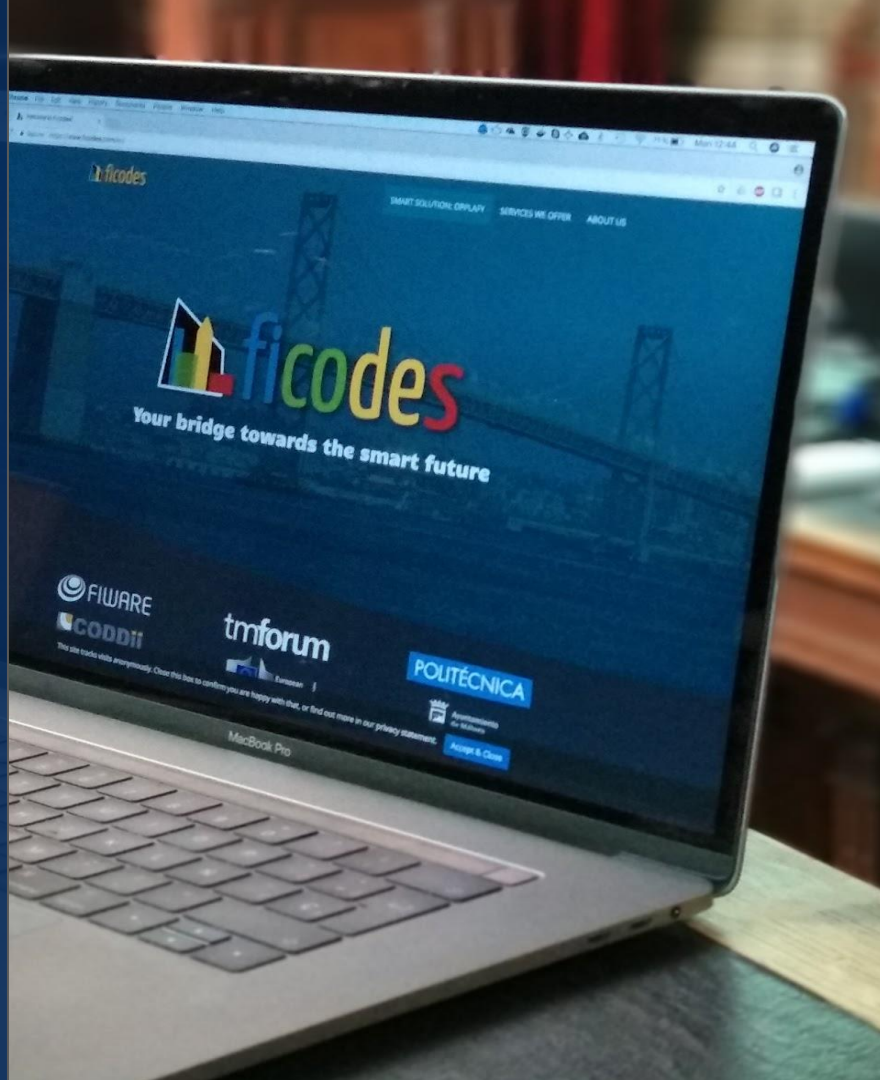
FIWARE Data Spaces

Deploying a FIWARE Data Space Connector

Stefan Wiedemann - Senior Software Engineer

Future Internet Consulting and Development Solutions S.L.
C/ Hespérides 5, 28232, Las Rozas de Madrid, Madrid, España



