Open APIs for Open Minds

Identity Management and Access Control

Security and API Management Chapter

Álvaro Alonso – alvaro.alonso@upm.es

FIWARE Security Team

Universidad Politécnica de Madrid

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

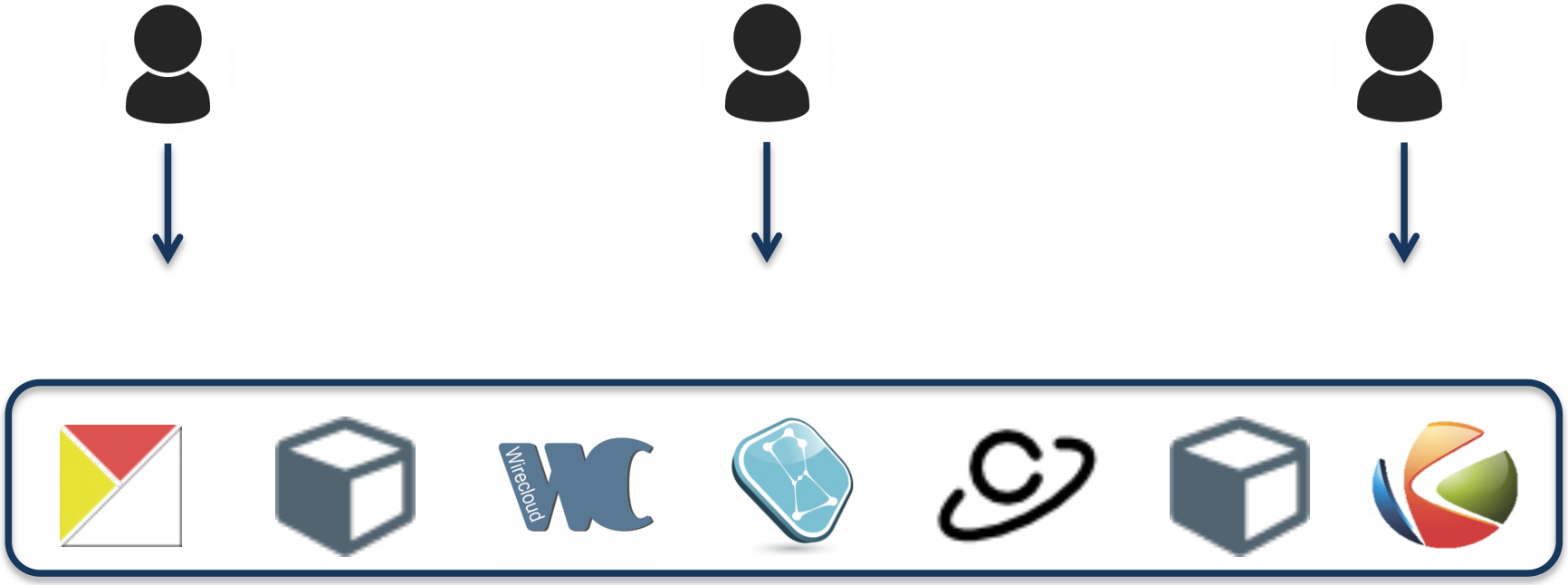
FIWARE Ecosystem

- 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

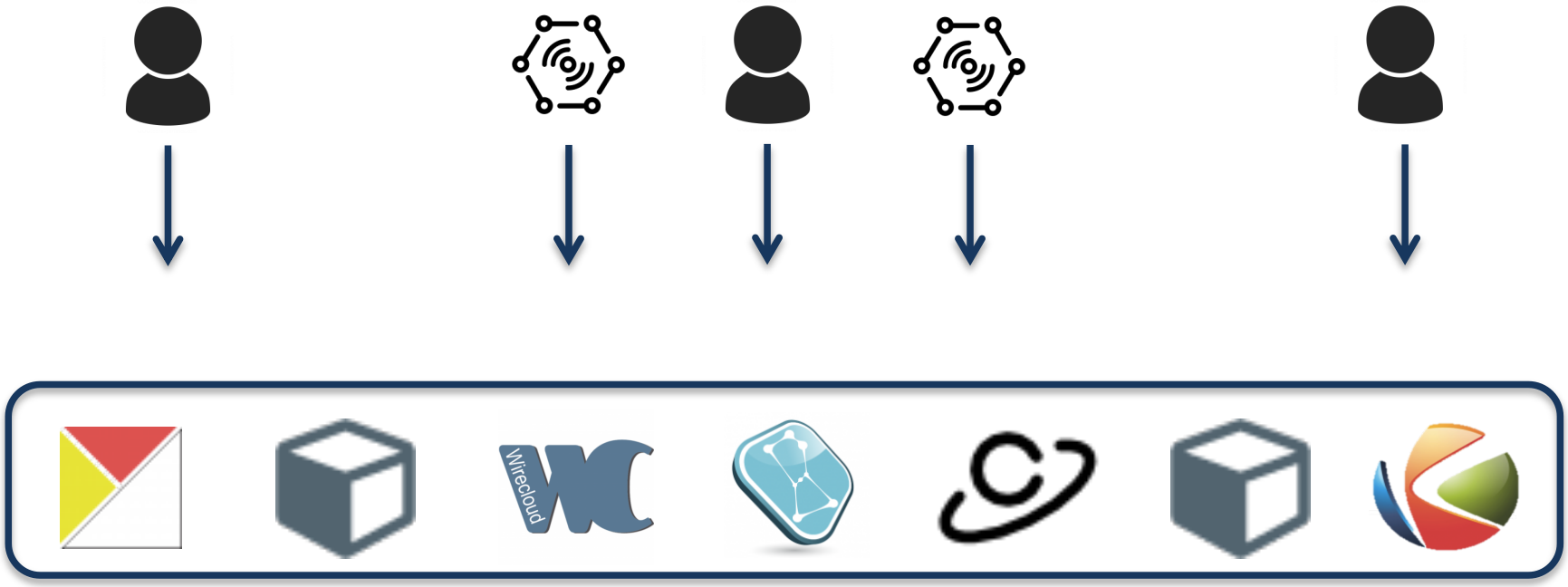
- A framework of **open source platform components** which can be assembled together and with other third-party components to accelerate the development of **Smart Solutions**.



FIWARE

FIWARE Ecosystem

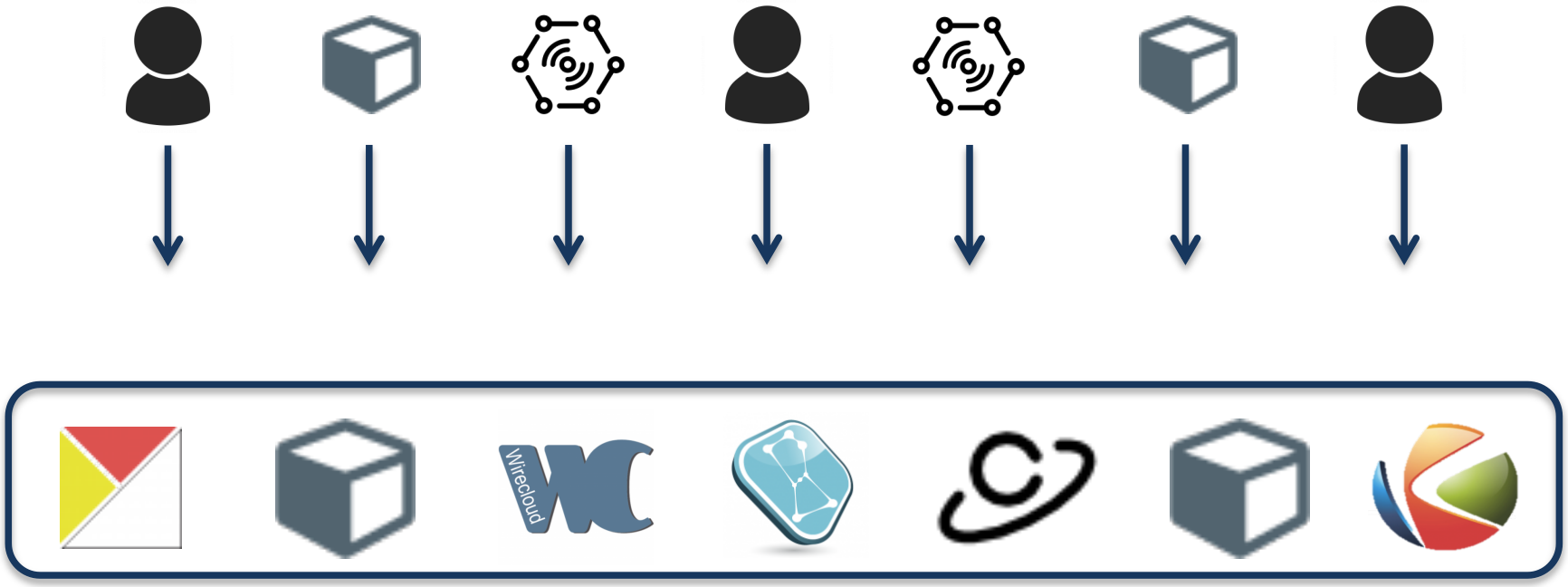
- A framework of **open source platform components** which can be assembled together and with other third-party components to accelerate the development of **Smart Solutions**.



