FIWARE
Global
Summit

From Data
to Value

OPEN SOURCE
OPEN STANDARDS
OPEN COMMUNITY

Basic Identity and Access Management principles in systems powered by FIWARE

Álvaro Alonso - alvaro.alonso@upm.es
Universidad Politécnica de Madrid
FIWARE Security Team

Vienna, Austria
12-13 June, 2023
#FIWARESummit

FIWARE
Open APIs for Open Minds

FIWARE Ecosystem

- A framework of **open source platform components** which can be assembled together and with other third-party components to accelerate the development of **Smart Solutions**.

FIWARE

FIWARE Ecosystem

- A framework of **open source platform components** which can be assembled together and with other third-party components to accelerate the development of **Smart Solutions**.

FIWARE

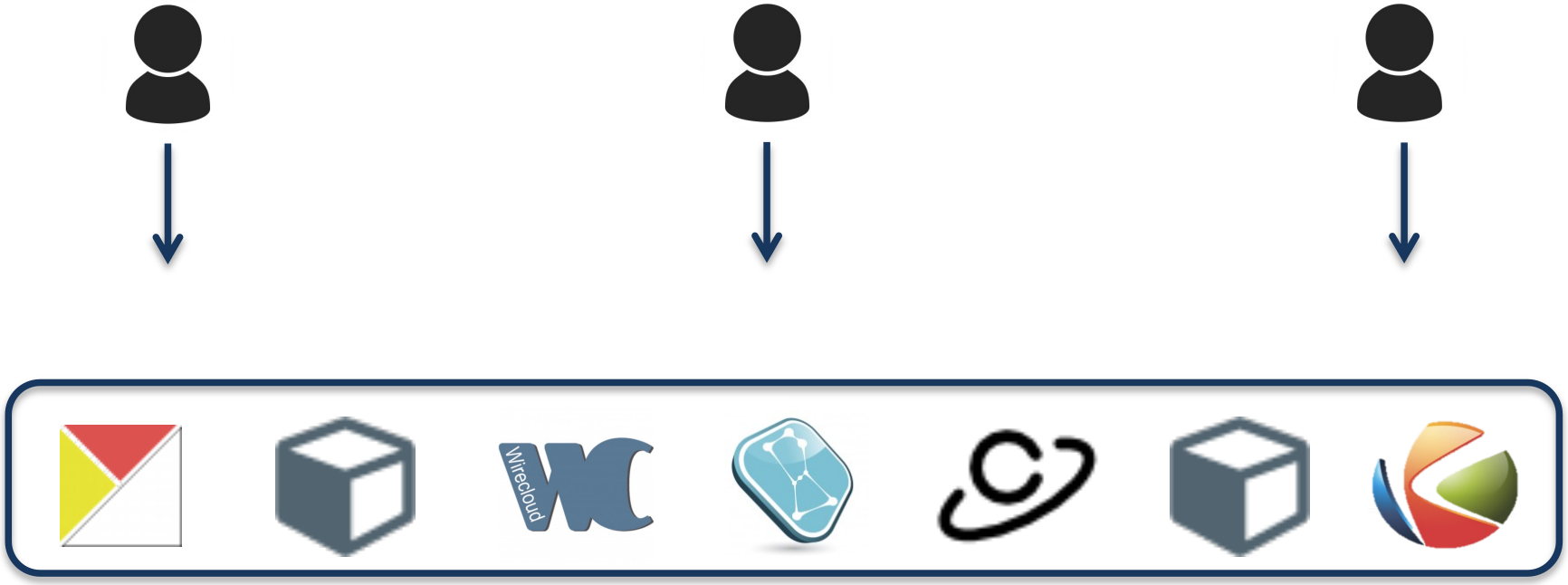
FIWARE Ecosystem

- A framework of **open source platform components** which can be assembled together and with other third-party components to accelerate the development of **Smart Solutions**.

FIWARE

FIWARE Ecosystem

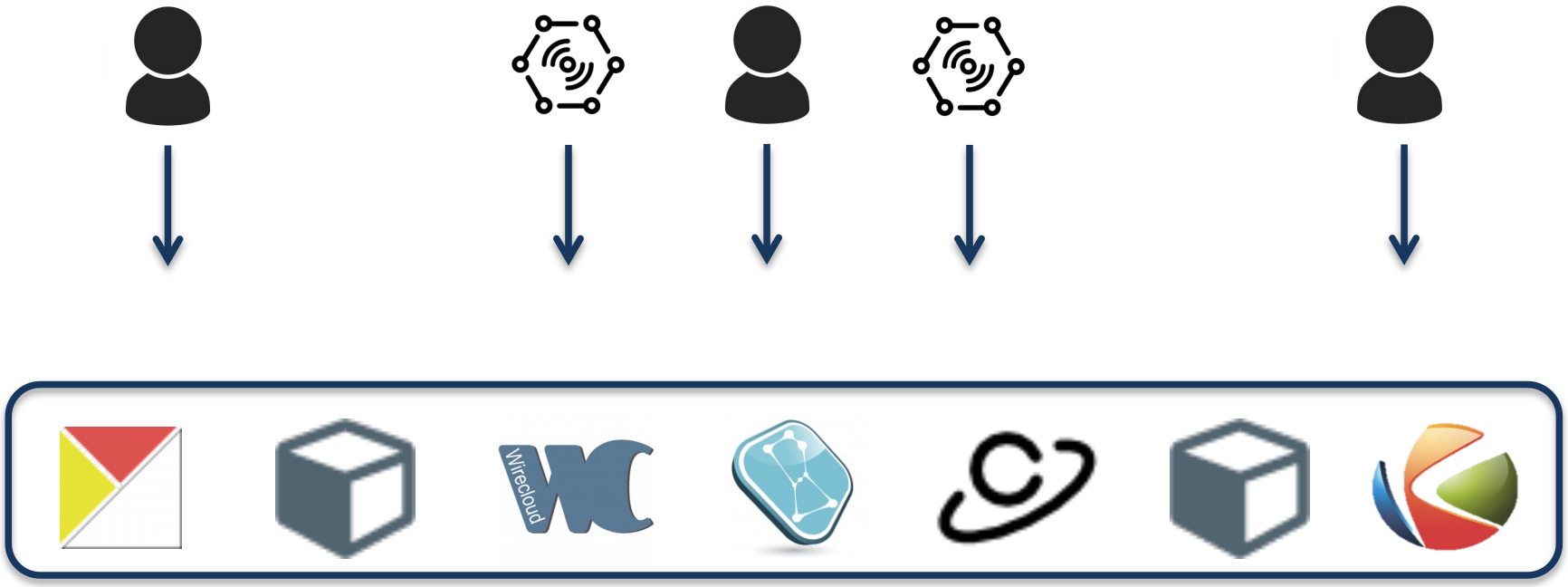
- A framework of **open source platform components** which can be assembled together and with other third-party components to accelerate the development of **Smart Solutions**.