Deploying a FIWARE DSC

1. Preconditions
2. Setting up the Trust Anchor
3. Deploying a Consumer
4. Deploying a Provider
5. Verifying the System

Preconditions

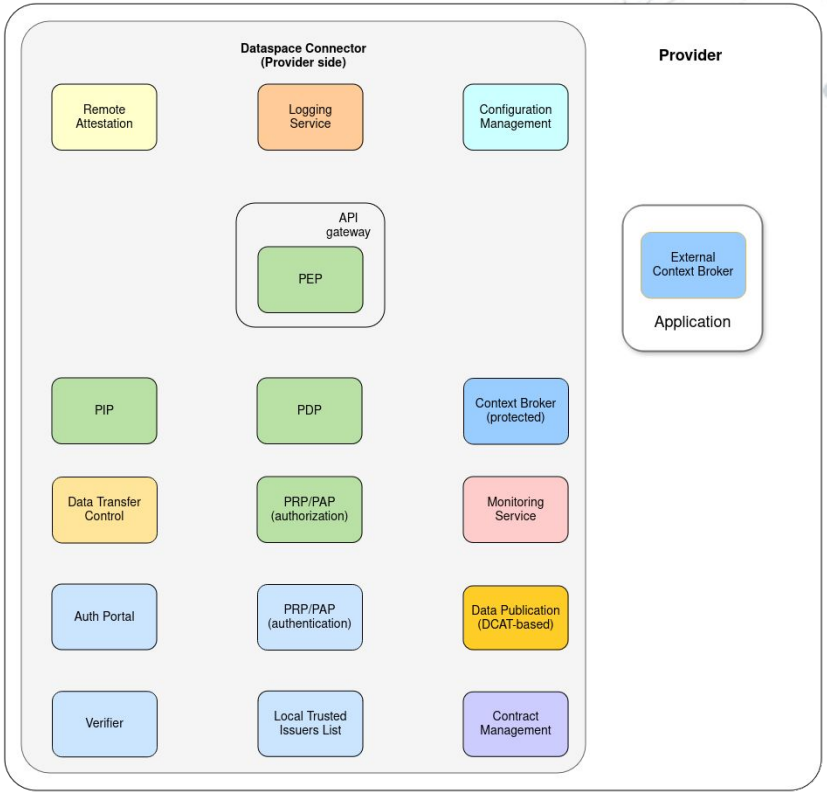
- Microservice architecture
- individual components can be enabled/disabled depending on the use-case
- reuse of existing OpenSource-Components
- various target environments

➢ requires solutions for internal and external networking

➢ support for configurable deployments

➢ allows integration of existing OpenSource deployment recipes

➢ abstraction of infrastructure



Preconditions

- Kubernetes
  - abstraction of infrastructure to a standardized API
  - supports internal networking through SDN
  - various options for external access, easy to control and configure
  - OpenSource and well-maintained(CNCF graduated)
  - various managed and self-hosted options available
- Helm
  - flexible configuration and configuration management
  - uses well-established tools(mustache) and principles(sane defaults, only overwrite required parts)
  - OpenSource and well-maintained(CNCF graduated)

Kubernetes

Kubernetes is an OpenSource container orchestration platform that automates deployment, scaling and management of containerized applications. It support different environments, such as on-premise data centers, public clouds or hybrid-setups.

- service discovery and load balancing allows to connect the individual microservices, balance their traffic and scale them individually, depending on the load
- provides self-healing and restart capabilities, to increase resilience of the system
- abstraction of infrastructure(computation, storage, networking) allows reuse of same recipes through different environments
- well-established and widely used

Helm

Helm is a package manager for Kubernetes that simplifies deployment and configuration of applications and services. It uses pre-configured templates of Kubernetes resources, enabling users to define, install and upgrade their applications

- Kubernetes resources are provided as mustache-templates
- contains defaults, allowing to install a standard-version with minimal additional configuration
- natively supports versioning of deployment-recipes
- allows reuse of existing “Charts” as dependencies
- supports repackaging to umbrella-charts