FIWARE

FIWARE Ecosystem

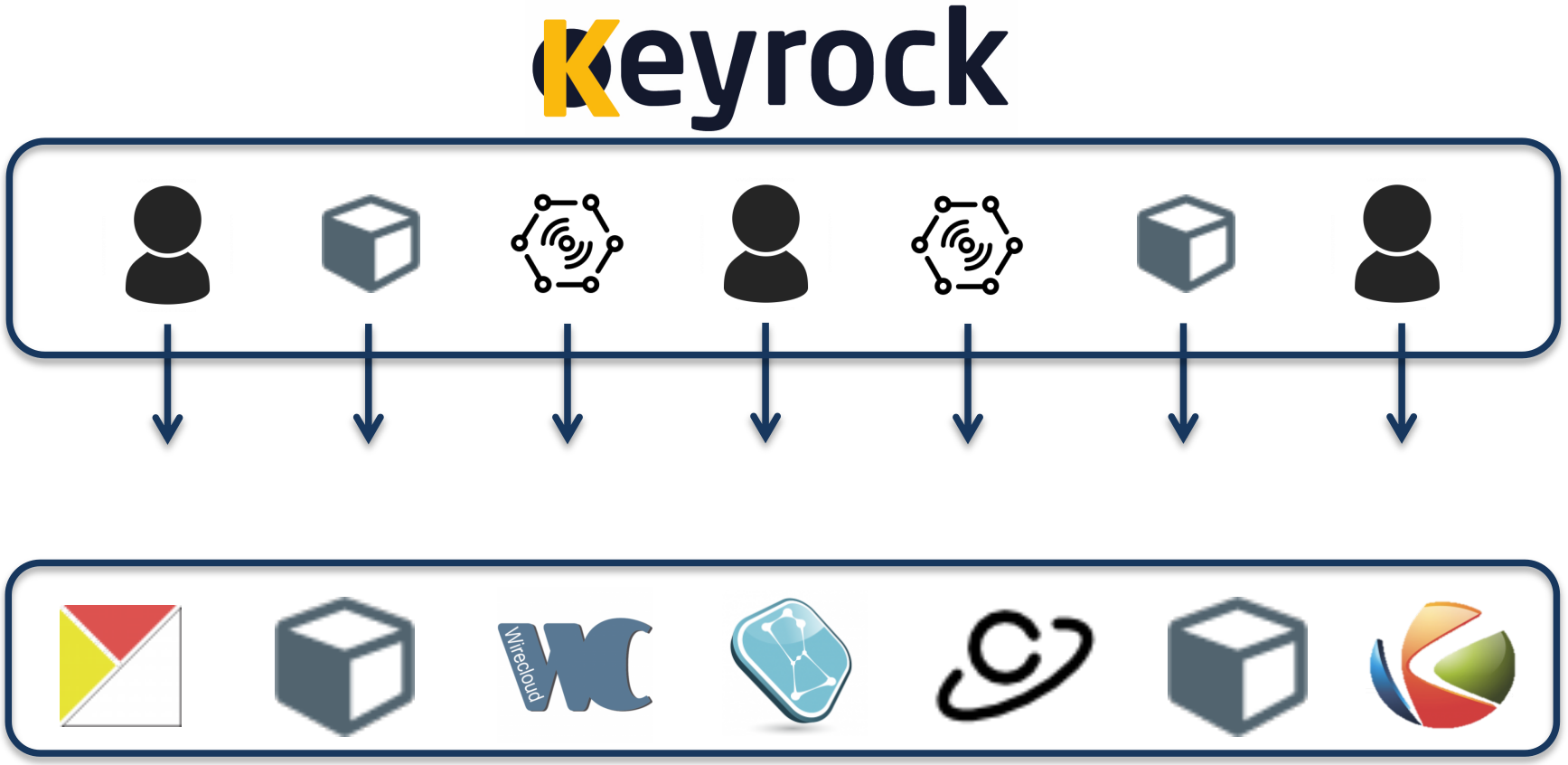
- A framework of **open source platform components** which can be assembled together and with other third-party components to accelerate the development of **Smart Solutions**.



FIWARE

FIWARE Ecosystem

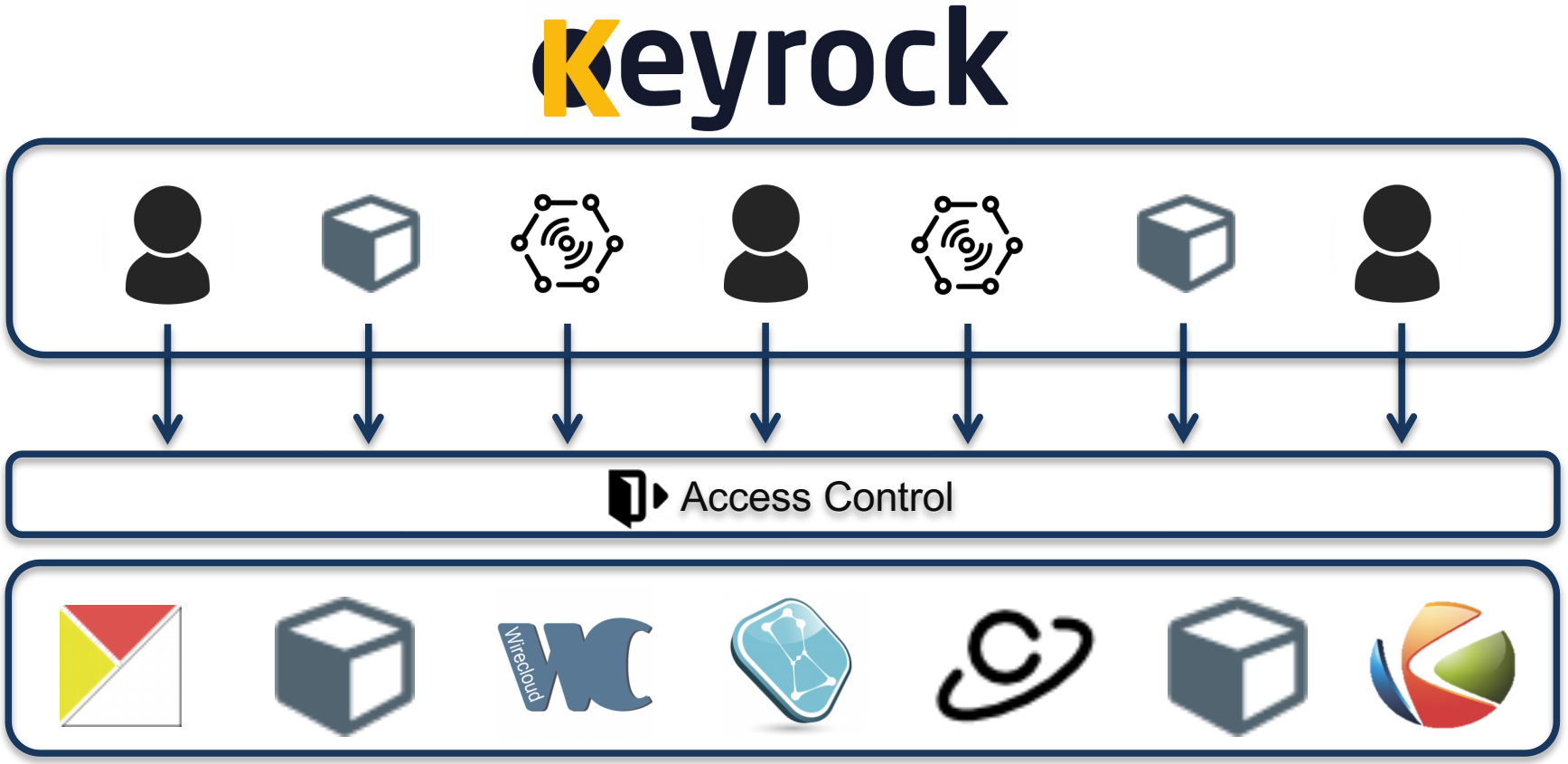
- A framework of **open source platform components** which can be assembled together and with other third-party components to accelerate the development of **Smart Solutions**.



