Open APIs for Open Minds

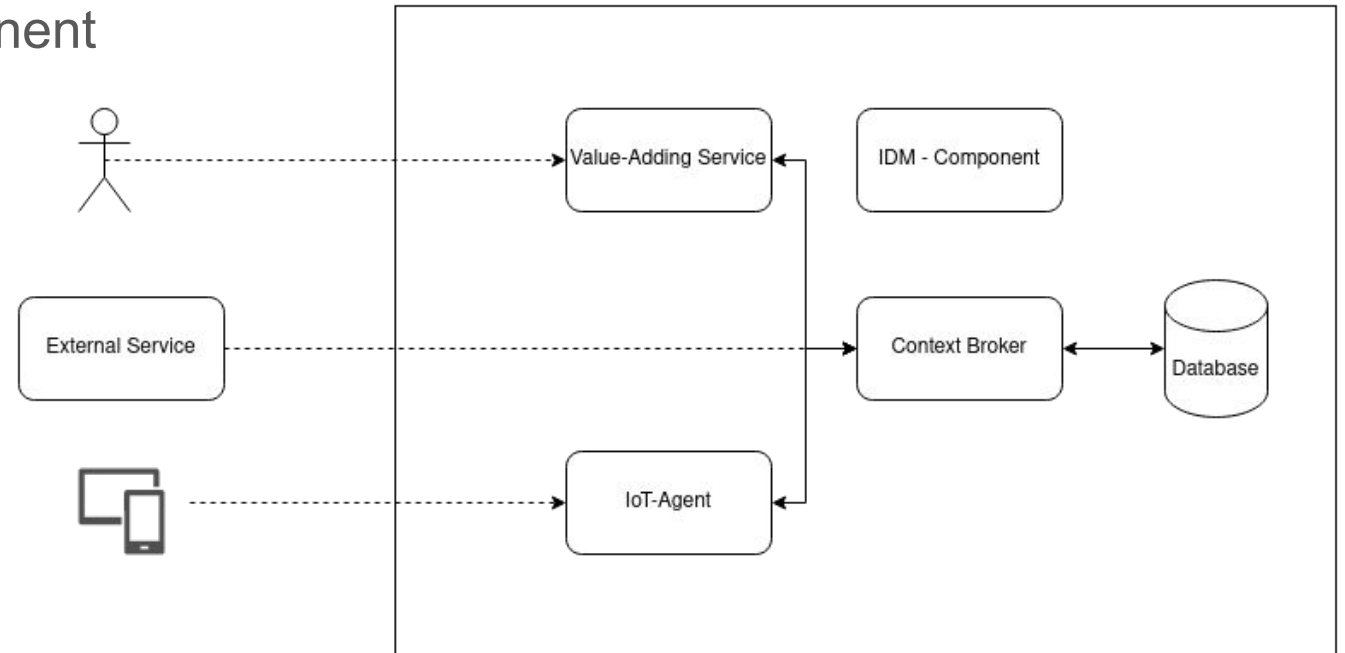# Kong, Keyrock, Keycloak, i4Trust - Options to secure FIWARE in production

Jason Fox, Senior Technical Evangelist
FIWARE Foundation

FIWARE

Role of an API-Gateway in FIWARE platforms

- Context Broker as the central component

- Contacted:
  - from different external actors
  - from different internal actors
  - with different loads