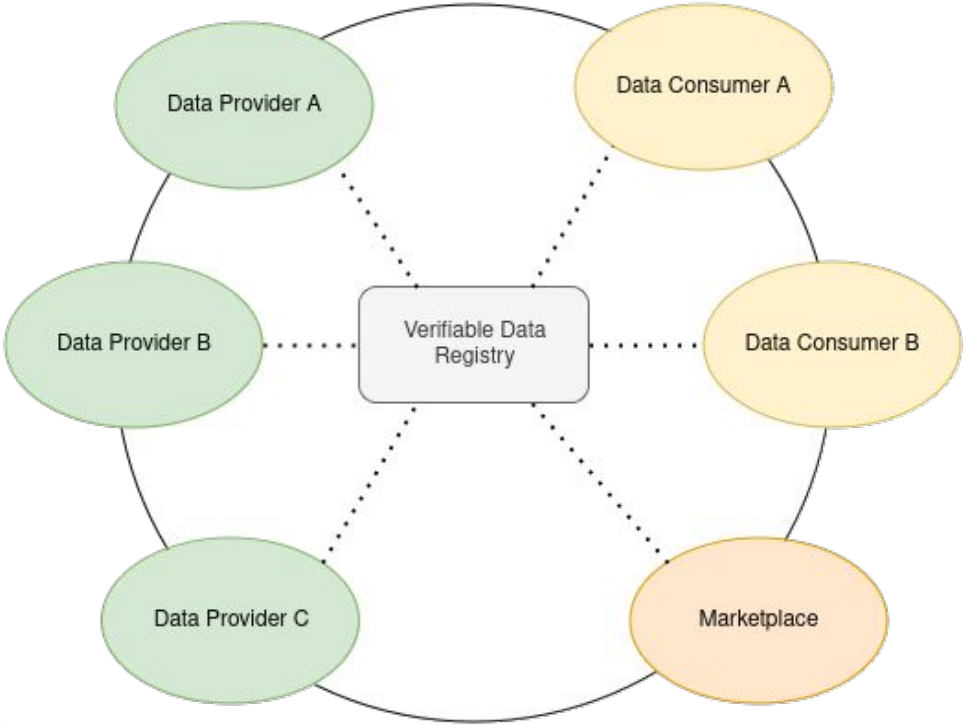
Operational considerations

- Monitoring
  - Prometheus endpoints available for most components
  - resource monitoring through Kubernetes
  - should be integrated with existing monitoring
- Logging
  - levels can be configured individually for each component
  - supports structured JSON-logging
  - should be integrated with existing logging
- Alerting
  - based on monitoring and logging, should be integrated with existing systems
- additional tooling like Service Mesh should be based on concrete requirements

The Connector

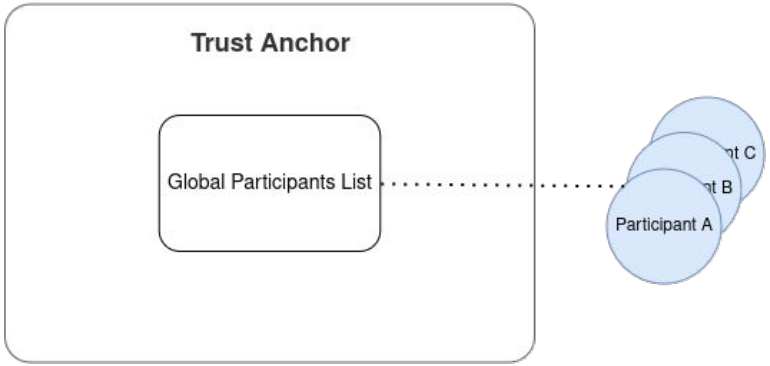
- Provided as Umbrella Helm-Chart: Data Space Connector Chart
  - reuse of Charts from FIWARE Helm Charts and Bitnami Helm Charts
  - extended with some convenience functionality for the Data Space Connector
  - all Sub-Charts can be individually disabled
  - individual parts can be exchanged(for example Databases, ApiGateway)
- automatically tested on K3s
- tested on Vanilla Kubernetes, contains support for OpenShift
- minimal Trust-Anchor Chart contained in the repo, to allow setup of a full Data Space