FIWARE

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

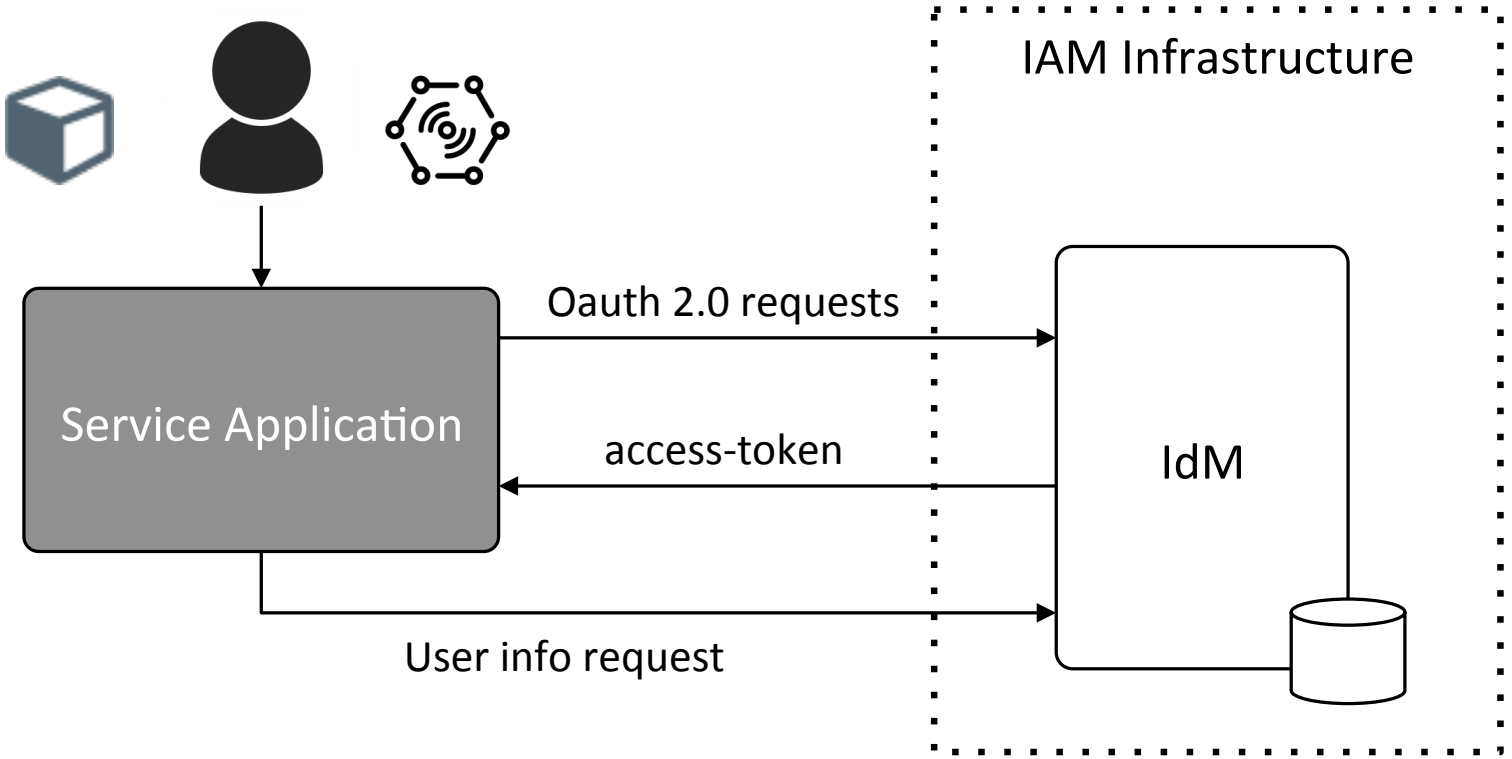
PAP and PDP Server for managing complex AC policies

- 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

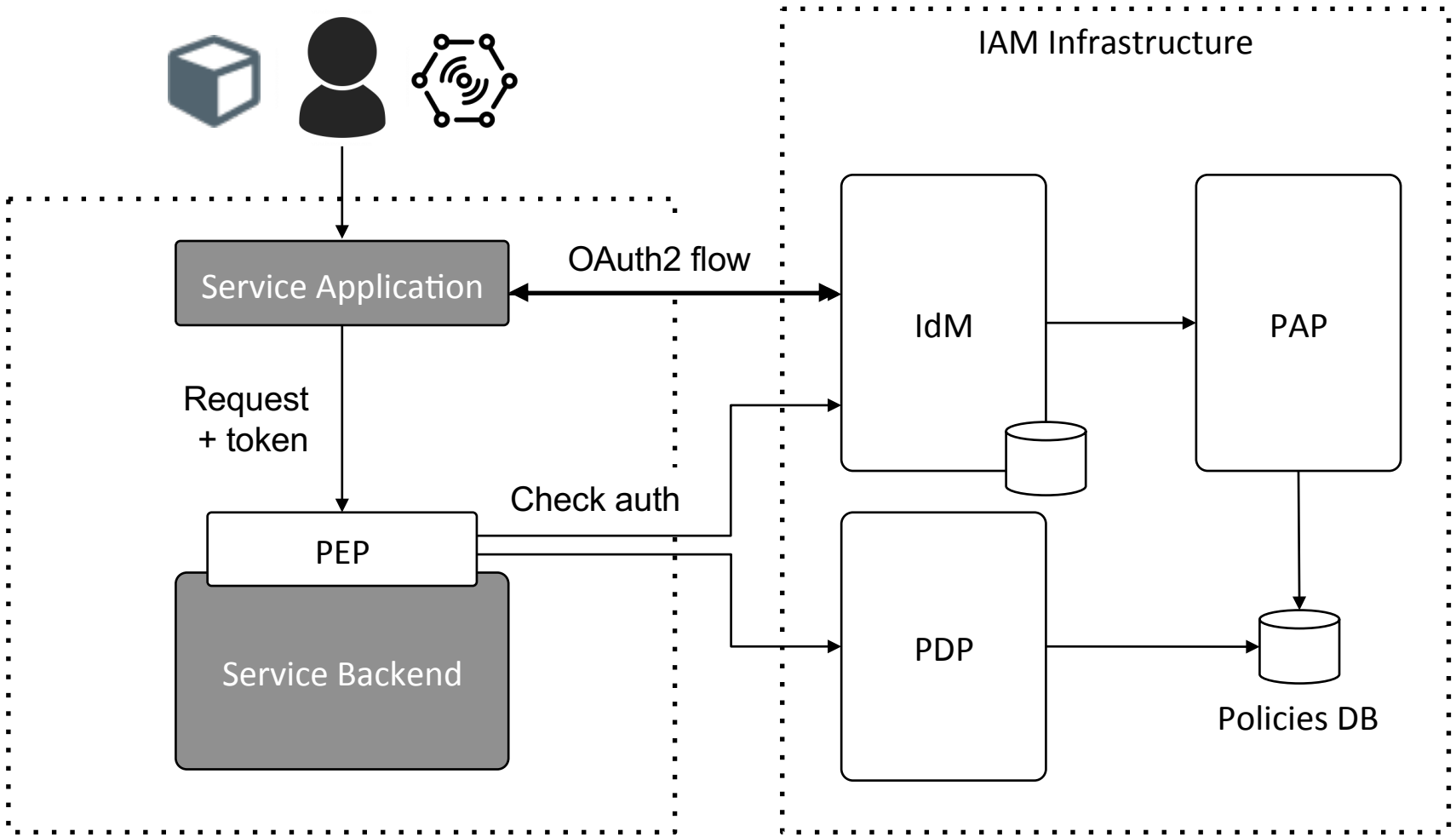
Identity and AC Management

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

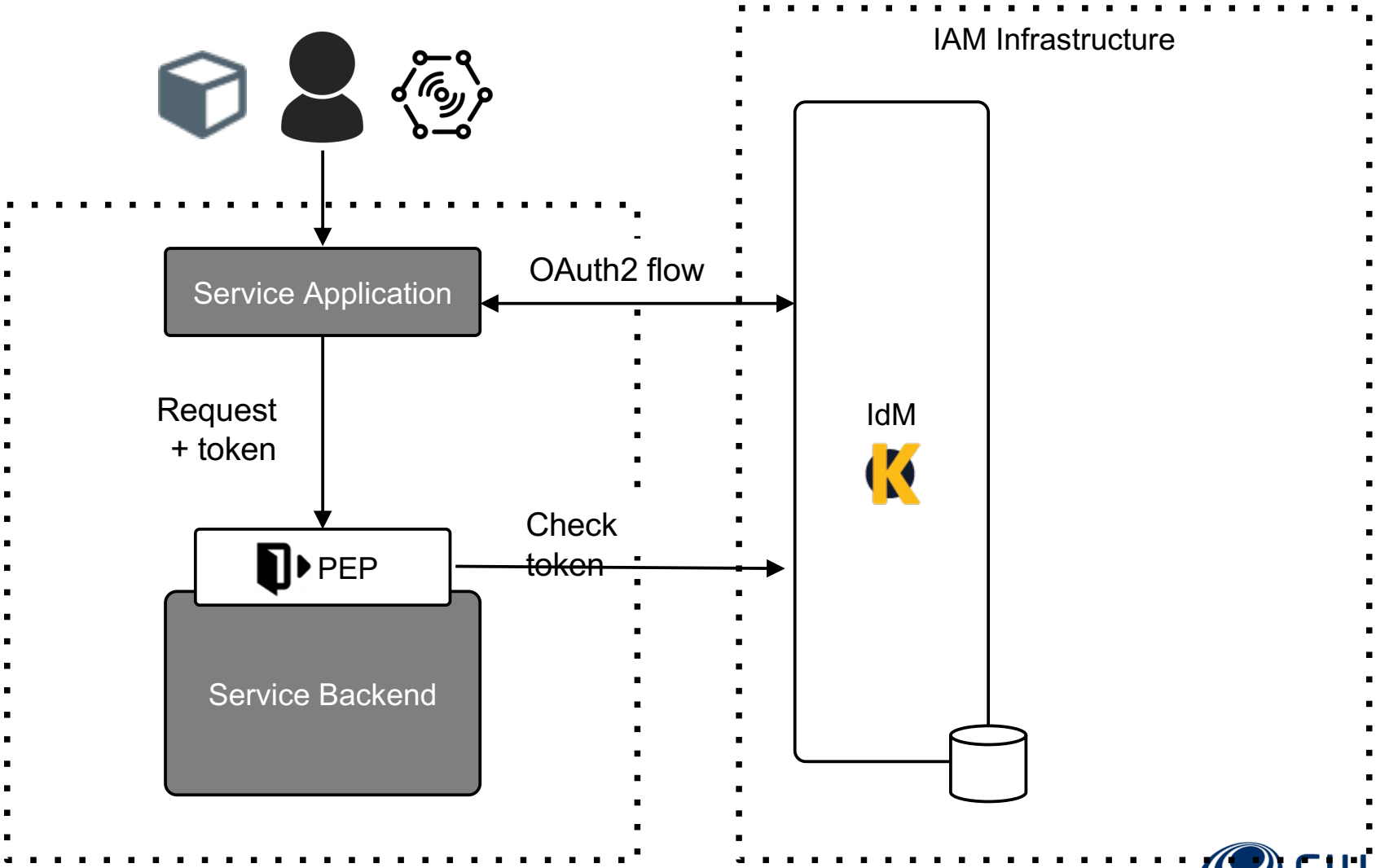
Identity and AC Management
Accessing GEs and services