FIWARE

FIWARE Ecosystem

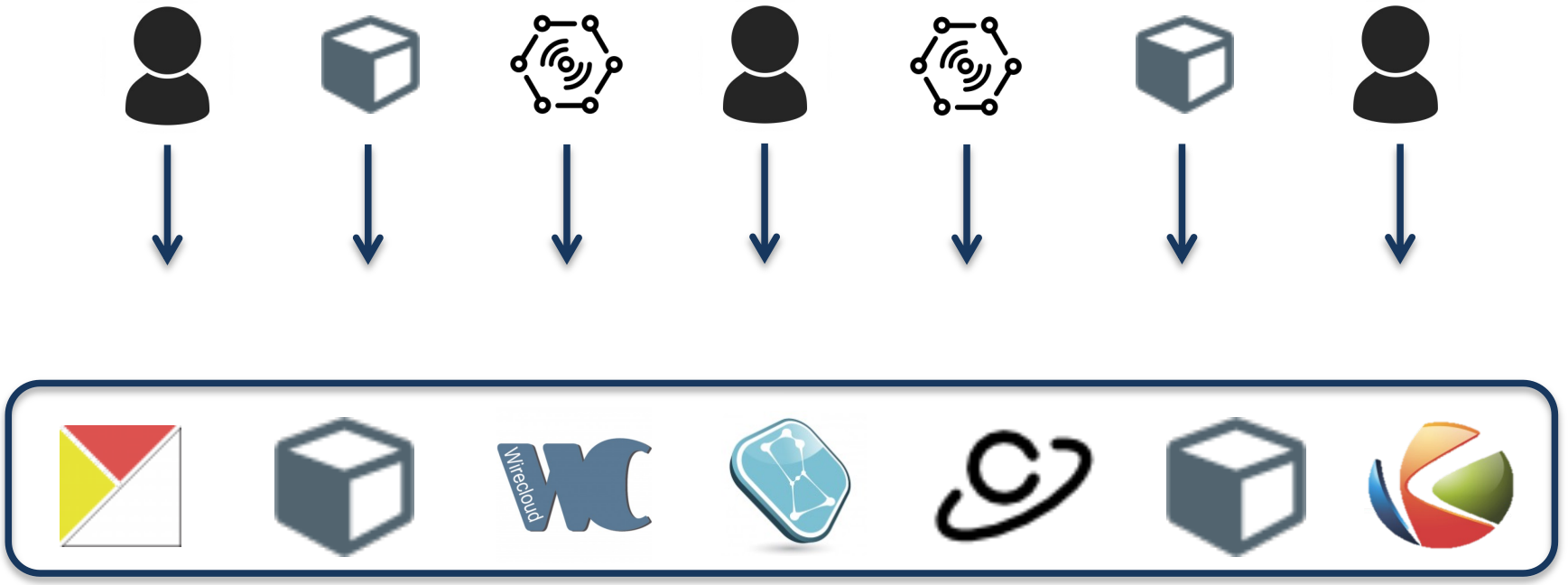
- A framework of **open source platform components** which can be assembled together and with other third-party components to accelerate the development of **Smart Solutions**.



FIWARE

FIWARE Ecosystem

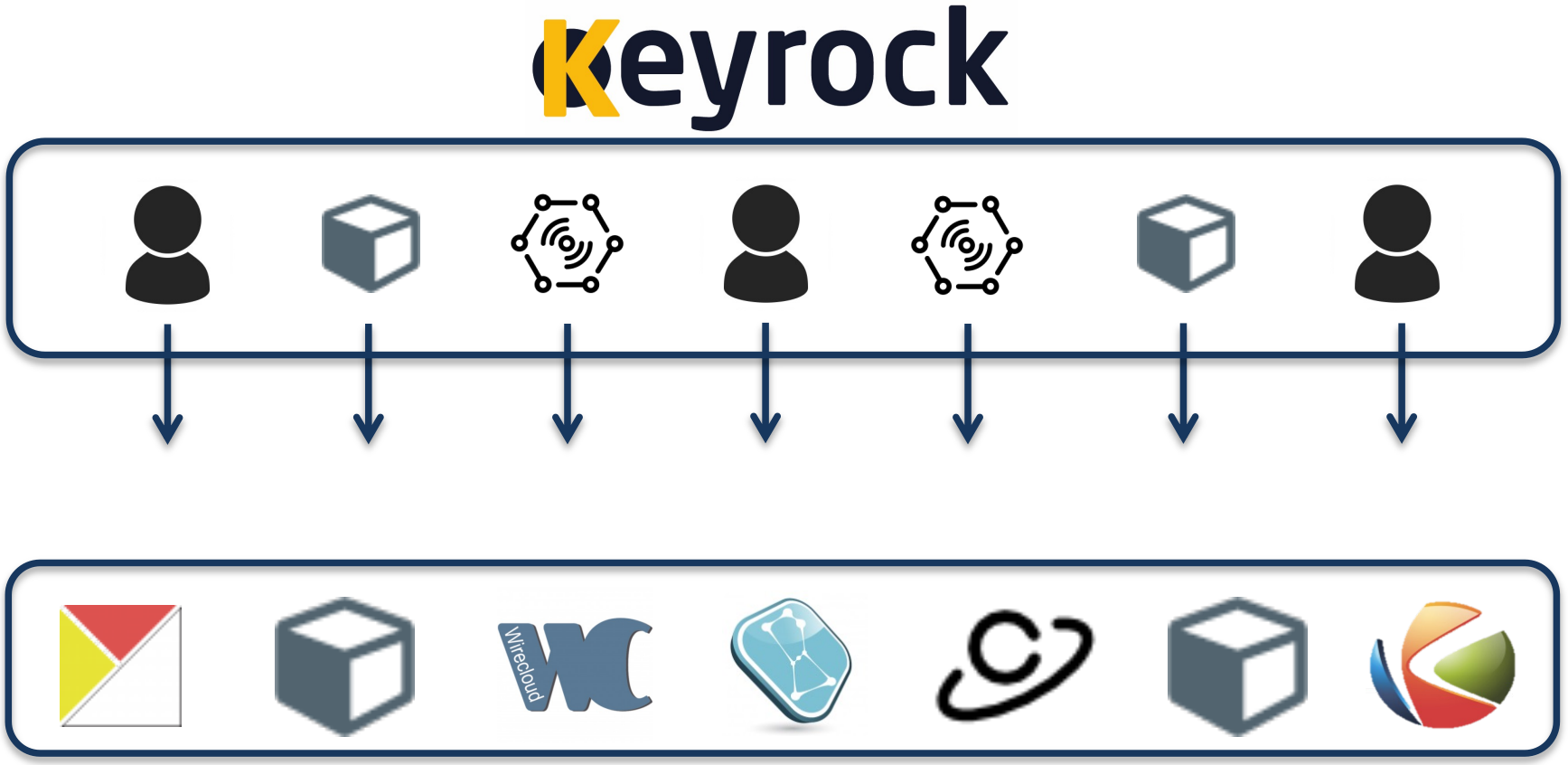
- A framework of **open source platform components** which can be assembled together and with other third-party components to accelerate the development of **Smart Solutions**.