The Data Space



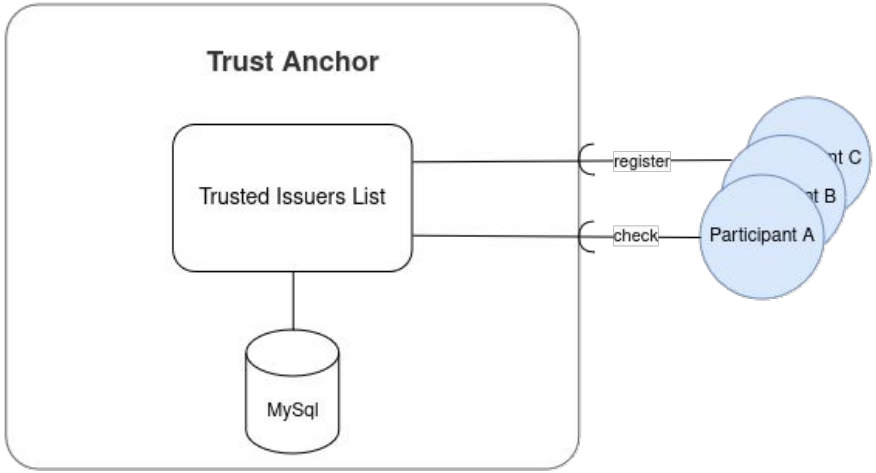
The Trust Anchor

- Provide the Global Trusted Participants list through the [EBSI Trusted Issuers Regsitry API]
- provide functionality to register new participants



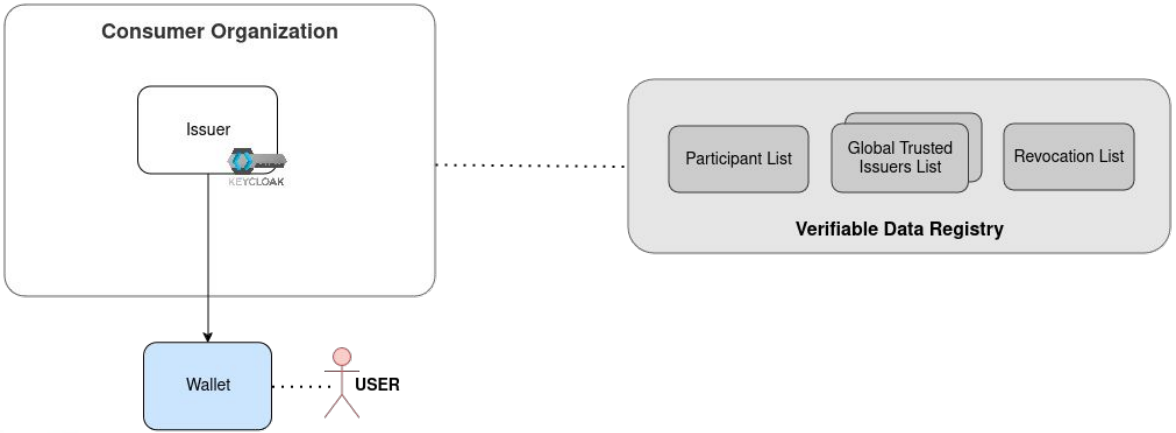
The Trust Anchor

- FIWARE Trusted Issuers List to provide two APIS: EBSI TIR API and TIL API for registration
- MySql as storage backend for the participants
    - DBaaS can be used



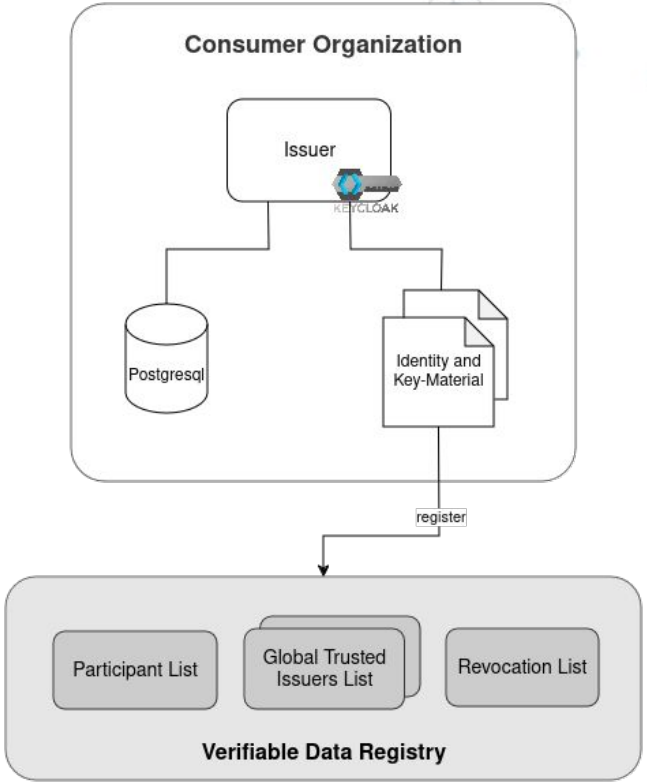
The Consumer

- Issues credentials to its users and services
- is registered at the Verifiable Data Registry