- **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

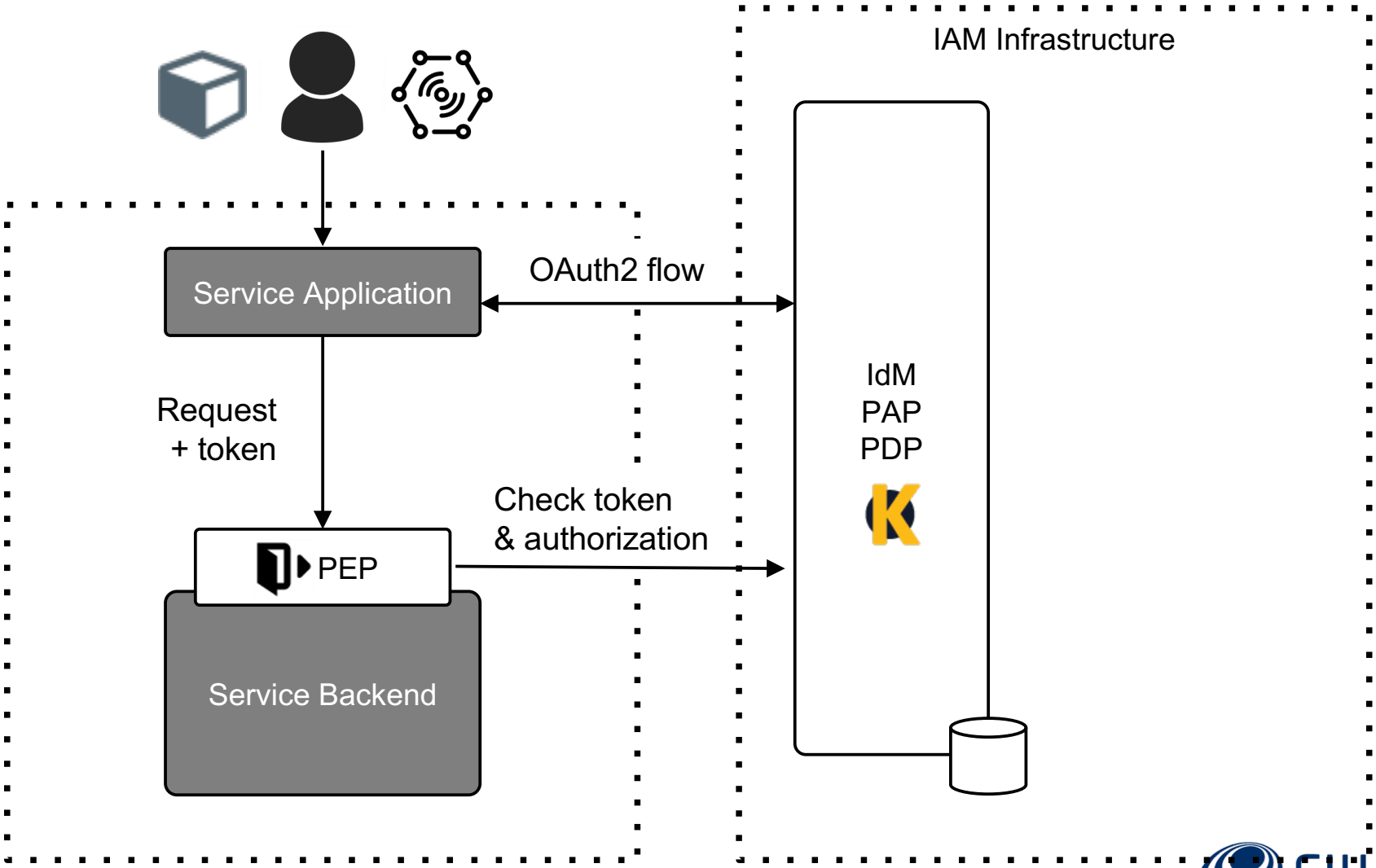
- **Level 2: Basic Authorization**
  - **Checks if a user has permissions to access a resource**
  - **HTTP verb + resource path**

- Level 3: Advanced Authorization

FIWARE

Identity and AC Management

Level 2: Basic Authorization



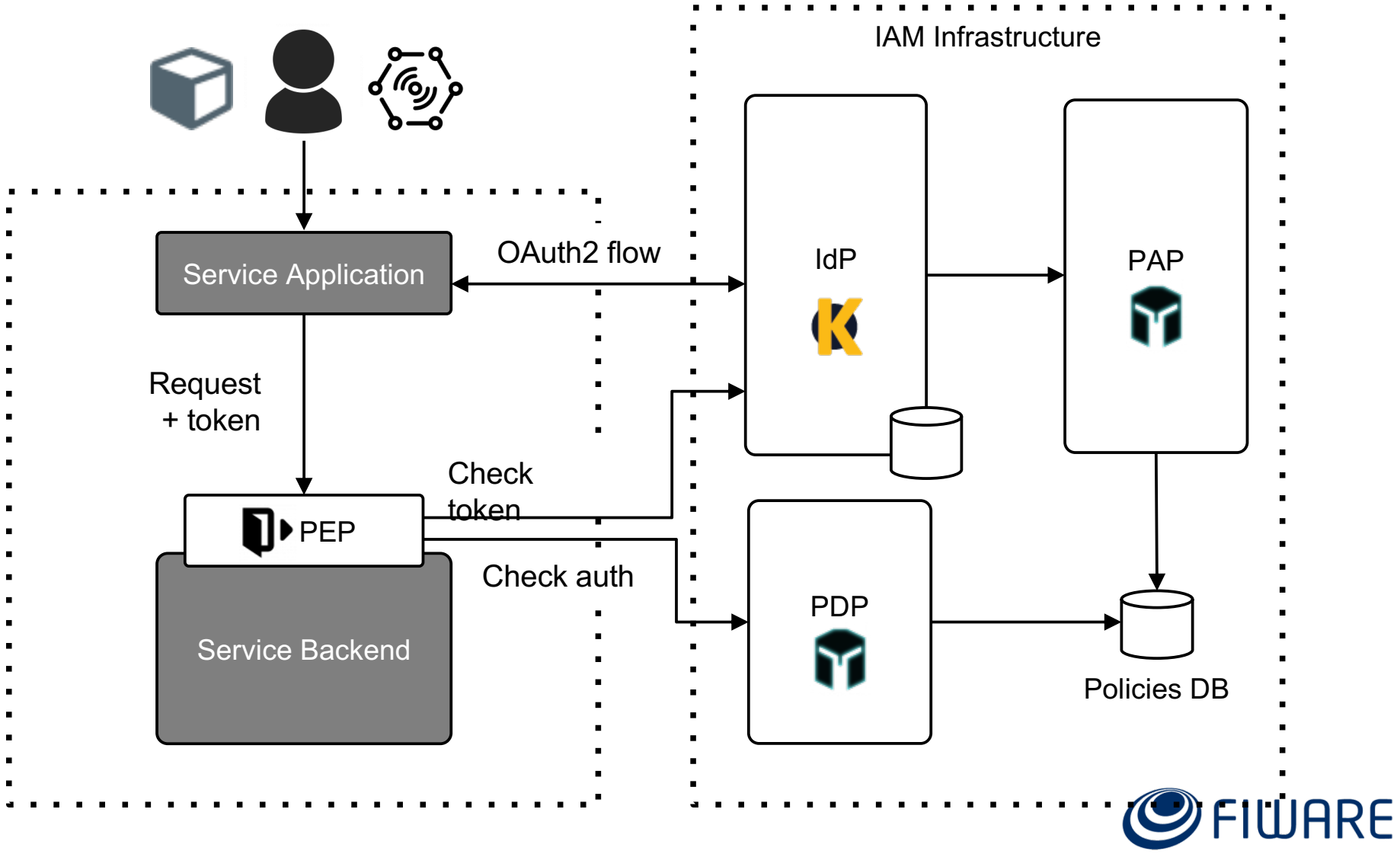
Identity and AC Management
Accessing GEs and services