FIWARE

FIWARE Ecosystem

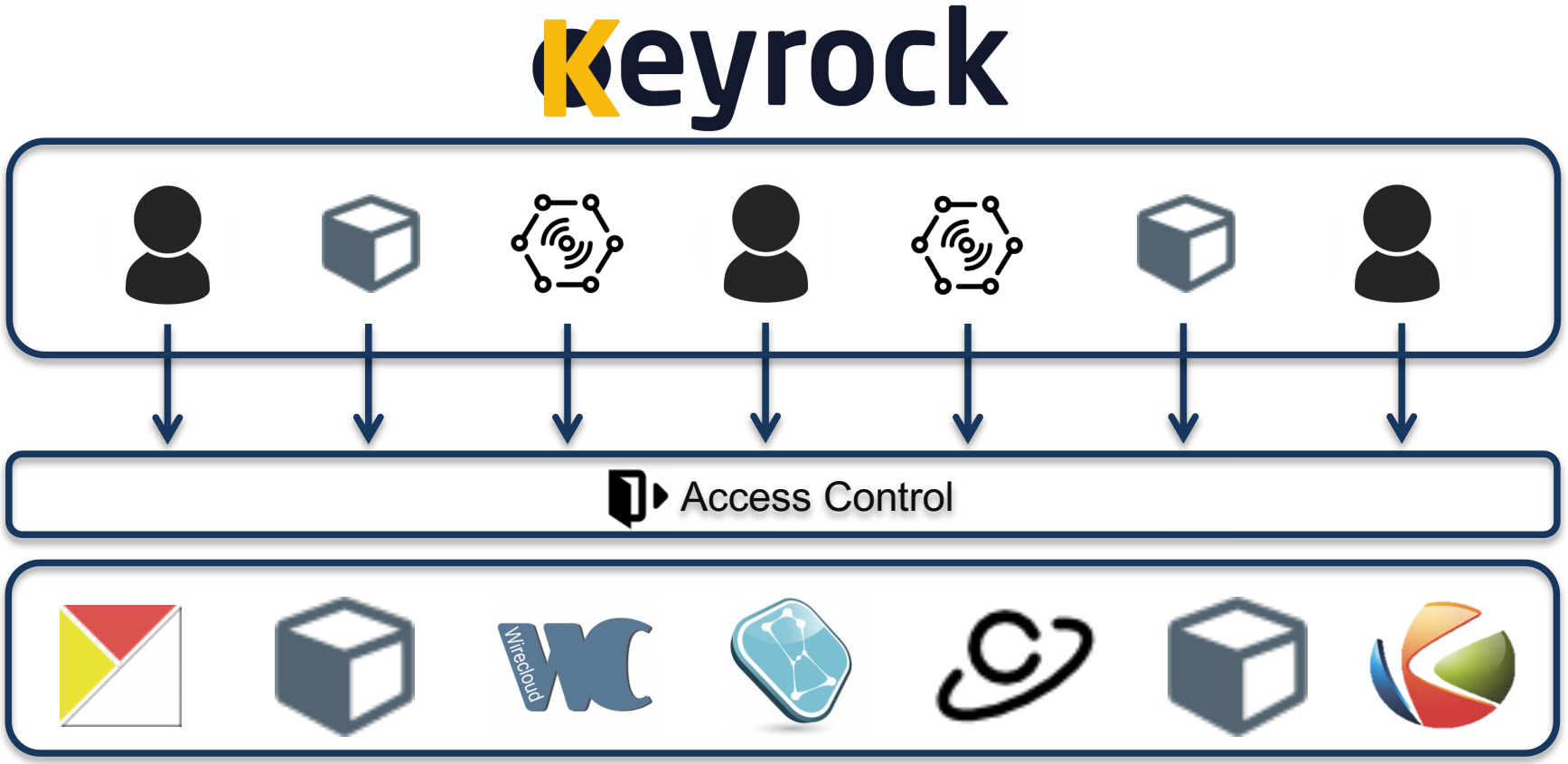
- A framework of **open source platform components** which can be assembled together and with other third-party components to accelerate the development of **Smart Solutions**.



FIWARE

FIWARE Ecosystem

- A framework of **open source platform components** which can be assembled together and with other third-party components to accelerate the development of **Smart Solutions**.



FIWARE

IAM Generic Enablers

Identity & Access Control Management

- Keyrock – Identity Management
- Wilma – PEP Proxy
- AuthZForce – Authorization PDP

FIWARE

https://keyrock-fiware.github.io

FIWARE

Keyrock

Main features

Web Interface and Rest API for managing Identity

- Users, devices and groups management
- OAuth 2.0 and OpenID Connect - Single Sign On
- Application - scoped roles and permissions management
- Support for local and remote PAP/PDP
- JSON Web Tokens (JWT) and Permanent Tokens support
- Two factor authentication
- MySQL / PostgreSQL and external DB driver
- European eID authentication compatibility (CEF eIDAS)

FIWARE

Wilma

Main features

PEP Proxy for securing service backends

- Basic and complex AC policies support
- OAuth 2.0 Access Tokens support
- JSON Web Tokens (JWT) support
- Custom PDP configuration
- Integrated with API Management tools
  - APInf & API Umbrella
  - KONG

FIWARE

AuthZForce

Main features

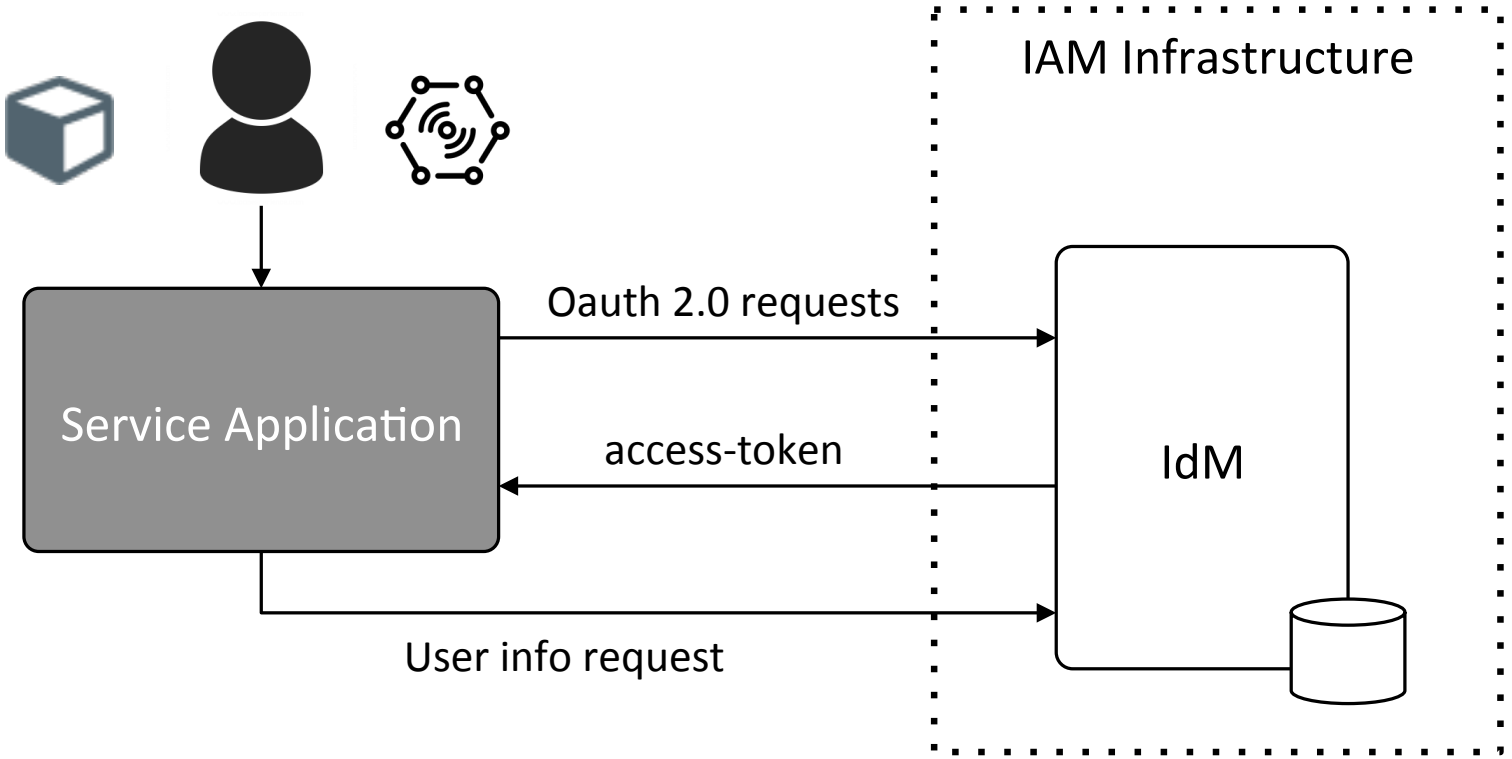
PAP and PDP Server for managing complex AC policies