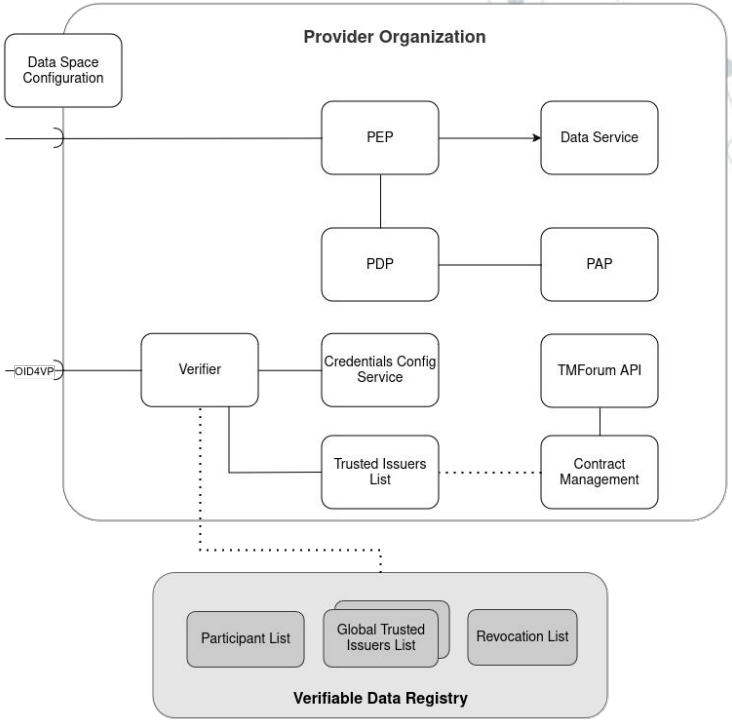
The Consumer

- Keycloak(26) as the issuing component
  - realm to be configured for OID4VCI
  - users and roles configured
  - credentials to be configured
- Postgresql as Database for Keycloak
  - DBaaS could be used
- Identity and Key-Material for the Organization have to be created and provided
- Organization has to be registered at the Verifiable Data Registry



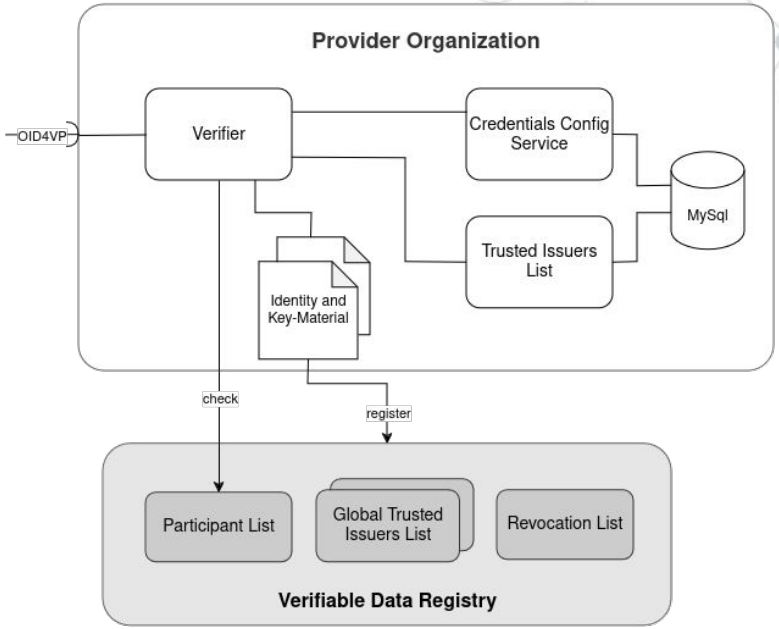
The Provider

- Authentication Services:
  - Verifier to offer OID4VP endpoints
  - Trusted Issuers List and Credentials Config Service for authentication config
  - registered and connected to Verfiable Data Registry
- Authorization Services:
  - PEP, PDP, PAP for enforcing and managing policies
- Data Service to be offered
- TMForum API and Contract Management for offering services
- Data Space Config as well-known endpoint



