

FIWARE
**Global
Summit**

Keyrock deep-dive

Alejandro Pozo Huertas – alejandro.pozo@upm.es

Universidad Politécnica de Madrid

FIWARE Security Team

Vienna, Austria
12-13 June, 2023
#FIWARESummit

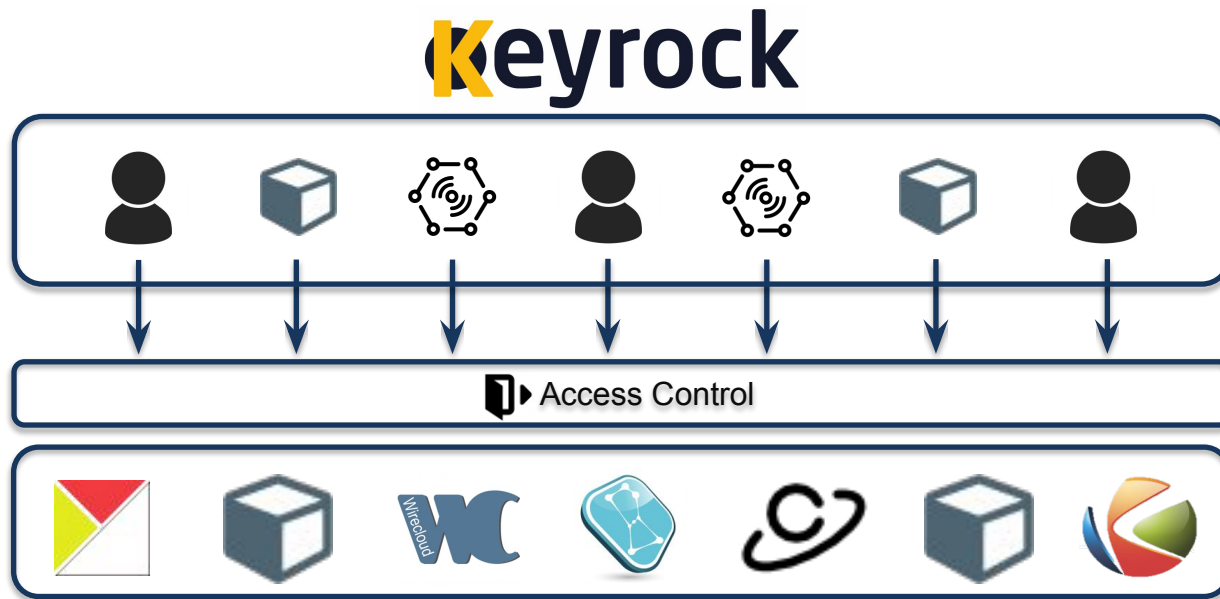
From Data to Value

OPEN SOURCE
OPEN STANDARDS
OPEN COMMUNITY



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**.