- XACML-3.0 standard-compliant
- Cloud-ready RESTful ABAC framework with XML optimization
- Multi-tenant REST API for PDP and PAP
- Standards:
  - OASIS: XACML 3.0 + Profiles (REST, RBAC, Multiple Decision)
  - ISO: Fast Infoset
- Extensible to attribute providers (PIP), functions, etc.

FIWARE

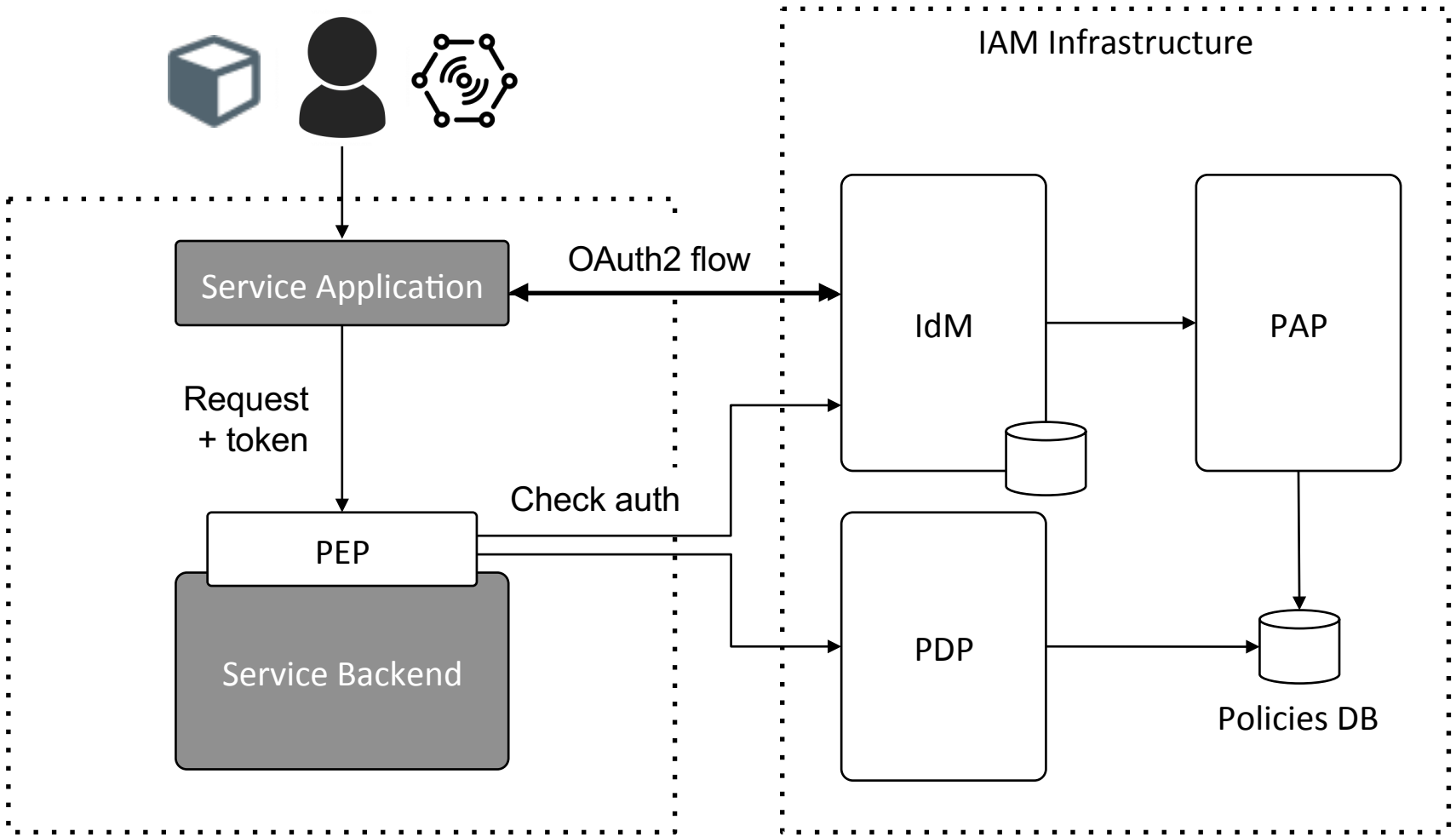
Identity and AC Management

OAuth 2.0 flow



Identity and AC Management

Accessing GEs and services



Identity and AC Management
Accessing GEs and services

- Level 1: Authentication
- Level 2: Basic Authorization
- Level 3: Advanced Authorization