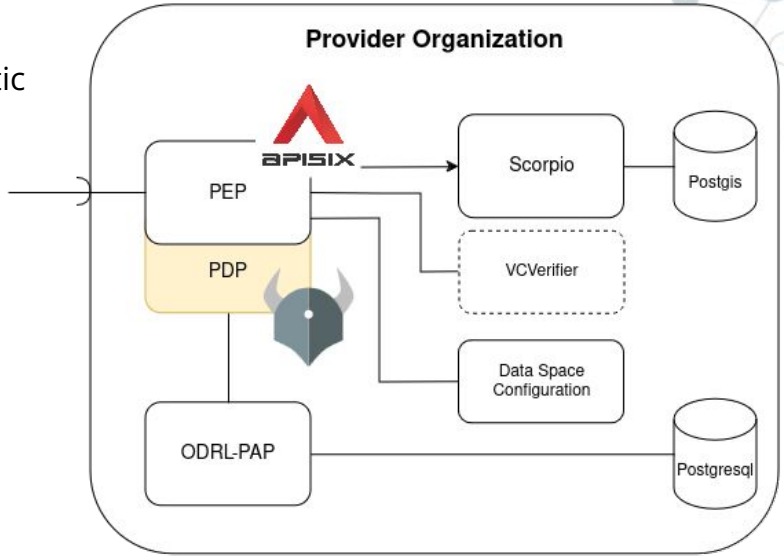
The Provider - Authentication

- VCVerifier to offer OID4VP
- Credentials Config Service and Trusted Issuers List to provide information about issuers and credentials for the verifier
- MySql as Storage Backend(can be shared instance)
  - DBaaS also possible
- Identity and Key-Material for the Organization have to be created and registered



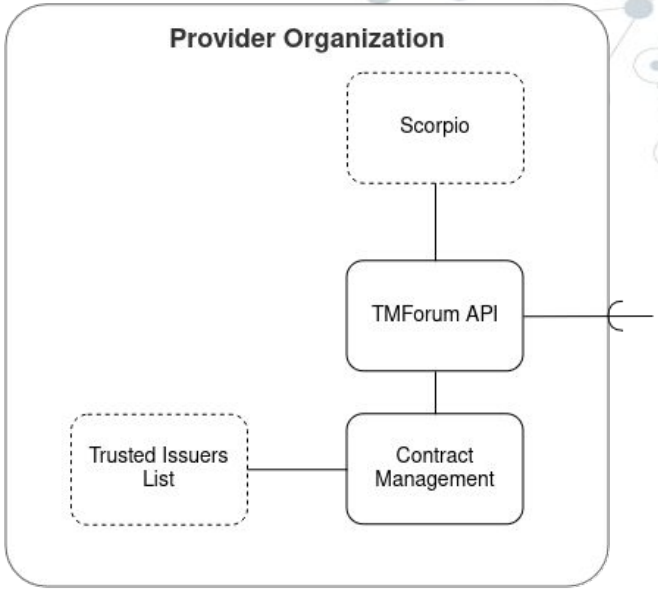
The Provider - Authorization

- APISIX Gateway as PEP and central entrypoint
  - routes well-known/openid-configuration from Verfier
  - routes well-known/data-space-configuration from static fileserver
  - checks JWT at Verifier
- Open Policy Agent as PDP
  - deployed as Sidecar for performance
- ODRL-PAP for managing Policies
  - Postgresql as storage backend, DBaaS also possible
- Scorpio as NGSI-LD compliant Data Service
  - Postgis as storage backend



The Provider - TMForum

- TMForum API's to offer marketplace and contracting functionality
    - uses an NGSI-LD Context Broker as storage backend
- Contract Management to integrate TMForum with the Authentication of the Data Space connector



Links

- Slides:
    - https://github.com/wistefan/presentations
- FIWARE Data Space Connector:
    - https://github.com/FIWARE/data-space-connector
- Demo-Deployment:
    - https://github.com/wistefan/deployment-demo

contact@ficodes.com | www.ficodes.com | +34 614 20 74 47 | C/ Hespérides 5 (28232) | Las Rozas de Madrid

ficodes