- No "self-defense" mechanism

We need a component to protect the platform

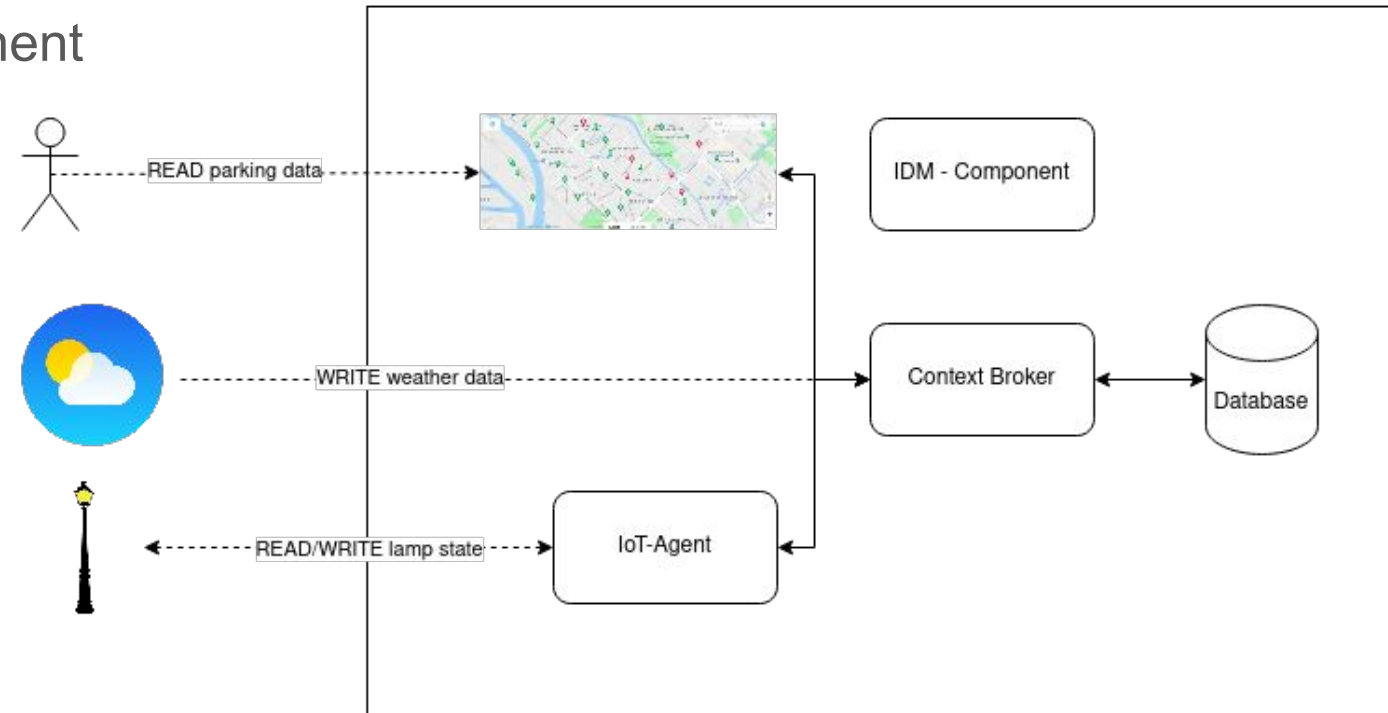# Role of an API-Gateway in FIWARE platforms

- Context Broker as the central component

- Contacted:

  - from different external actors

  - from different internal actors

  - with different loads

- No "self-defense" mechanism

We need a component to protect the platform

FIWARE

Role of an API-Gateway in FIWARE platforms

- Access control: PEP-Proxy & Policy-decision Point

  - Allow to control who can access what

- Additional requirements:

  - Rate-limiting?

  - Usage-Control?

  - Monitoring?