- 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
```

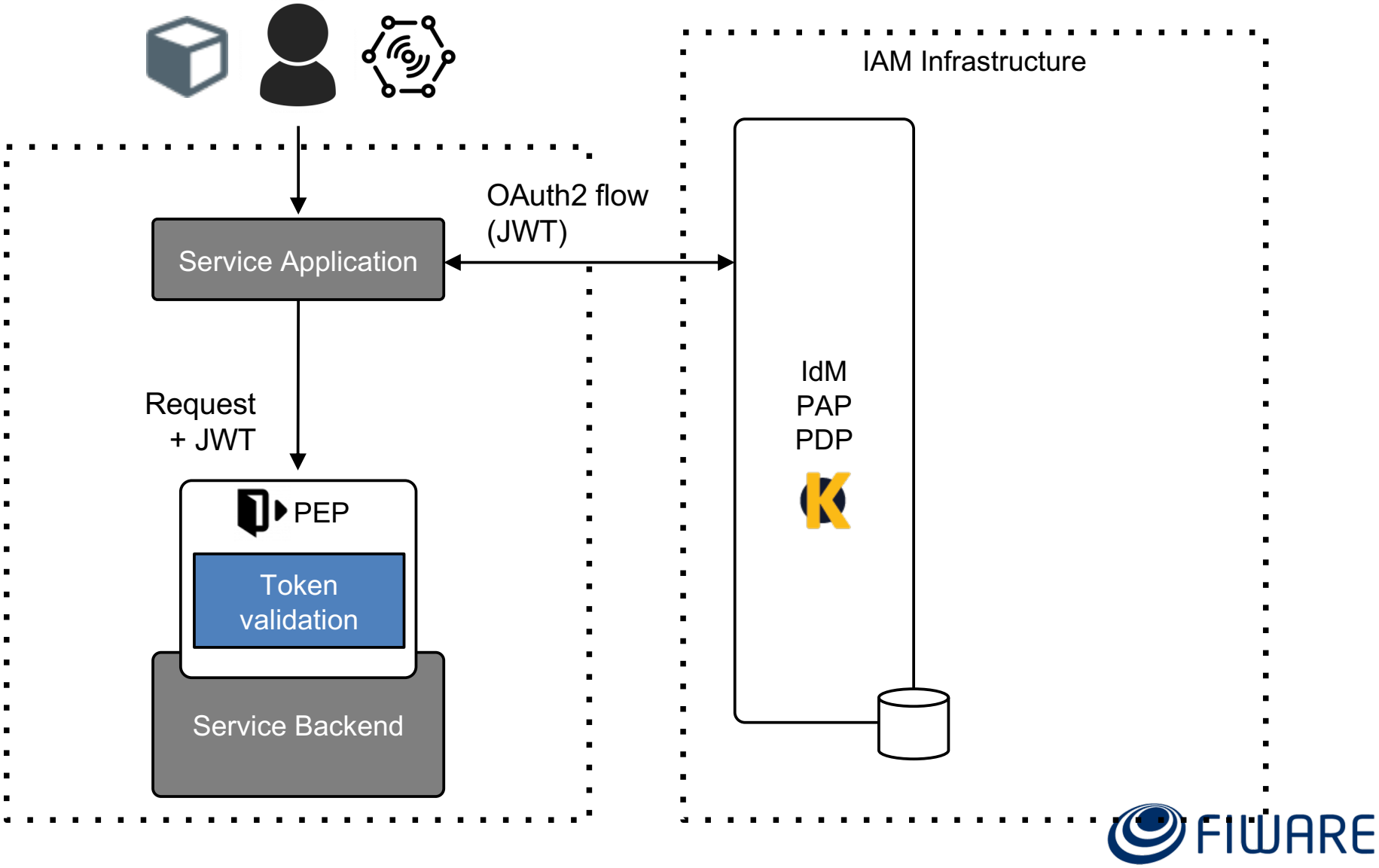
```
{
  "alg": "HS256",
  "typ": "JWT"
}
{
  "id": 1,
  "displayName": "Demo user",
  "email": "demo@fiware.org",
  "roles": [
    {
      "id": 15, "name": "Manager"
    }
  ],
  "organizations": [
    {
      "id": 12,
      "name": "Universidad Politecnica de Madrid",
      "roles": [
        {
 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

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

FIWARE

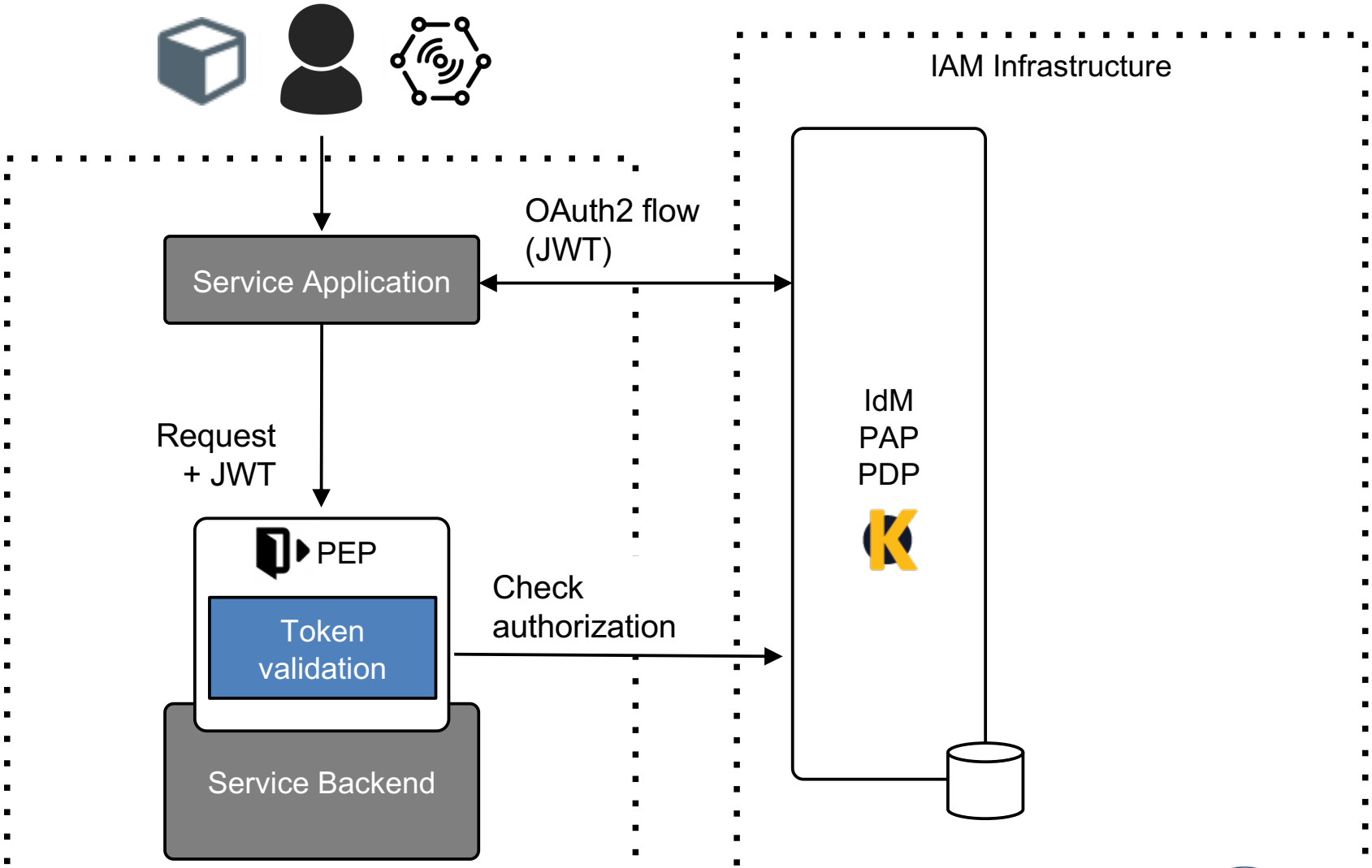
Identity and AC Management

JSON Web Tokens



Identity and AC Management

JSON Web Tokens



Keyrock
Identity attributes

- Definition of custom attributes in users' profile
  - List of attributes configurable in config file
  - Users can define the values in the UI
- The attributes are included in the users' profile returned when validating a token
- Service providers can use them for personalizing the services