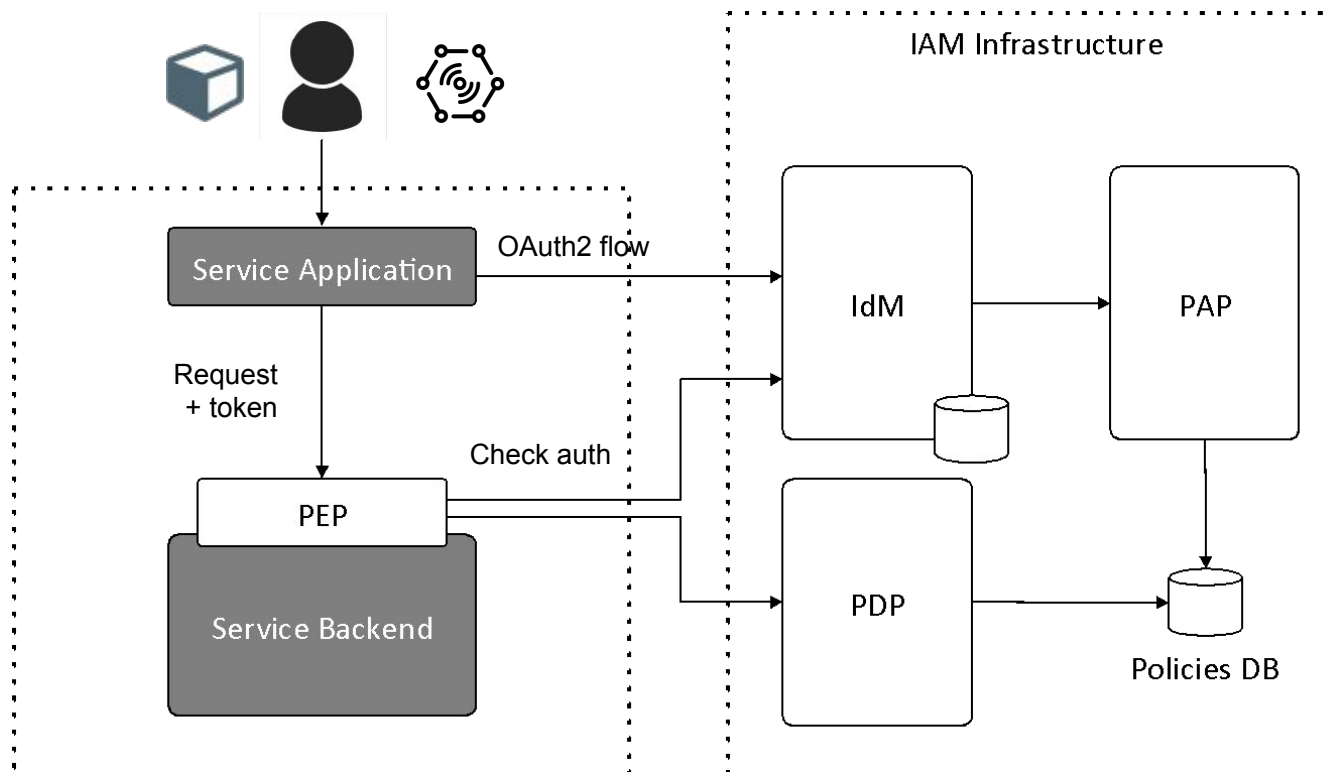


Keyrock

IDENTITY MANAGER

<https://keyrock-fiware.github.io>

Identity and AC Management



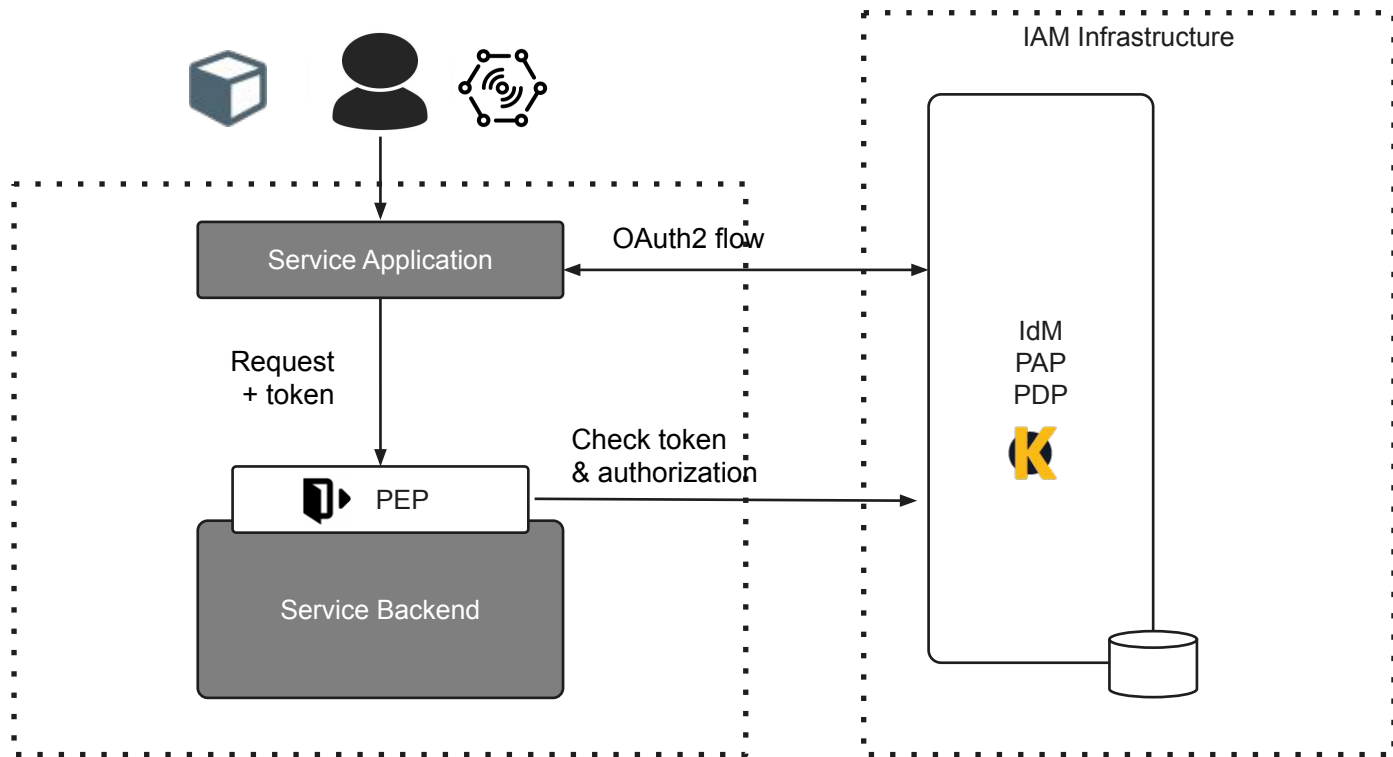
Keyrock deep-dive

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

Using Keyrock as PDP

Using Keyrock as PDP

Architecture



Using Keyrock as PDP Views

Keyrock Identity Manager admin

Main menu

- Home
- Organizations
- Applications
- Notify
- Administrators
- Users

Canarias app

edit manage roles

Description

FIWARE Summit Canarias app

Url

http://localhost

Callback Url

http://localhost/login

OAuth2 Credentials ^


?