API-Gateway as the central entry point can provide those capabilities

FIWARE

Role of an API-Gateway in FIWARE platforms
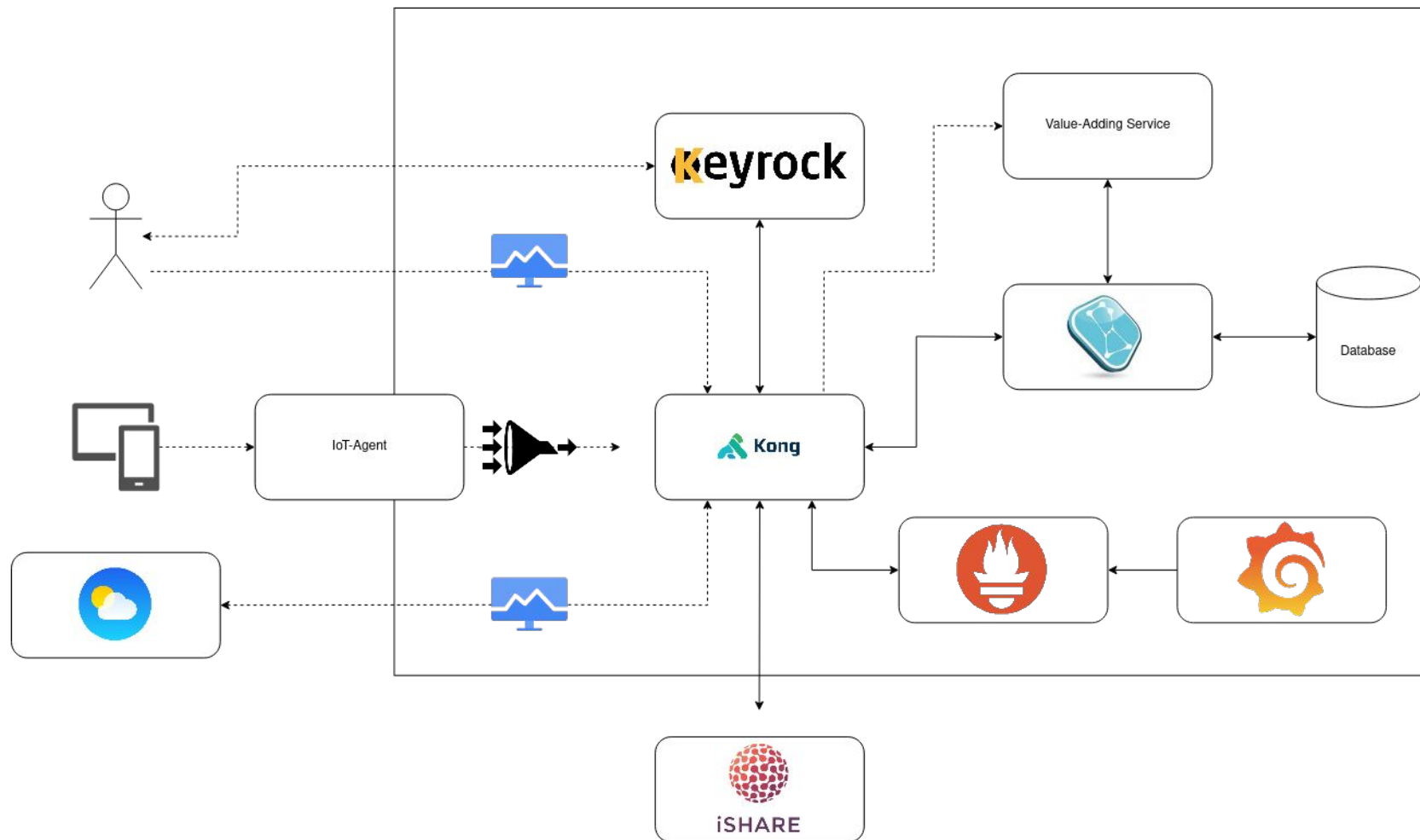
Why Kong?

- One of the most popular and adopted solutions in the market

- OpenSource(and Enterprise) Version available, maintained by a huge and active community

- Production ready deployment tools

- Plugin-support:

  - FIWARE specific functionality can be implemented as plugin

  - Supports various languages, e.g lua, go and python

- Plugins for the additional requirements available - Kong Hub:

  - Rate-limiting

  - Usage monitoring

FIWARE

Why Kong?

Kong Plugin Hub

Extend Kong Konnect with powerful plugins and easy integrations

All Plugins
Konnect
Third-Party

SUBSCRIPTION TIERS

Free
Plus
Enterprise

FUNCTIONALITY

Authentication
Security
Traffic Control
Serverless
Analytics & Monitoring
Transformations
Logging
Deployment

Authentication

ENTERPRISE

Portal Application Registration

Allow portal developers to register applications against Services

Support by:
Kong Inc.