FIWARE

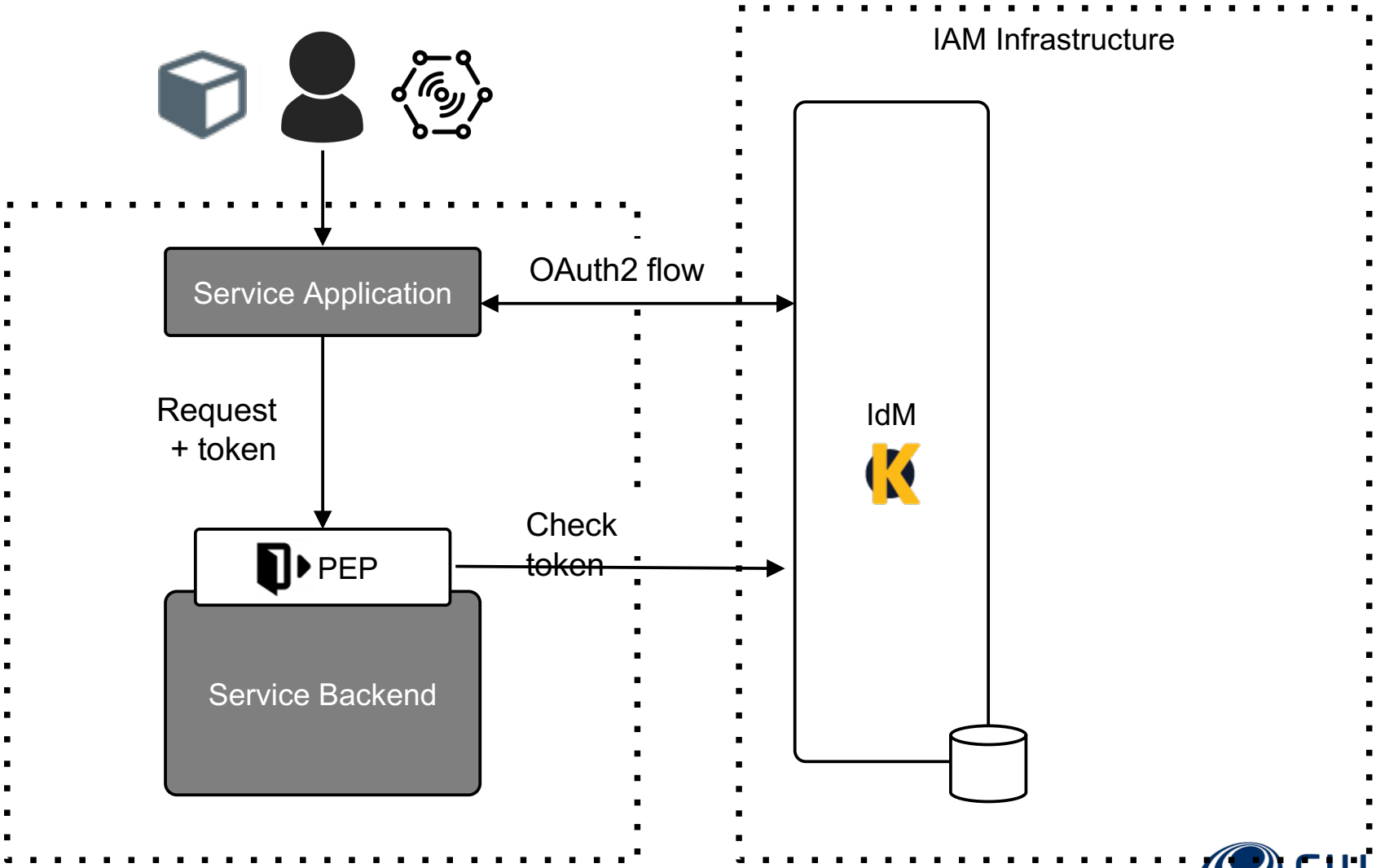
Identity and AC Management
Accessing GEs and services

- **Level 1: Authentication**
  - **Check if a user has been authenticated**
- Level 2: Basic Authorization
- Level 3: Advanced Authorization

FIWARE

Identity and AC Management

Level 1: Authentication



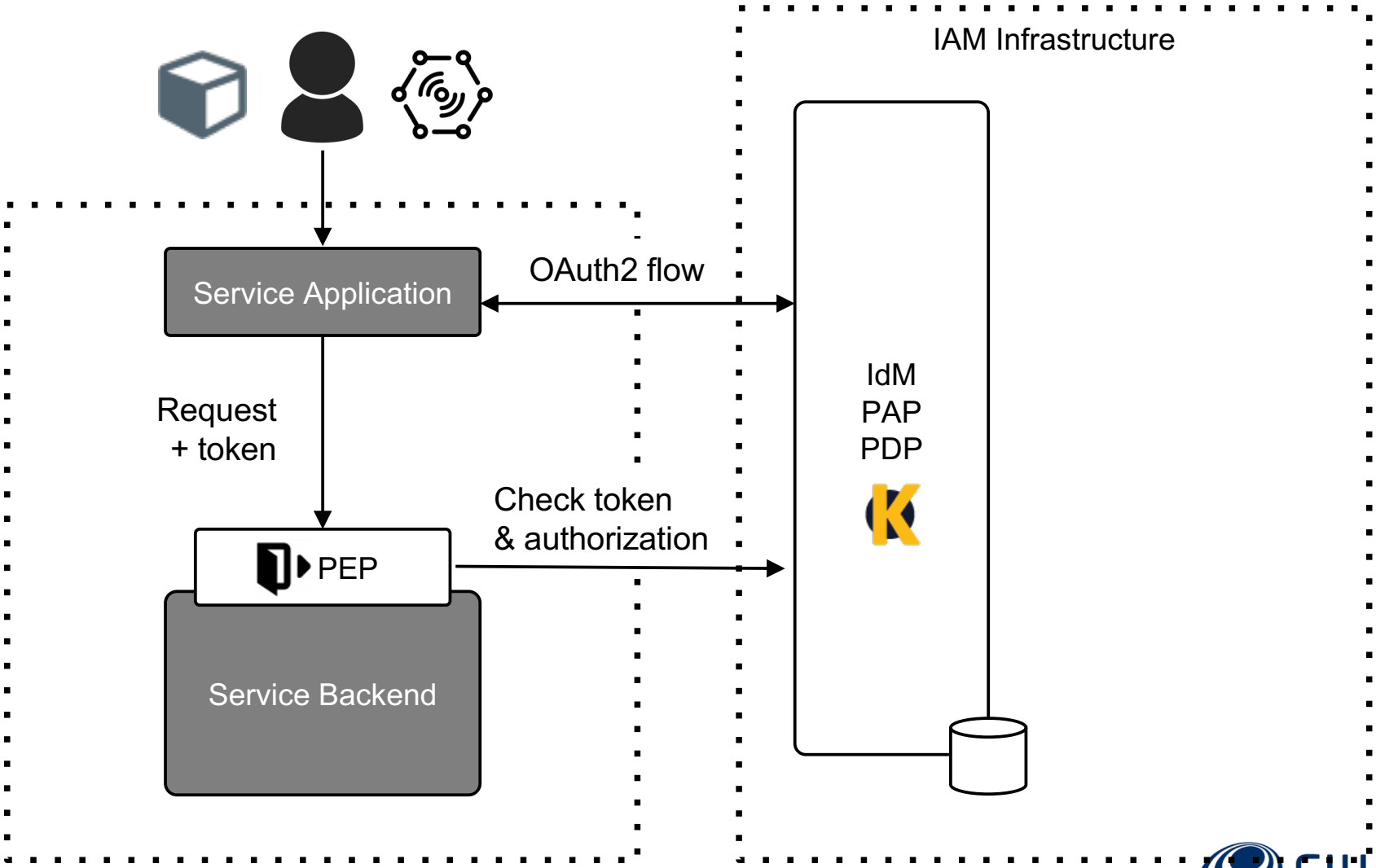
Identity and AC Management
Accessing GEs and services

- Level 1: Authentication
  - Check if a user has been authenticated
- **Level 2: Basic Authorization**
  - **Checks if a user has permissions to access a resource**
  - **HTTP verb + resource path**
- Level 3: Advanced Authorization