PEP Proxy ^

?

IoT Sensors ^

?



Using Keyrock as PDP Views

Keyrock Identity Manager admin

Main menu

- Home
- Organizations
- Applications
- Notify
- Administrators
- Users

Manage Roles

Roles

Provider

Purchaser

Permissions

Get and assign only public owned roles

✓ Get and assign all public application roles

Manage authorizations

Manage roles

Manage the application

Get and assign all internal application roles

Save

Using Keyrock as PDP Views

The screenshot shows the Keyrock Identity Manager interface with a 'Create permission' modal dialog open. The dialog has a title bar with a close button (X). The form inside the dialog contains the following fields and options:

- Permission Name:** A text input field containing 'Comments creator'.
- Description:** A text input field containing 'Enables to create new comments'.
- HTTP Verb, Resource Rule and Authorization Headers:** A section header.
- HTTP action:** A text input field containing 'POST'.
- Resource:** A text input field containing '/comments'.
- Is regular expression?:** An unchecked checkbox.
- Authorization Service Header:** A text input field.
- Use Authorization Service Header:** An unchecked checkbox.
- Save:** A dark blue button at the bottom right of the dialog.

The background interface shows a sidebar with a 'Main menu' containing links for Home, Organizations, Applications, Notify, Administrators, and Users. The top right corner shows the user 'admin'.

Using Keyrock as PDP

Checking authorization

Request

```
GET /user
?access_token=2YotnFZFEjr1zCsicMwpAA
&action=POST
&resource=comments
&app_id=958c495a-58ea-4167-b8a9-562b2f923426
```

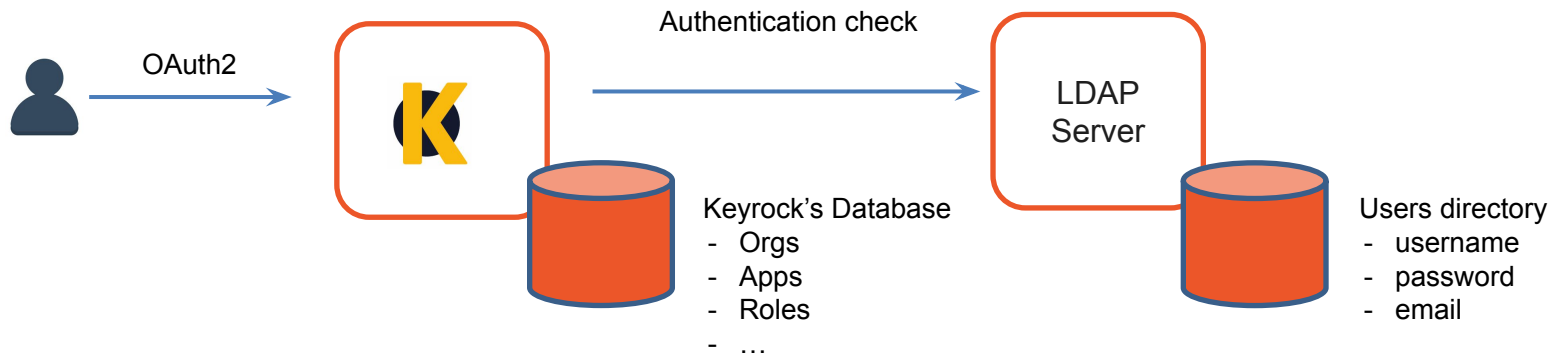
Response

```
{
  "organizations": [],
  "displayName": "Alvaro Alonso",
  "roles": [
    {
      "id": "9c4e8db4-a56b-4731-bfc6-7dd8fb2fbea3",
      "name": "creator"
    }
  ],
  "app_id": "958c495a-58ea-4167-b8a9-562b2f923426",
  "email": "alvaroalonso@test.com",
  "id": "63b522f7-079b-44b1-babb-20dcf8b88dd5",
  "authorization_decision": "Permit",
  "app_azf_domain": "",
  "username": "alvaroalonso"
}
```

External authentication

External 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

External authentication

Configuration file

```
// External user authentication with LDAP
// Testing credentials from https://www.forumsys.com/tutorials/integration-how-to/ldap/online-ldap-test-server/
config.external_auth_ldap = {
  enabled: false,
  id_prefix: 'external_ldap_',
  database: {
    host: 'ldap.forumsys.com',
    port: 389,
    reader_dn: 'cn=read-only-admin,dc=example,dc=com',
    reader_password: 'password',
    suffix: 'dc=example,dc=com',
    idAttribute: 'uid',
    usernameAttribute: 'uid',
    emailAttribute: 'mail'
  }
}
```

