI
JhY2NvdW50IiwiaWF0Ij0iIiwiaXNjaW50UG5JQmsIiwiaXNjaW50UG5JQmsIiwiaXNjaW50UG5JQmsIiwiaXNjaW50UG5JQmsI
1iMwIiwiaWF0Ij0iIiwiaXNjaW50UG5JQmsIiwiaXNjaW50UG5JQmsIiwiaXNjaW50UG5JQmsIiwiaXNjaW50UG5JQmsI
5fbmFtZSI6ImRhdGFfchJvZHVhdF9vd25lc1IsImZhbnVseV9uYV1IiwiaWF0Ij0iIiwiaXNjaW50UG5JQmsIiwiaXNjaW50UG5JQmsI
iF-34wrTzYGV25qsQmNW0DoLALsd1Bd55mocc40AQXEp-9j9J70AXL1SgUoQyE0kwtR7RcuAK10fFHPQTJ92FN7_wEDgjcZ
JH8SKrSttRDBWgCL5BUEIM4XGWFsdVZRvbMSG4jJ9eqNa10KfjRE2CYLSb3f1EG3mwsCY8I2A",
      "Content-Type" : "application/x-www-form-urlencoded"
    }
  },
  "body" : "audience=DataProductManager&grant_type=urn:ietf:params:oauth:grant-type:uma-ticke
",
  "action" : "access"
}
  
```

```

{
  "result" : true,
  "metadata" : {
    "decision_id" : "4c16e297-aaef-43e2-8693-d21b12aebda4"
  }
}
  
```


Access Control



IA

Este trabajo es un logro significativo en la gestión de datos y la seguridad, especialmente en el dinámico panorama de la inteligencia artificial

IETF Datatracker Groups Documents Meetings Other User

Knowledge Graphs for YANG-based Network Management draft-marcas-nmop-knowledge-graph-yang-02

Status Email expansions History

Versions:
00 01 02

This document is an Internet-Draft (I-D). Anyone may submit an I-D to the IETF. This I-D is **not endorsed by the IETF** and has no force.

draft-marcas-nmop-knowledge-graph-yang 01 02
May 2024

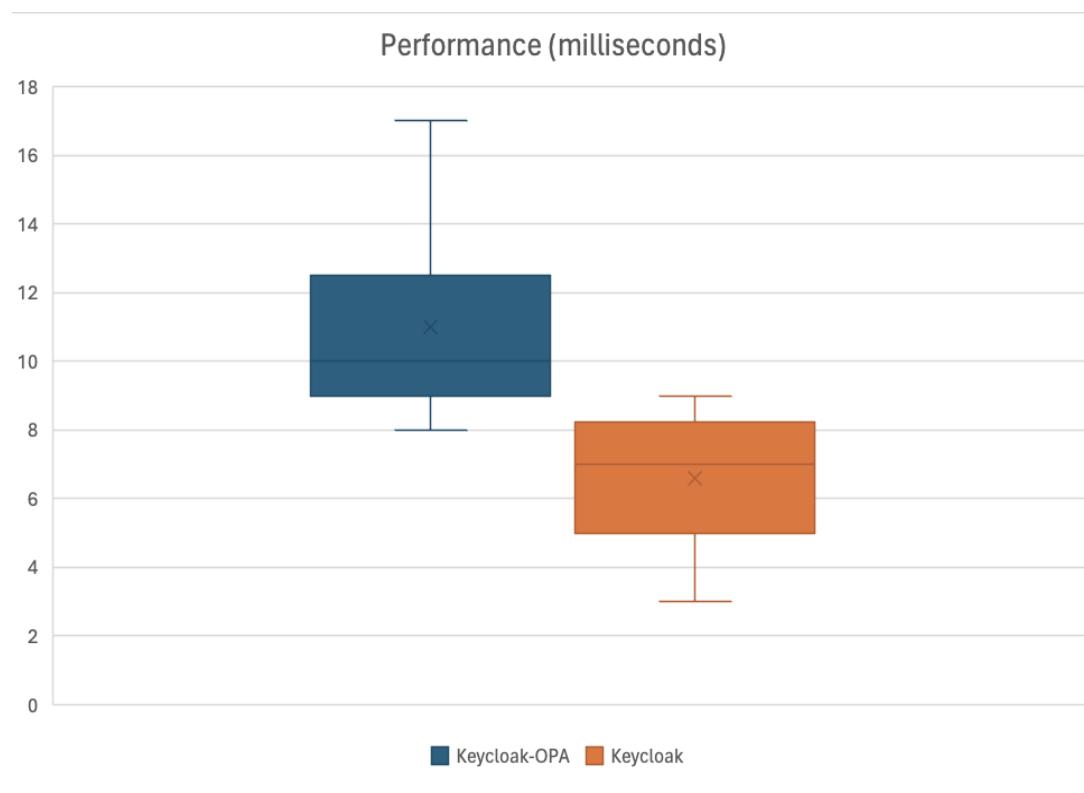
Document	Type	Active Internet-Draft (individual)
Authors		Ignacio Dominguez Martinez-Casanueva ✉, Lucía Cabanillas Rodríguez ✉

Access Control



Rendimiento

A pesar de un ligero aumento de la latencia, este nuevo enfoque mejora la seguridad al proporcionar un marco de control de acceso más sólido y flexible



Access Control

Exploración

- Exploración de consultas directas a OPA
- Continuación de las contribuciones comunitarias
- Participación en la elaboración de normas
- Investigación e innovación continuadas