FIWARE

Identity and AC Management

Level 2: Basic Authorization



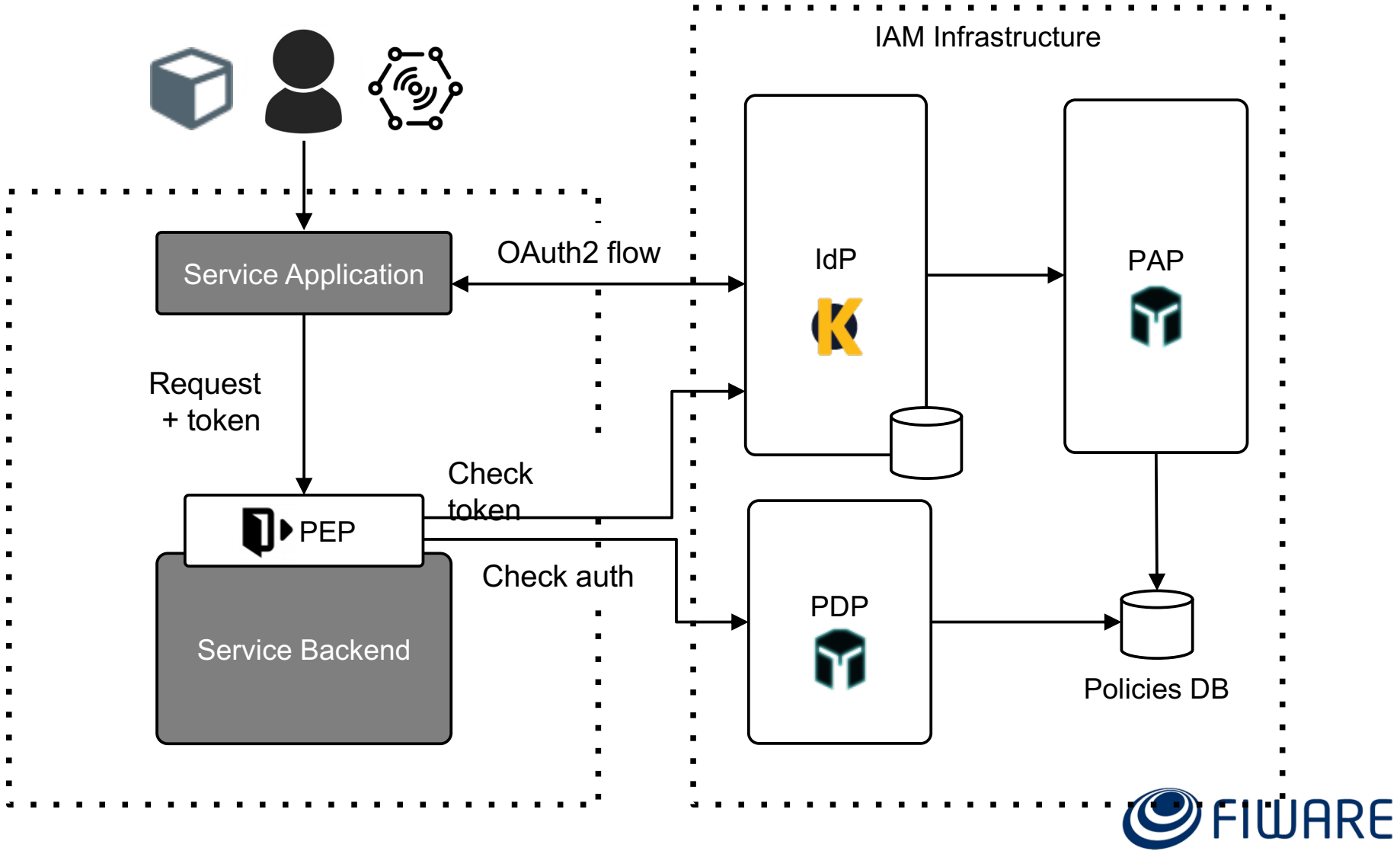
Identity and AC Management
Accessing GEs and services

- Level 1: Authentication
  - Check if a user has been authenticated
- Level 2: Basic Authorization
  - Checks if a user has permissions to access a resource
  - HTTP verb + resource path
- **Level 3: Advanced Authorization**
  - **Custom XACML policies**

FIWARE

Identity and AC Management

Level 3: Advanced Authorization



Identity and AC Management
JSON Web Tokens

- A JSON Web Token (JWT) is a JSON object defined in RFC 7519 as a safe way to represent a set of information between two parties.
- The token is composed of a header, a payload, and a signature.

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ
pZCI6MSwiZGlzcGxheU5hbWUiOiJEZW1vIHVzZXI
iLCJlbWFpbCI6ImRlbW9AZml3YXJlLm9yZyIsInJ
vbGVzIjpbeyJpZCI6MTUsIm5hbWUiOiJNYW5hZ2V
yIn1dLCJvcmdhbml6YXRpb25zIjpbeyJpZCI6MTI
sIm5hbWUiOiJVbml2ZXJzaWRhZCBQb2xpdGVjbml
jYSBkZSBNYWRyaWQiLCJyb2xlcyI6W3siaWQiOjE
0LCJuYW1lIjoiQWRtaW4ifV19XX0.OvRSa7SwMgM
2pKq4NnmN3gYeD-aZ1PpNLRkAI82SAIk
```

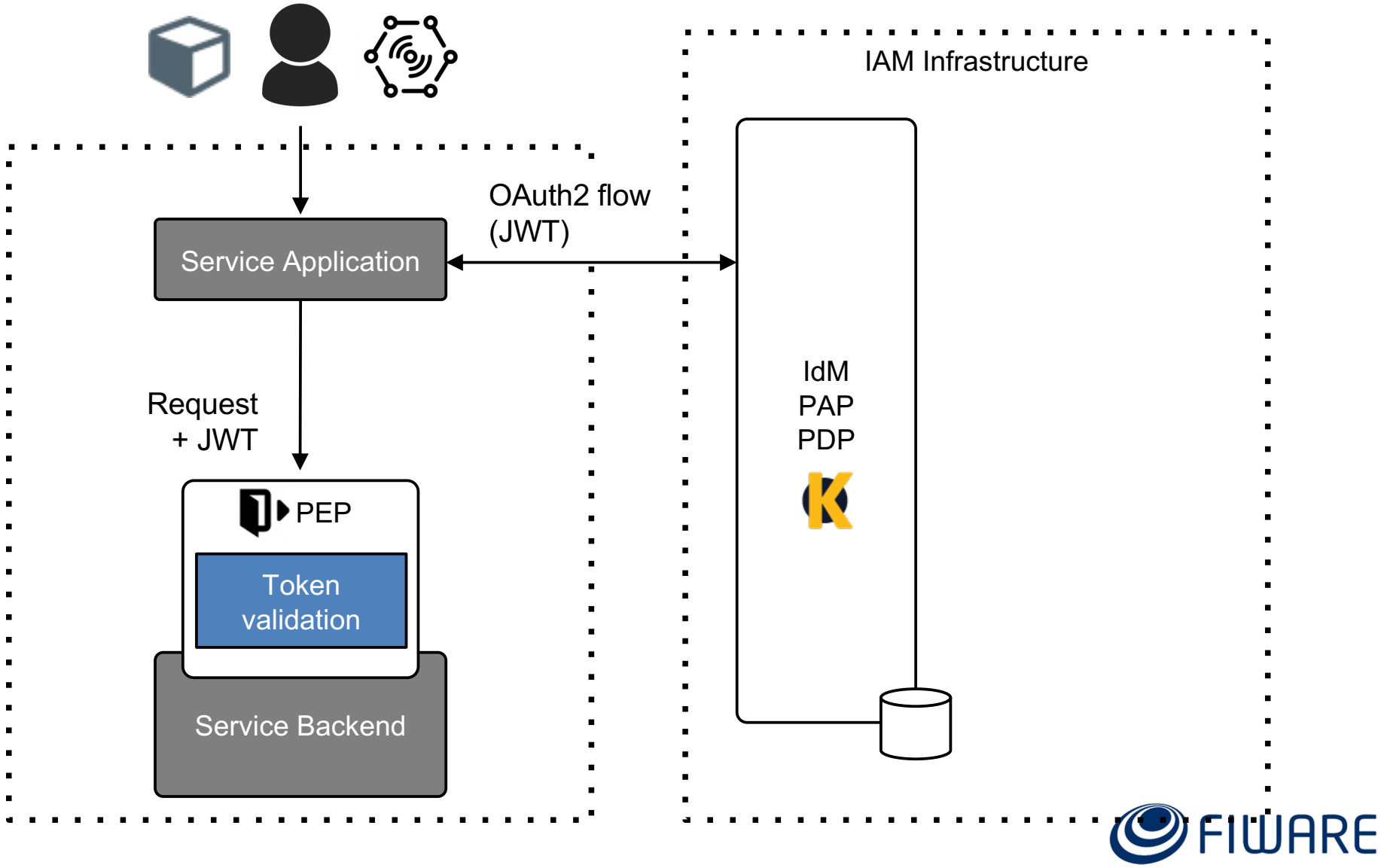
```
{
  "alg": "HS256",
  "typ": "JWT"
}
{
  "id": 1,
  "displayName": "Demo user",
  "email": "demo@fiware.org",
  "roles": [
    {
      "id": 15, "name": "Manager"
    }
  ],
  "organizations": [
    {
      "id": 12,
      "name": "Universidad Politecnica de Madrid",
      "roles": [
        {
          "id": 14, "name": "Admin"
        }
      ]
    }
  ]
}
```

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  my-secret
```