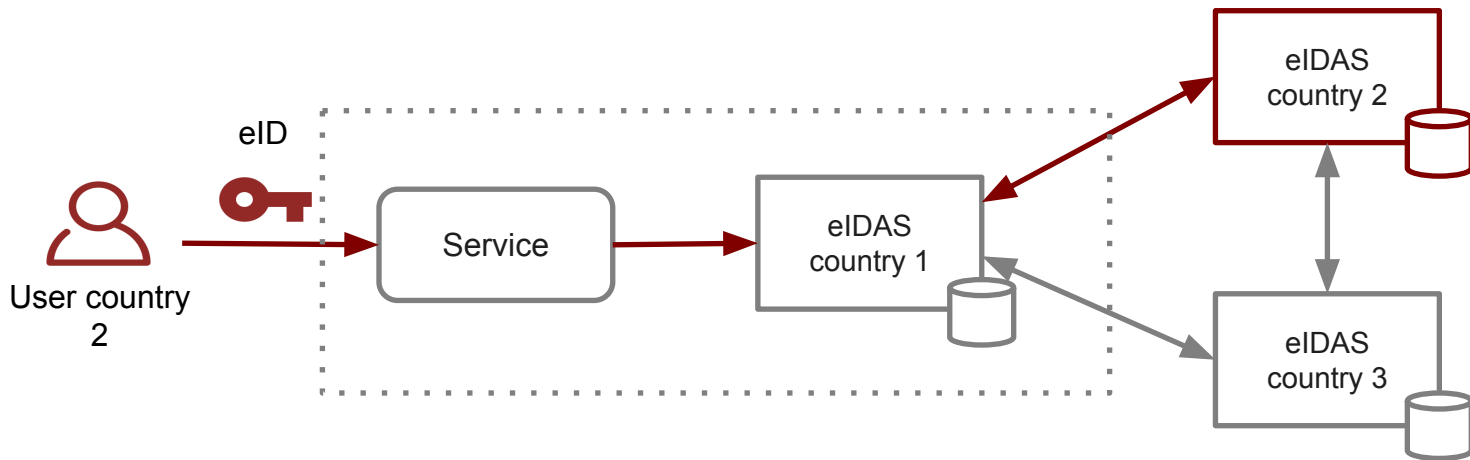
European Digital Identity eIDAS

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



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

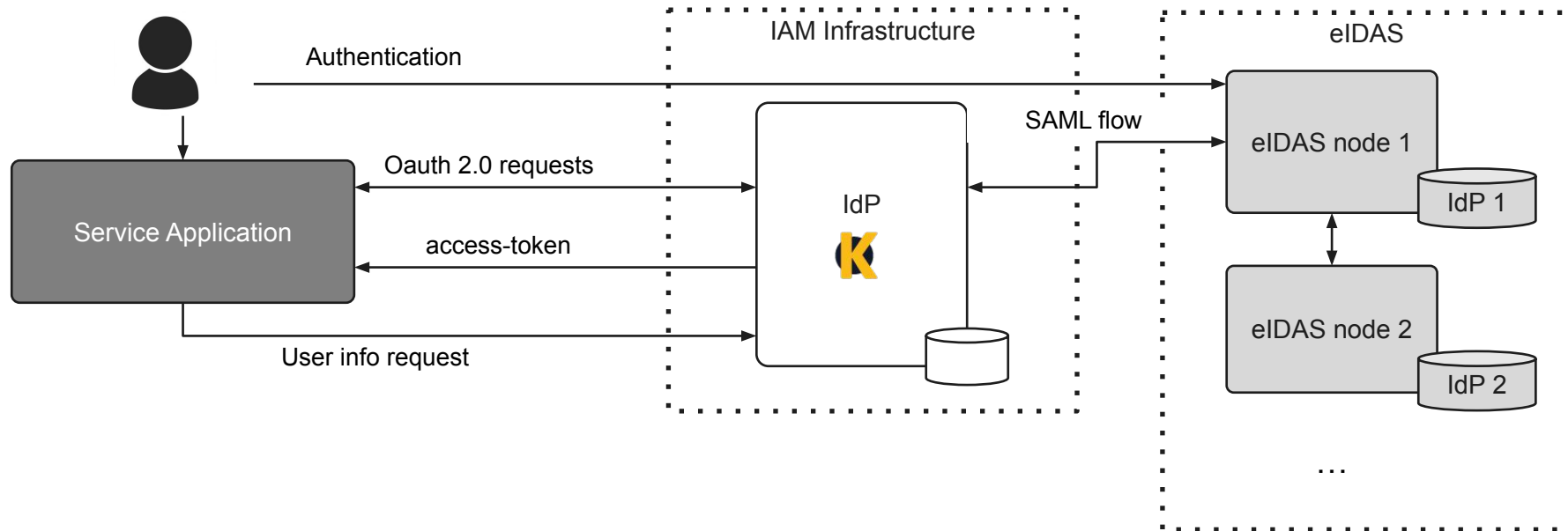


Co-financed by the Connecting Europe
Facility of the European Union



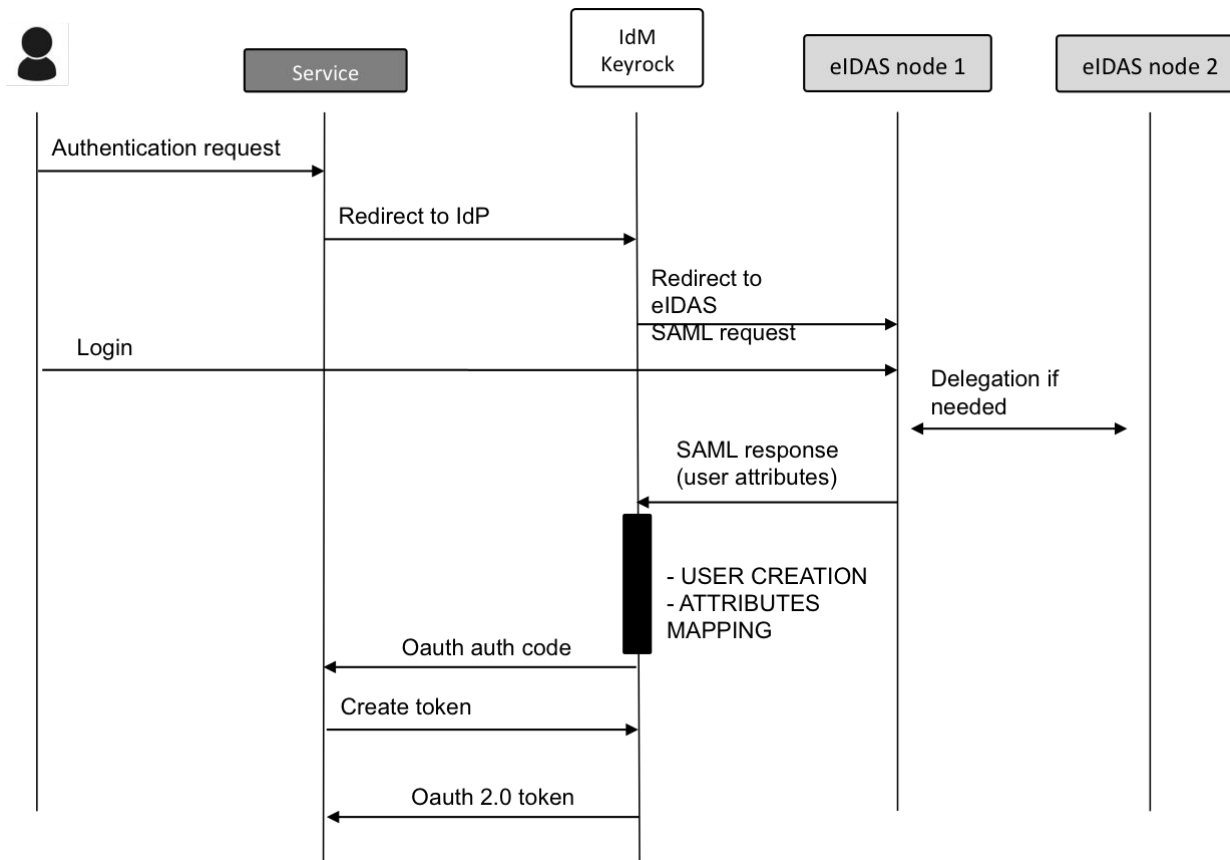
eID Integration

FIWARE Identity Gateway



eID Integration

Authentication flow



eID Integration

Configuration in Keyrock

```
config.eidas = {  
    enabled: true,  
    gateway_host: 'localhost',  
    node_host: 'https://eidas.node.es/EidasNode',  
    metadata_expiration: 60 * 60 * 24 * 365 // One year  
};
```

eID Integration

Creating an application with eID enabled

1

2

3

eIDAs Information

Support Contact Person

Name	Surname
<input type="text"/>	<input type="text"/>
Email	Telephone Number
<input type="text"/>	<input type="text"/>
Company	
<input type="text"/>	

Technical Contact Person

Name	Surname
<input type="text"/>	<input type="text"/>
Email	Telephone Number
<input type="text"/>	<input type="text"/>
Company	
<input type="text"/>	