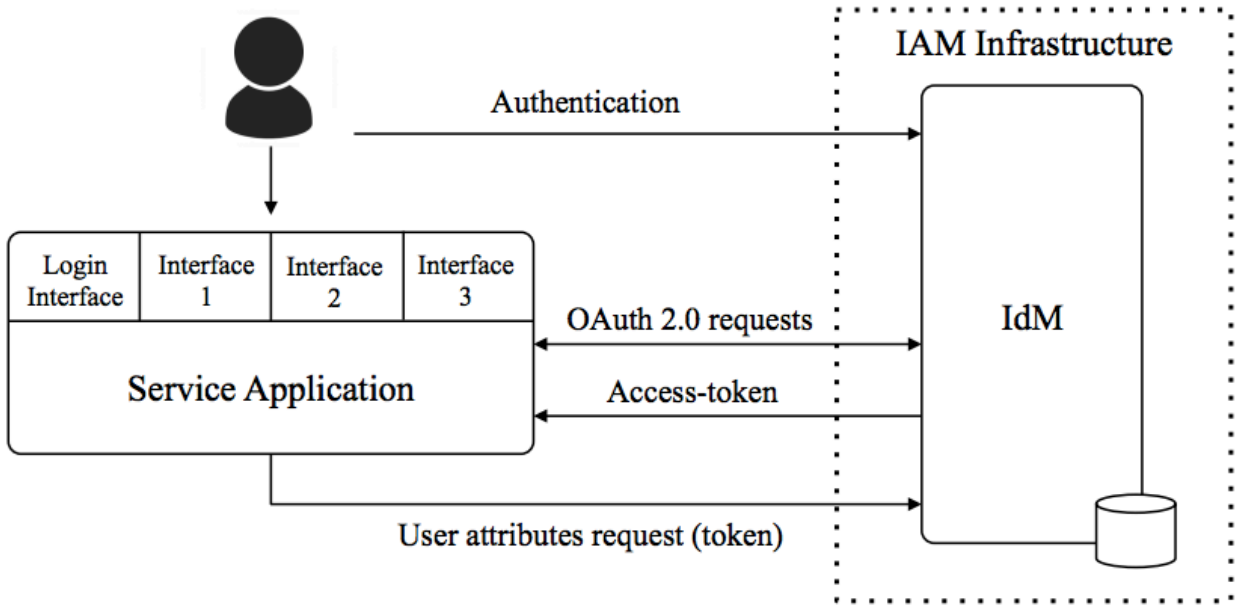
- Typical use case -> Accessibility

  Research paper published at https://doi.org/10.3390/app9183813

FIWARE

Keyrock
Identity attributes

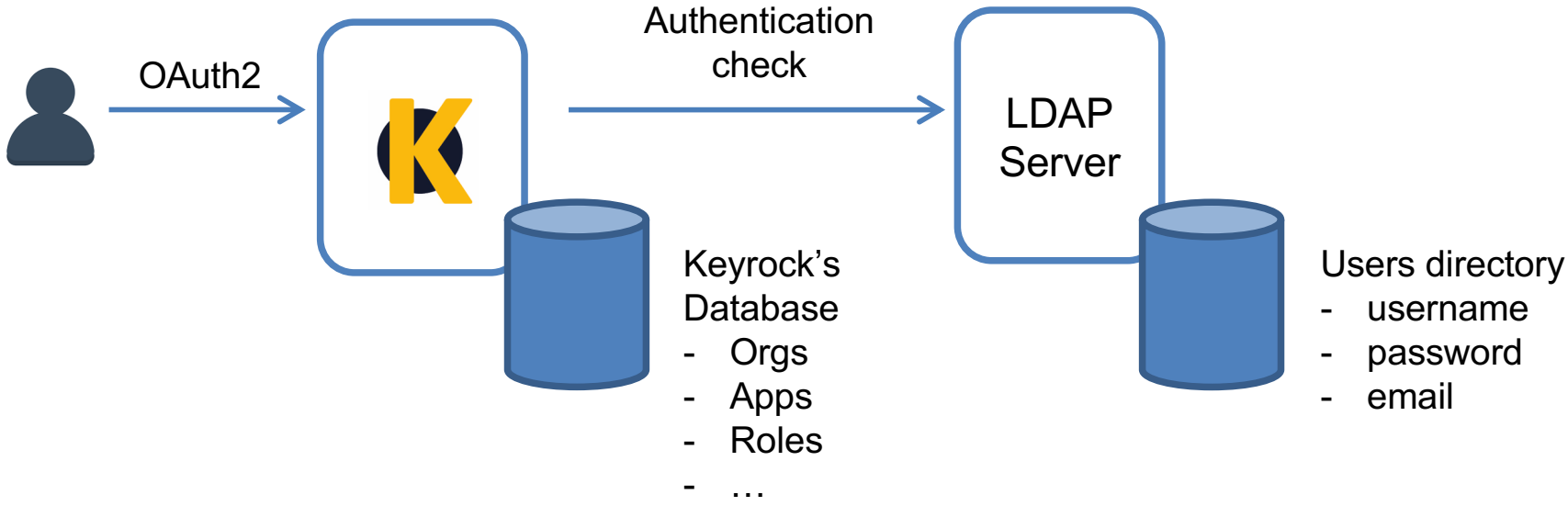
- Typical use case -> Accessibility
  - Provide interfaces adapted to the users' functional capabilities



FIWARE

Keyrock
External DB Authentication

- SQL/LDAP External Authentication Driver

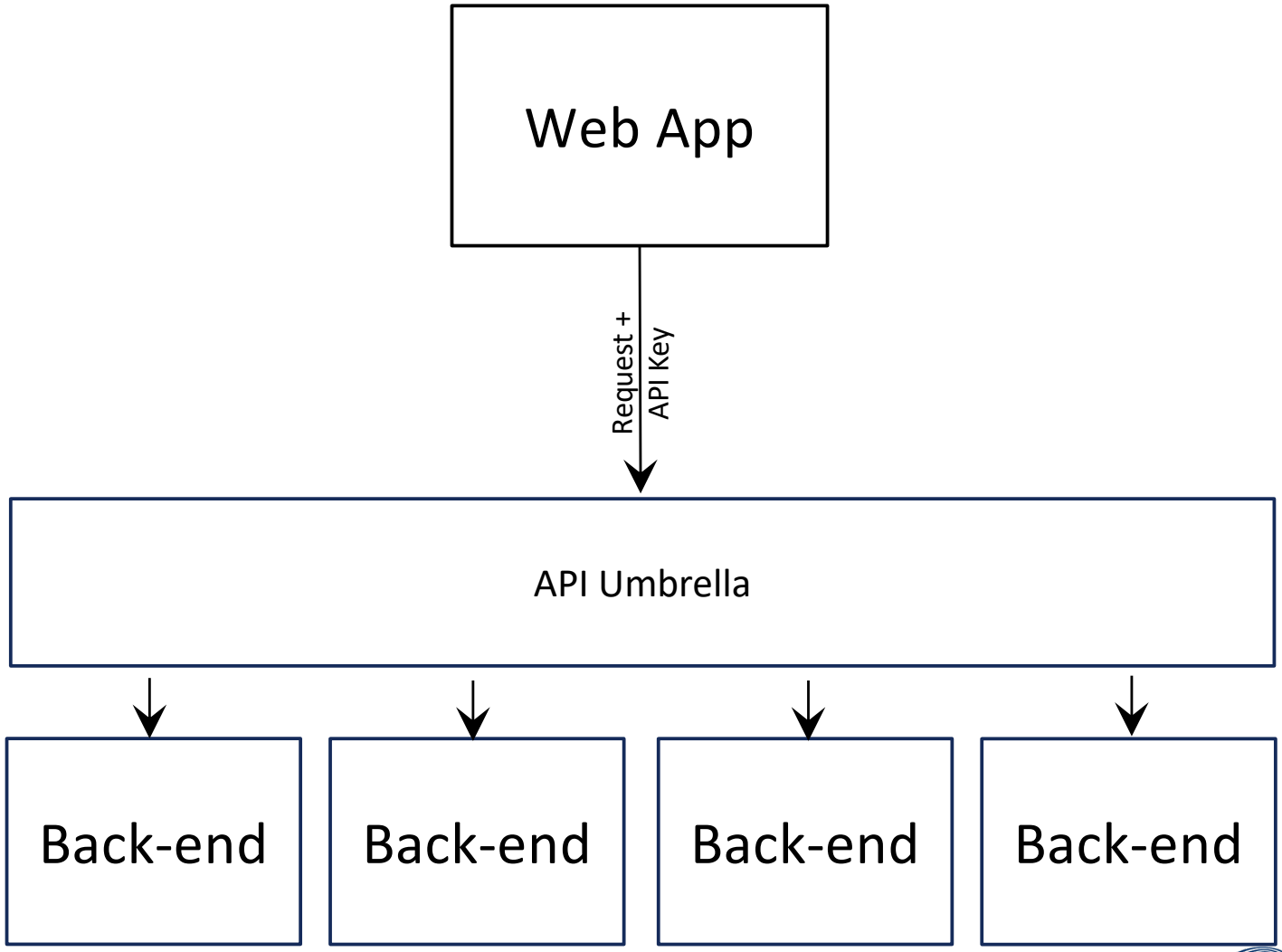


- Documentation available
  - https://fiware-idm.readthedocs.io/en/latest/installation_and_administration_guide/configuration/index.html#external-authentication-ldap