FIWARE

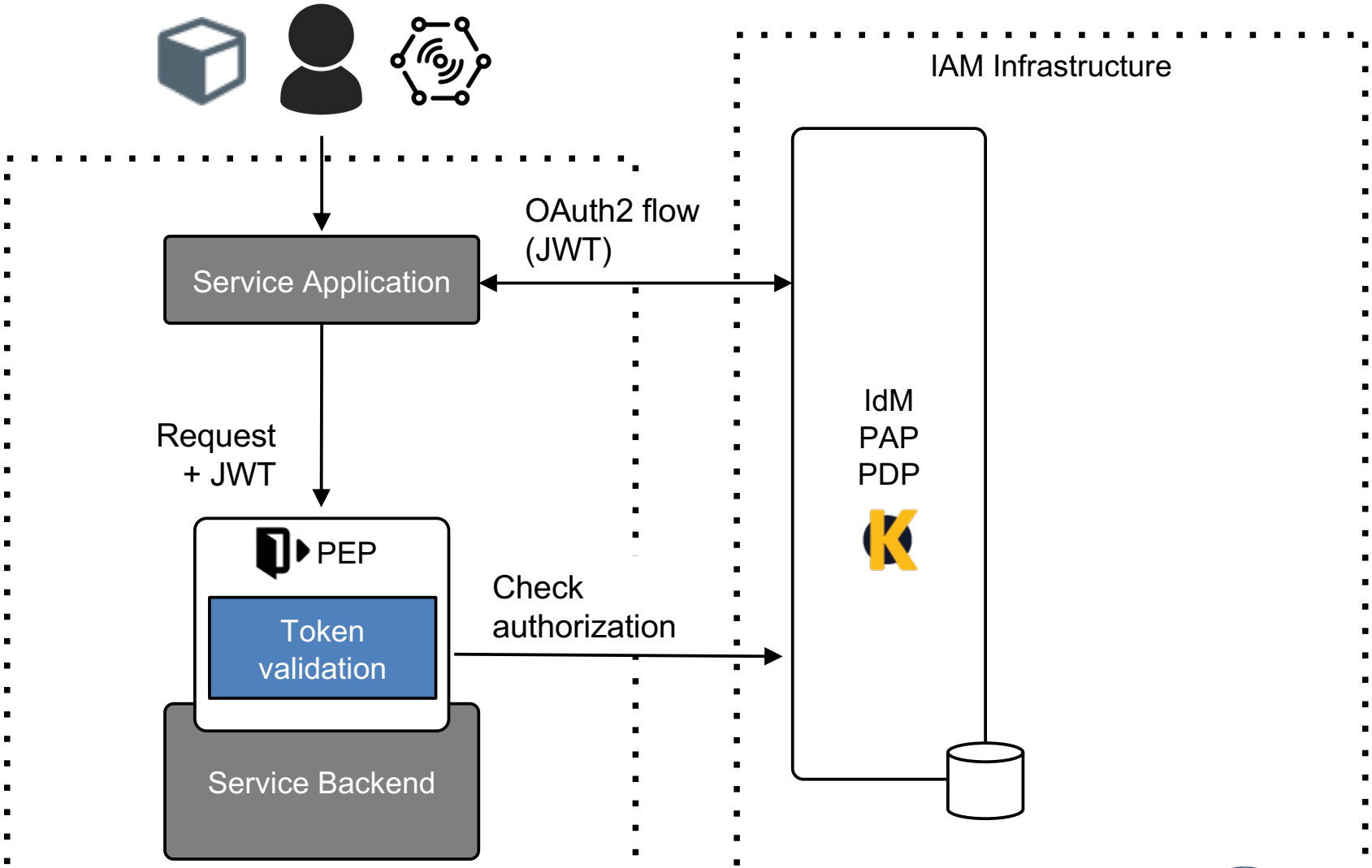
Identity and AC Management

JSON Web Tokens



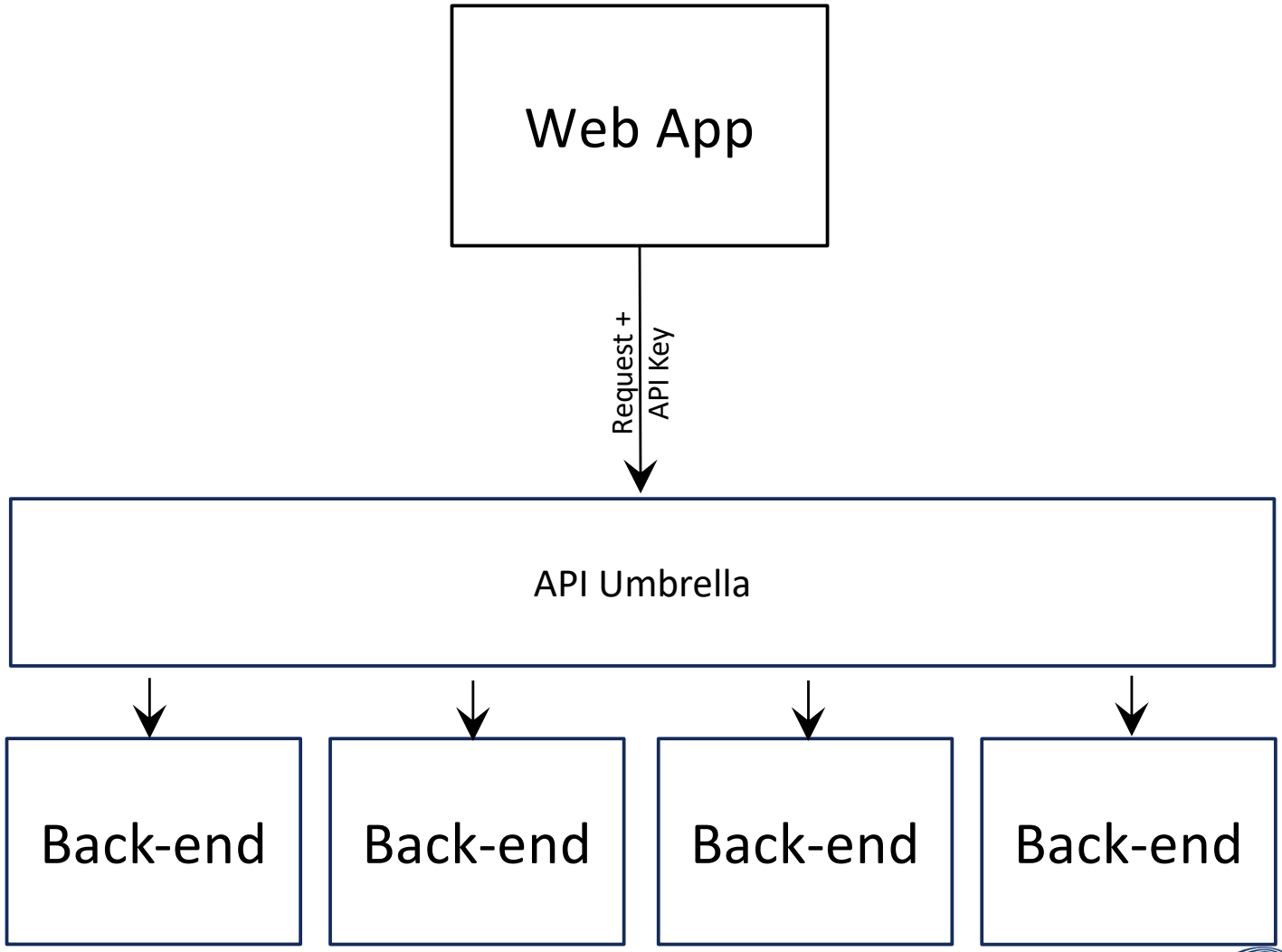
Identity and AC Management

JSON Web Tokens



API Management

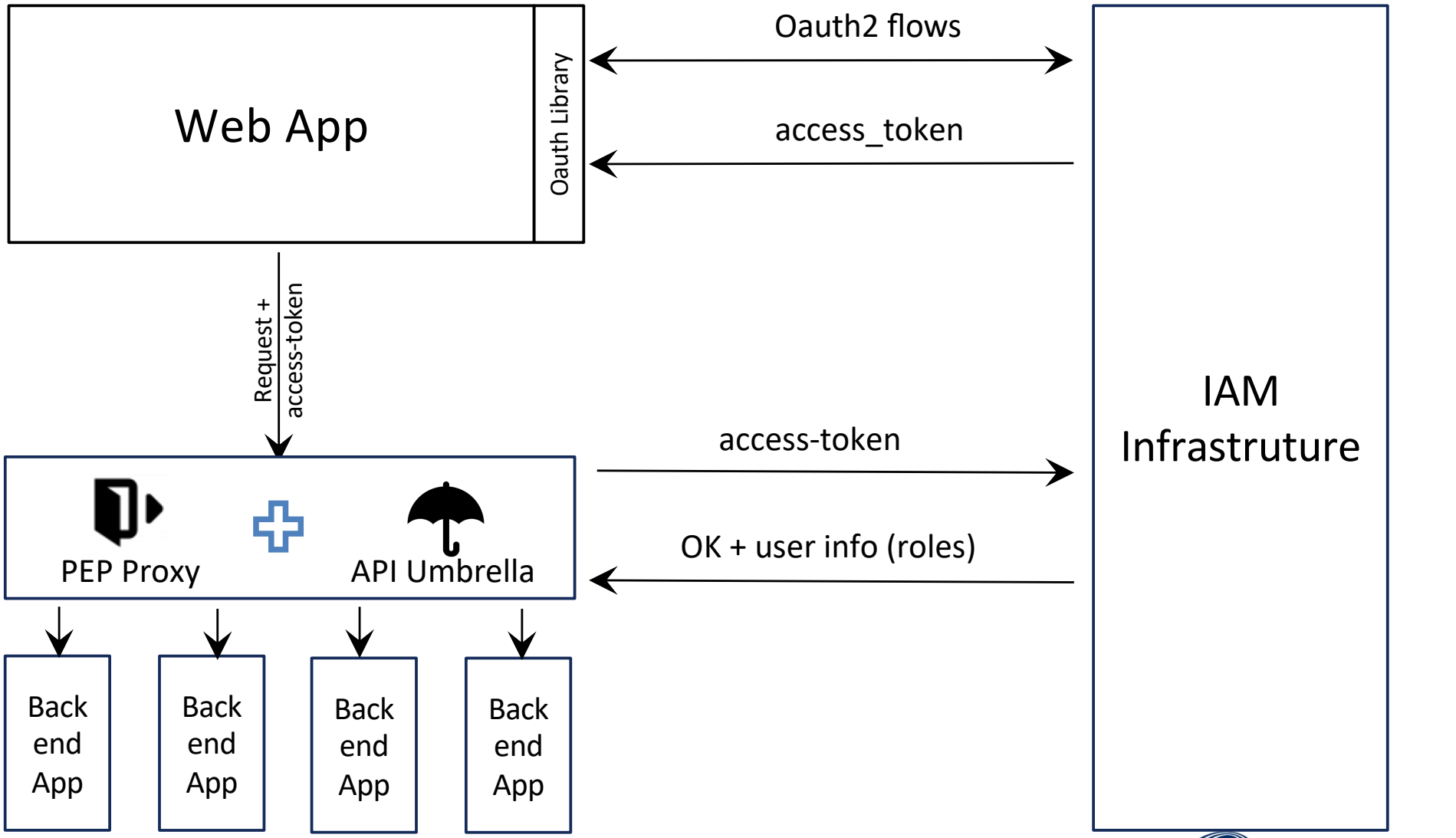
API Umbrella & PEP Proxy



FIWARE

API Management

API Umbrella & PEP Proxy



Security GEs documentation

- Identity Management – Keyrock
  - https://keyrock-fiware.github.io
  - https://github.com/ging/fiware-idm
  - https://catalogue.fiware.org/enablers/identity-management-keyrock
- PEP Proxy – Wilma
  - https://github.com/ging/fiware-pep-proxy
  - https://catalogue.fiware.org/enablers/pep-proxy-wilma
- Authorization PDP – AuthZForce
  - https://github.com/authzforce/server
  - https://catalogue.fiware.org/enablers/authorization-pdp-authzforce

FIWARE

Keyrock deep-dive

- Using Keyrock as PDP
- External authentication
- European Digital Identity (eIDAS)
- Securing IoT devices access to your services
- Identity attributes

FIWARE

FIWARE Global Summit

Find Us On

Stay up to date

JOIN OUR NEWSLETTER

Be certified and featured

FIWAREMarketplace

Global Business Sponsor

FundingBox

Keystone Sponsors

CleanCarbon

Red Hat

Telefónica

Hosting Partner

Cabildo de Gran Canaria

spegc Sociedad de Promoción Económica

Supporting Partners

BEST IN GRAN CANARIA

cidihub

FiiHUB

innovalia ASSOCIATION

Media Partners

bee smart city

CITIES FORUM

CitiesToday

Our Future Water

polis MOBILITY

RENEWABLE MATTER

the smartcity journal

ThoughtLab

Gran Canaria, 14-15 September, 2022 | #FIWARESummit

FIWARE

www.fiware.org

FIWARE
Global
Summit

Thanks!

Gran Canaria,
Spain
14-15 September,
2022
#FIWARESummit

FIWARE
Open APIs for Open Minds