Organization

Name	Url
<input type="text"/>	<input type="text"/>
NIF	
<input type="text"/>	

Next

eID Integration

Authenticating users



Application with eIDAS connection

Application with eIDAS connection

Log In

Email

Password

☐ remember me

Sign with eID

Sign In

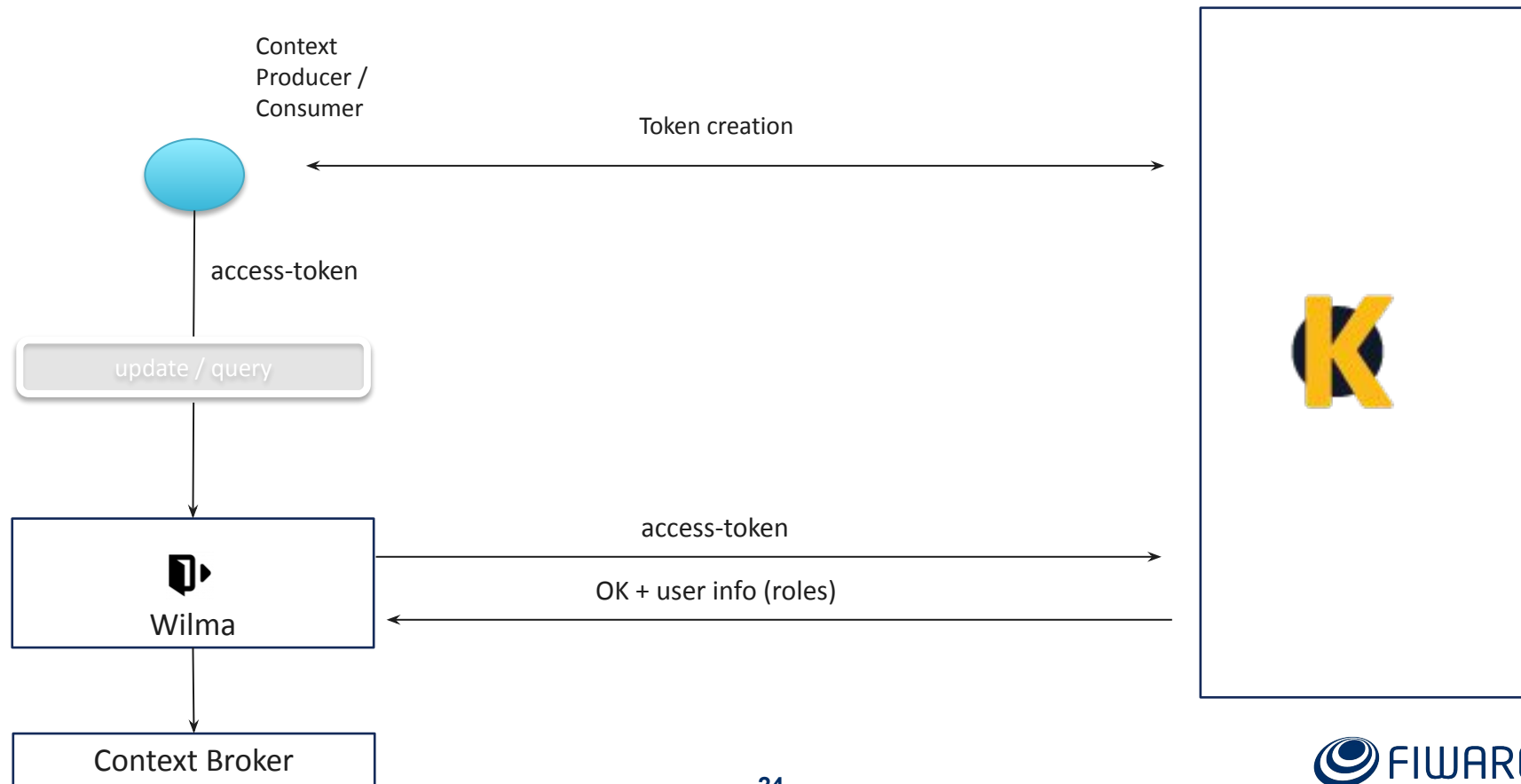
[Sign up](#)

[Forgot password](#)

[Confirmation not recieved?](#)

Securing IoT devices access to your services

Securing IoT devices



Securing IoT devices

Registering a sensor in Keyrock


keyrock Identity Manager admin

Main menu

- Home
- Organizations
- Applications
- Notify
- Administrators
- Users

Canarias app

edit manage roles



Description

FIWARE Summit Canarias app

Url

http://localhost

Callback Url


http://localhost/login

OAuth2 Credentials ^ ?

PEP Proxy ^ ?


IoT Sensors v ?