FIWARE

API Management

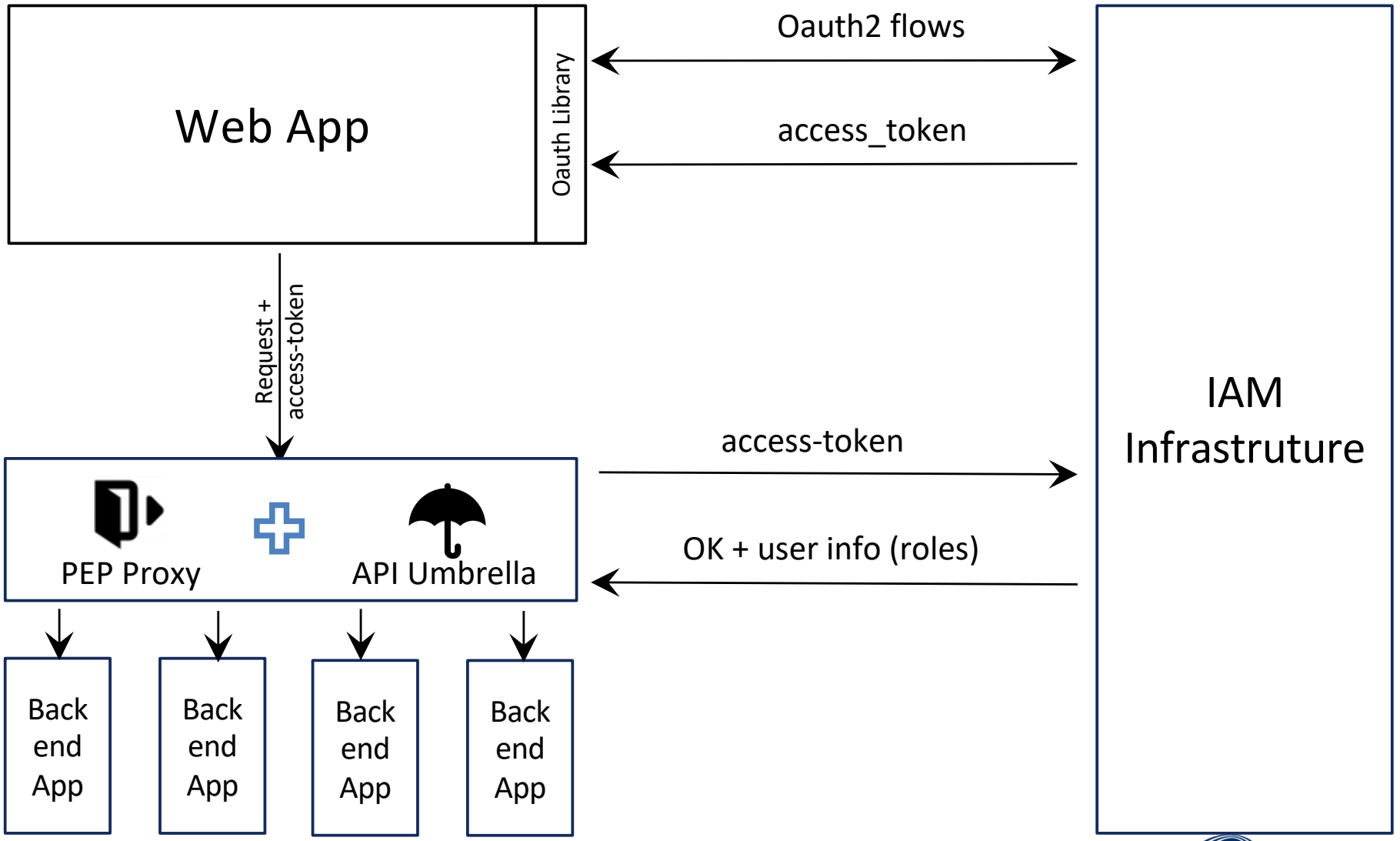
API Umbrella & PEP Proxy



FIWARE

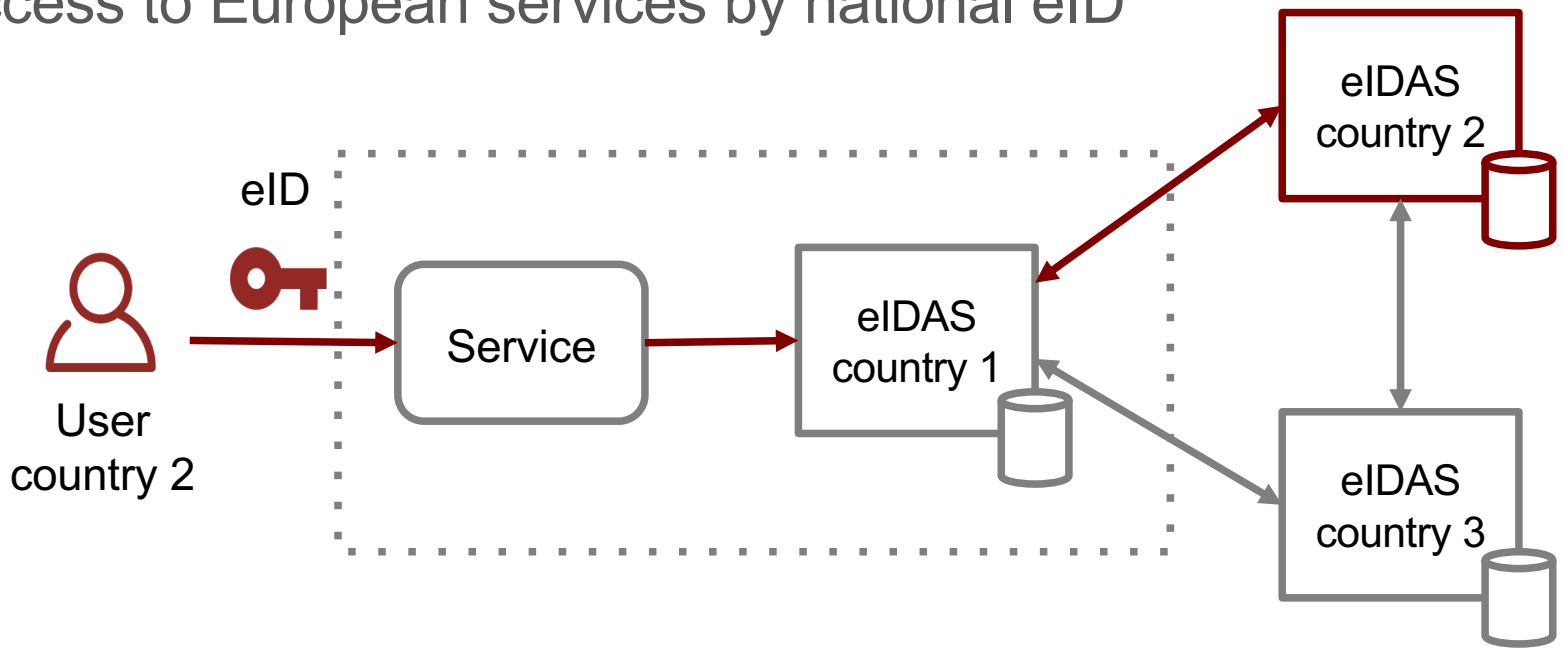
API Management

API Umbrella & PEP Proxy



eID Integration
CEF eIDAS

- **eIDAS** (electronic IDentification, Authentication and trust Services) is an EU regulation to enable secure and seamless electronic interactions between businesses, citizens and public authorities.
- Access to European services by national eID



FIWARE

eID Integration
FIWARE Identity Gateway

- Integration of FIWARE Security Framework with eIDAS
- Every application registered in Keyrock can be linked to a eIDAS node
  - By an OAuth 2.0 – SAML2 gateway
- Users can then authenticate using their national eID
  - AC policies based on user eIDAS profile
- Transparent for applications providers