Basic Authentication

Add Basic Authentication to your Services

Support by:
Kong Inc.

HMAC Authentication

Add HMAC Authentication to your Services

Support by:
Kong Inc.

JWT

Verify and authenticate JSON Web Tokens

Support by:
Kong Inc.

ENTERPRISE
PLUS

Kong JWT Signer

Verify and sign one or two tokens in a request

Support by:
Kong Inc.

Key Authentication

Add key authentication to your Services

Support by:
Kong Inc.

FIWARE

Running Kong

- Multiple solutions available: Kong - Install and run

- Running with Helm on OpenShift:

  - Kong in the FIWARE demo environment

- Some details about the demo environment:

  - Uses the official Kong Helm-Chart

  - Extended with support for OpenShift routes

  - Pre-built image from FIWARE, already including the plugins

  - Declarative configuration via ConfigMap

  - Applied via GitOps - ArgoCD

FIWARE

Kong as PEP-Proxy

- Plugins for using Kong as a PEP in FIWARE:

  - ngsi-ishare-policies to enforce iTrust compliant authz/n

  - Keyrock as PDP - delegate role-based decisions to Keyrock

  - Keycloak as PDP - delegate decisions to Keycloak

  - External-Authz - delegate decisions to a compliant endpoint, for example the DSBA-PDP to support Verifiable Credentials

FIWARE

General plugin configuration

```
kong:
    …
    env:
        …
        plugins: bundled,pep-plugin,ngsi-ishare-policies
        pluginserver_names: pep-plugin
        pluginserver_pep_plugin_start_cmd: "/go-plugins/pep-plugin"
        pluginserver_pep_plugin_query_cmd: "/go-plugins/pep-plugin -dump"
        …
    dblessConfig:
        configMap: kong-configmap
```

General plugin configuration

```
services:
-   host: "fiware-orion-ld"
    name: "orion-keyrock"
    port: 1026
    protocol: http

    routes:
    -   name: orion-keyrock
        paths:
        -   /keyrock
        strip_path: true

plugins:
-   name: pep-plugin
    config:
        <PLUGIN_SPECIFIC_CONFIGURATION>
```

Examples:
- i4Trust configuration
- Keyrock configuration

FIWARE

Keyrock configuration

```
# keyrock example
- host: "fiware-orion-ld"
  name: "orion-keyrock"
  port: 1026
  protocol: http

  routes:
    - name: orion-keyrock
      paths:
        - /keyrock
      strip_path: true

  plugins:

    - name: pep-plugin
      config:
        authorizationendpointtype: Keyrock
        authorizationendpointaddress: https://keyrock.fiware.dev/user
        keyrockappid: 7c902139-d4d0-461a-bb14-7fa29aa143fe

    - name: request-transformer
      config:
        remove:
          headers:
            - Authorization
            - authorization
```

FIWARE

i4Trust configuration

```
  # i4Trust example
- host: "fiware-orion-ld"
  name: "orion-i4trust"
  port: 1026
  protocol: http

  routes:
    - name: orion-i4trust
      paths:
        - /i4trust
      strip_path: true

  plugins:

    - name: ngsi-ishare-policies
      config:
        access_token:
          header_names:
            - "authorization"
            - "Authorization"
       ar:
          identifier: "EU.EORI.NL000000004"
          host: "https://ar.isharetest.net"
          token_endpoint: "https://ar.isharetest.net/connect/token"
          delegation_endpoint: "https://ar.isharetest.net/delegation"
        satellite:
          identifier: "EU.EORI.NL000000000"
          host: "https://scheme.isharetest.net"
          token_endpoint: "https://scheme.isharetest.net/connect/token"
          trusted_list_endpoint: "https://scheme.isharetest.net/trusted_list"
        jws:
          identifier: …
          private_key: …
          x5c: …
```