Register a new IoT Sensor



Securing IoT devices

Registering a sensor in Keyrock

 Identity Manager admin

Main menu

Home

Organizations

Applications

Notify

Administrators

Users

Canarias app

edit

manage roles

Description

FIWARE Summit Canarias app

Url

http://localhost

Callback Url

http://localhost/login

OAuth2 Credentials ^

PEP Proxy ^

IoT Sensors v

Id of Sensor

lot_sensor_7a54ae32-481c-45a8-afb4-8bf49f6b0cf2


Reset password

Delete

Password of Sensor

lot_sensor_930c89b2-0694-43be-9684-79d1087f2eb7

Register a new IoT Sensor



Securing IoT devices

- OAuth 2.0 grant types

- **Authorization Code Grant**

- Web applications
 - Redirection to IdP page
 - Access-Token provided on server side

- **Implicit Grant**

- Similar to Authorization Code Grant
 - But Access-Token provided directly

- **Resource Owner Password Credentials Grant**

- Without browser redirection
 - Credentials shared with the service

- **Client Credentials Grant**

- Authentication using service credentials

Securing IoT devices

- OAuth 2.0 grant types

- **Authorization Code Grant**

- Web applications
 - Redirection to IdP page
 - Access-Token provided on server side

- **Implicit Grant**

- Similar to Authorization Code Grant
 - But Access-Token provided directly

- **Resource Owner Password Credentials Grant**

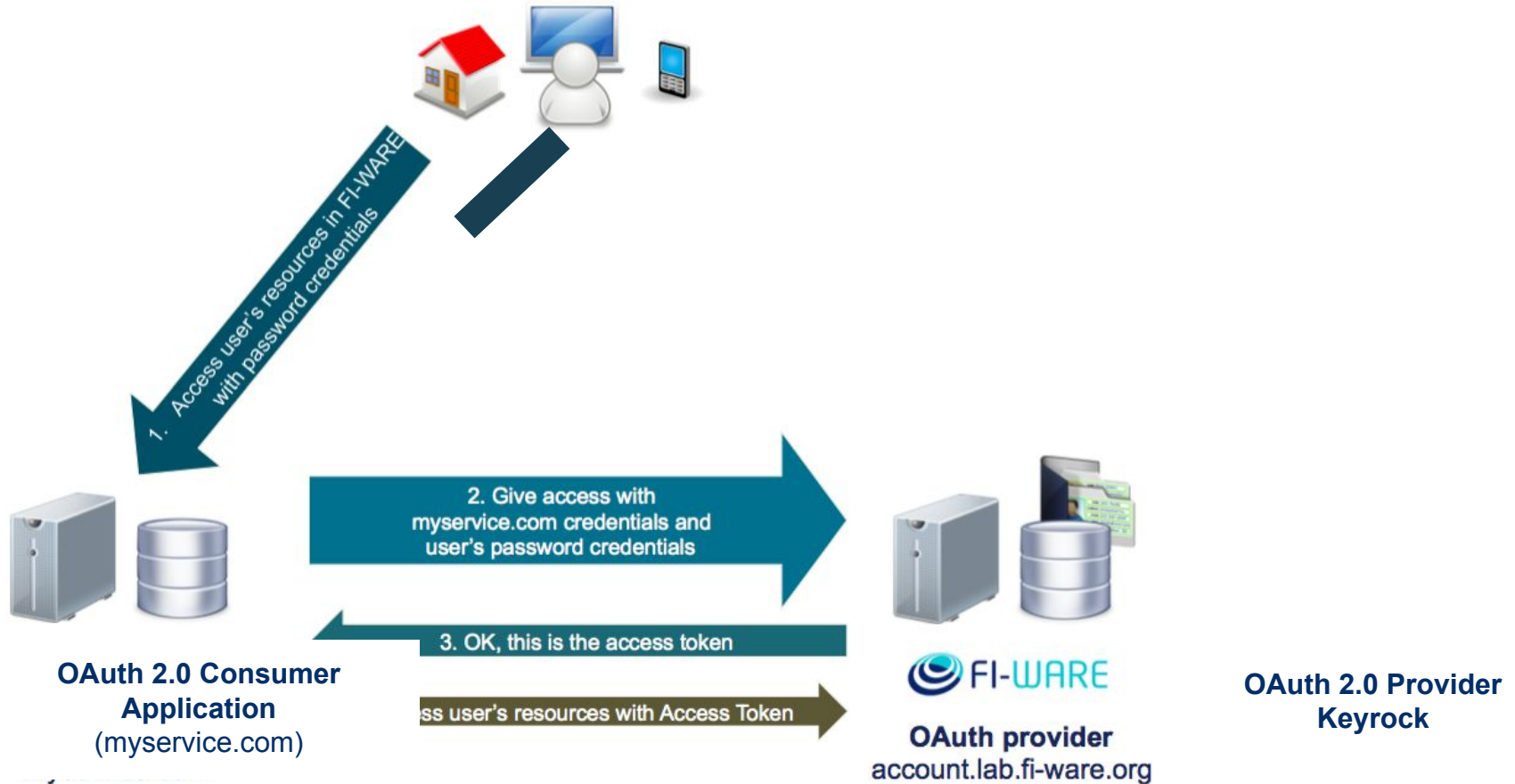
- Without browser redirection
 - Credentials shared with the service

- **Client Credentials Grant**

- Authentication using service credentials

Securing IoT devices

Resource Owner Password Credentials Grant



Securing IoT devices

Resource Owner Password Credentials Grant

Access Token Request

```
POST /oauth2/token HTTP/1.1
Host: keyrock-host
Authorization: Basic kDGas2jjcoa21879Qjco
Content-Type: application/x-www-form-urlencoded

grant_type=password&username=USER&password=PASSWORD
```