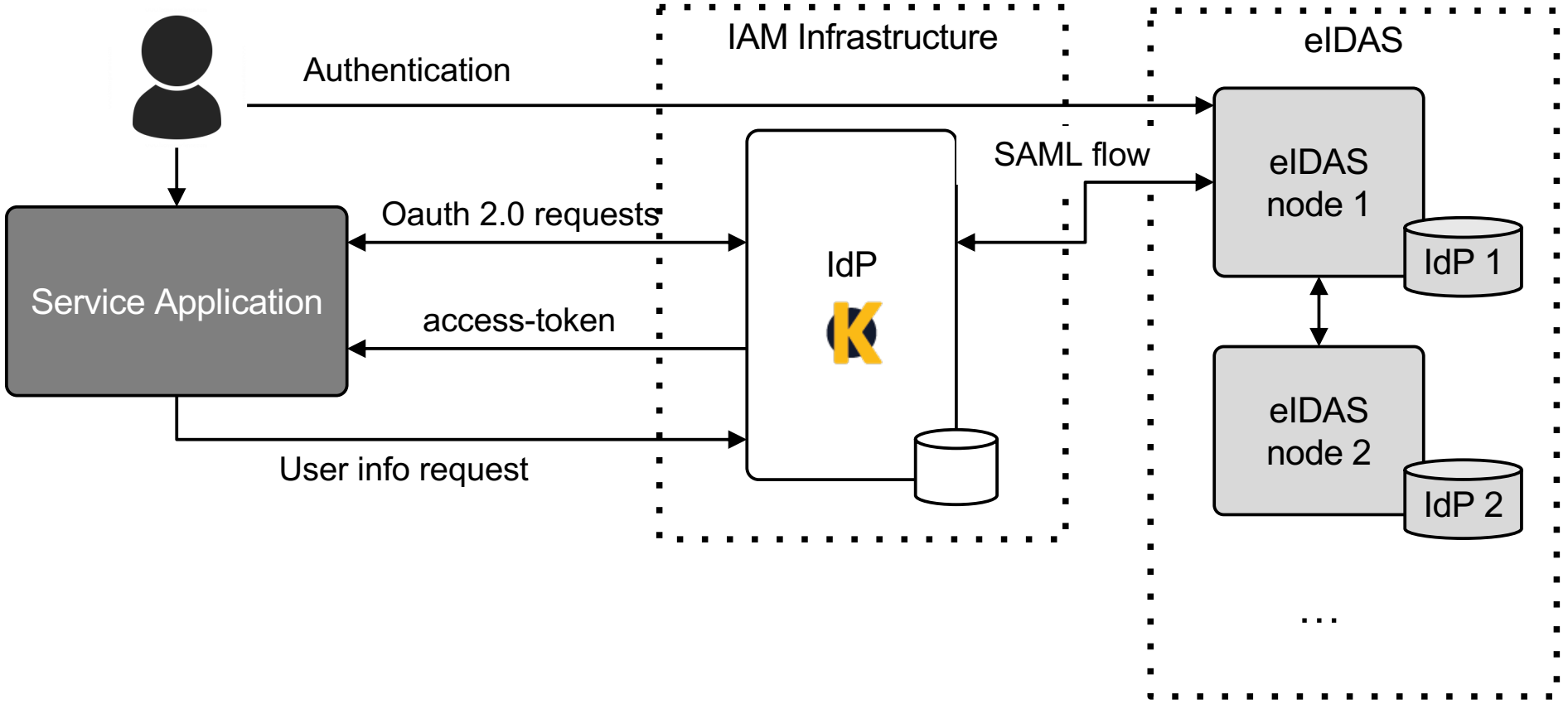
Co-financed by the Connecting Europe Facility of the European Union

eID FIWARE CEF

FIWARE

eID Integration

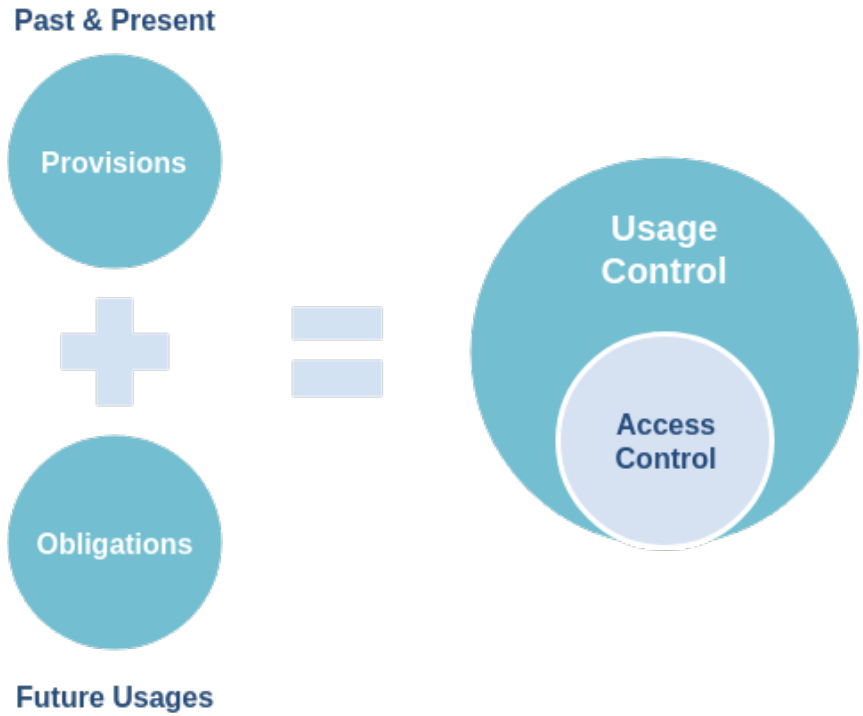
FIWARE Identity Gateway



FIWARE

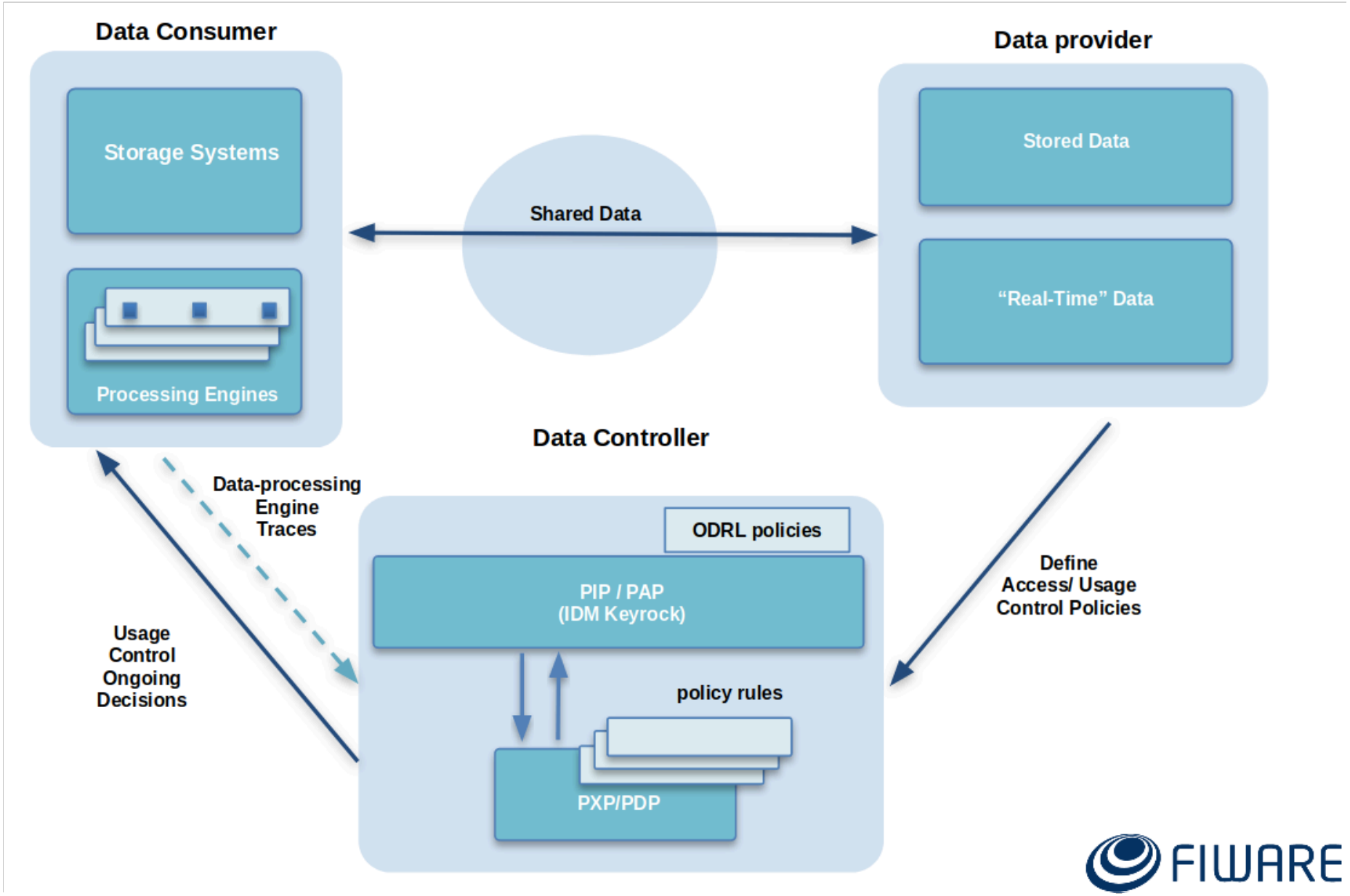
Data Usage Control

- Security Framework and **Data Usage Control**
  - Ensures data **sovereignty**
  - Regulates what is **allowed to happen** with the data (future usage).
- Integration with **Big Data** and **Processing GEs**



FIWARE

Data Usage Control



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

Thank you!

http://fiware.org
Follow @FIWARE on Twitter