FIWARE

Keycloak configuration

```
# keycloak example
- host: "fiware-orion-ld"
  name: "orion-keycloak"
  port: 1026
  protocol: http

  routes:
    - name: orion-keycloak
      paths:
        - /keycloak
      strip_path: true

  plugins:
    - name: pep-plugin
      config:
        authorizationendpointtype: Keycloak
        authorizationendpointaddress: http://fiware-keycloak:80
        keycloakrealm: fiware-server
        keycloakclientid: orion-pep
        keycloakclientsecret: 978ad148-d99b-406d-83fc-578597290a79

    - name: request-transformer
      config:
        remove:
          headers:
            - Authorization
            - authorization
```

Keycloak Realm:
https://github.com/FIWARE-Ops/fiware-gitops/blob/master/aws/fiware/keycloak/templates/realmConfigMap.yaml

FIWARE

Rate-limiting

- Rate-limiting plugin:
  - https://docs.konghq.com/hub/kong-inc/rate-limiting/
  - Configure per route

```
- host: "fiware-orion-ld"
  name: "orion-limited"
  port: 1026
  protocol: http

  routes:
  - name: orion-limited
    paths:
      - /limited
        strip_path: true

    plugins:
      - name: rate-limiting
        config:
          minute: 3
```

FIWARE

Monitoring

- Prometheus integration:
  - https://docs.konghq.com/hub/kong-inc/prometheus/
  - Configure per route and enable scraping

```
- host: "fiware-orion-ld"
  name: "orion-keyrock"
  port: 1026
  protocol: http

  routes:
  - name: orion-keyrock
    paths:
      - /keyrock
        strip_path: true

    plugins:
      - name: prometheus
```

```
kong:
  podAnnotations:
    prometheus.io/scrape: 'true'
    prometheus.io/port: '9102'
```
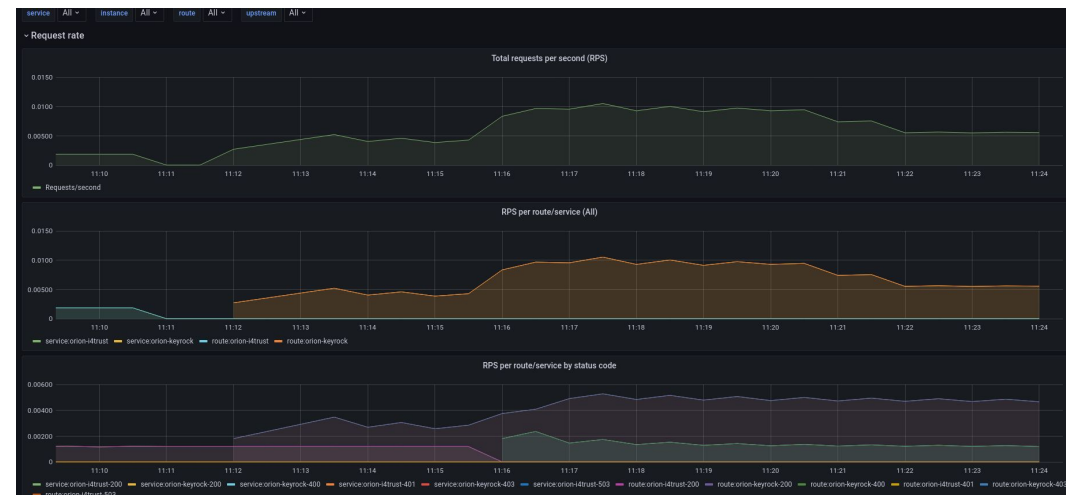
Further reading

- i4Trust-tutorials: https://github.com/i4Trust/tutorials

- UI: https://github.com/pantsel/konga

- Plugin development:
    - Lua
    - Go

- Slides: https://github.com/wistefan/presentations

FIWARE

Thank you!

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

FIWARE