Authorization:

Base64(ClientId:ClientSecret)

Securing IoT devices

Resource Owner Password Credentials Grant

Access Token Response

```
HTTP/1.1 200 OK
Transfer-Encoding: chunked
Content-Type: application/json

{
  "access_token": "BuKHtSDdsak323XsL09UGub",
  "token_type": "Bearer",
  "expires_in": 3600,
  "refresh_token": "zHDSd07VmoYGfdasf21aAgAKor"
}
```

Identity attributes

Identity attributes

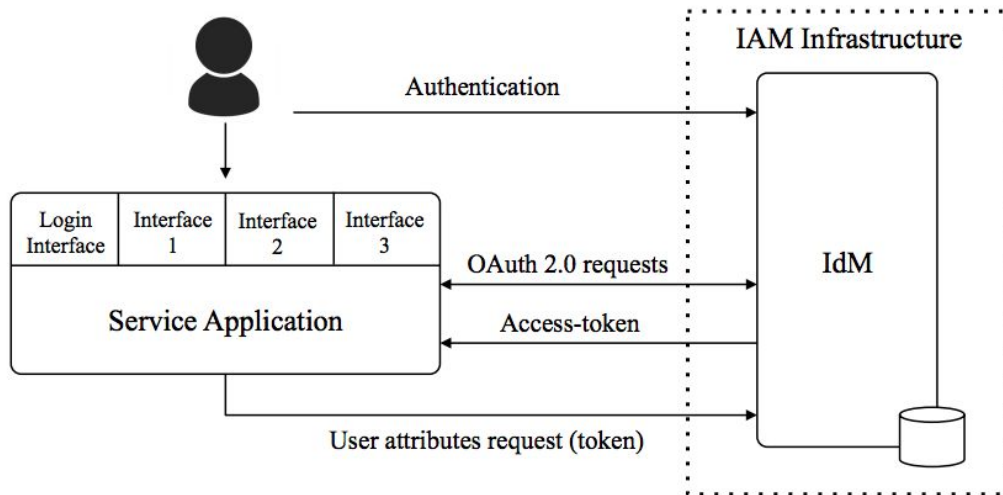
- Definition of custom attributes in users' profile
 - List of attributes configurable in config file
 - Users can define the values in the UI
- The attributes are included in the users' profile returned when validating a token
- Service providers can use them for personalizing the services
- Typical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

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

Identity attributes

Typical use case -> Accessibility

Provide interfaces adapted to the users' functional capabilities



Identity attributes

Definition in configuration file

```
// Enables the possibility of adding identity attributes in users' profile
config.identity_attributes = {
  enabled: true,
  attributes: [
    {name: 'Vision', key: 'vision', type: 'number', minVal: '0', maxVal: '100'},
    {name: 'Color Perception', key: 'color', type: 'number', minVal: '0', maxVal: '100'},
    {name: 'Hearing', key: 'hearing', type: 'number', minVal: '0', maxVal: '100'},
    {name: 'Vocal Capability', key: 'vocal', type: 'number', minVal: '0', maxVal: '100'},
    {name: 'Manipulation Strength', key: 'manipulation', type: 'number', minVal: '0', maxVal: '100'},
    {name: 'Reach', key: 'reach', type: 'number', minVal: '0', maxVal: '100'},
    {name: 'Cognition', key: 'cognition', type: 'number', minVal: '0', maxVal: '100'}
  ]
}
```

Identity attributes

Assignment in user profile

Keyrock Identity Manager User 43

Identity attributes

Attribute	Value (%)
Vision	100
Color Perception	
Hearing	
Vocal Capability	
Manipulation Strength	
Reach	
Cognition	

Update User

Identity attributes

Returned when validating OAuth 2.0 token

```
1  {
2    "id": "bdfd8f23-44be-41eb-95ff-58280cbd04a0",
3    "displayName": "User 4",
4    "description": "This is a testing user for validating the use of identity attributes in KeyRock.",
5    "image": "",
6    "email": "user4@test.com",
7    "app_id": "5cf95a5d-dd95-4ad1-ae9c-08440c9cbf56",
8    "roles": [{
9      "id": "0146dd11-125a-2e2f-915a-0a228d532aab",
10     "name": "test_role_1"
11   }],
12   "attributes": {
13     "color": "0",
14     "reach": "0",
15     "vocal": "0",
16     "vision": "100",
17     "hearing": "0",
18     "cognition": "0",
19     "manipulation": "0"
20   }
21 }
```

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>

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)



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*



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.



Find Us On



Stay up to date

JOIN OUR NEWSLETTER

Be certified and featured



FIWAREMarketplace

Hosting Partner



vienna
business
agency

Keystone Sponsors



Media Partners



FIWARE
**Global
Summit**

Thanks!

Vienna, Austria
12-13 June, 2023
#FIWARESummit

