Open APIs for Open Minds

MVDS for INPACE hackathon using FIWARE DSC

Juanjo Hierro
Chairman, FIWARE TSC
Chief Strategy Officer, SEAMWARE
juanjose.hierro@seamware.com

FIWARE

FIWARE Data Space Connector: integration of EDC and FDC

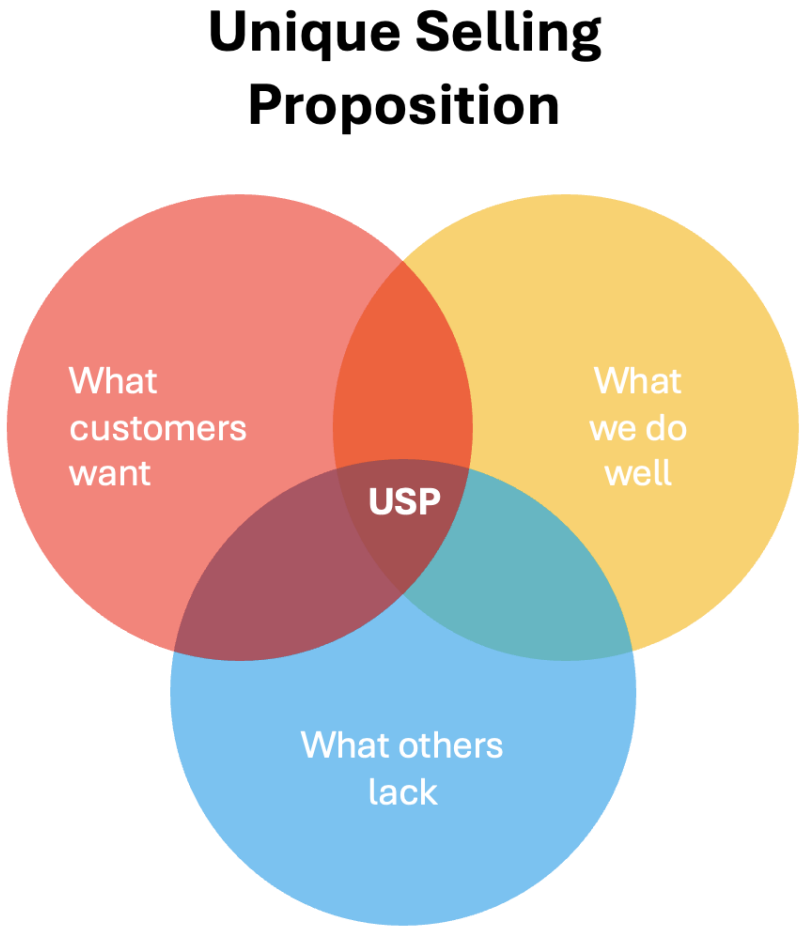
- EDC (Eclipse Dataspace Components) enable B2B data exchange:
  - implements DCP for authentication of organizations
  - implements DSP for catalog publishing, contract negotiation and transfer process management
- FDC (FIWARE Dataspace Components) enable B2B data exchange, as well as direct user* access to data services and applications
  - implements OID4VC for authentication of organizations/users
  - implements TM Forum APIs for catalog publishing, contract negotiation
- FIWARE Data Space Connector combine EDC and FDC therefore supporting compatibility with EDC-only Data Space Connectors while overcoming the limitations of these connectors and the data space vision they support (check link)

(*) users can be natural persons using their wallets or devices, robots, AI or software agents each with their own identity within an organization

FIWARE

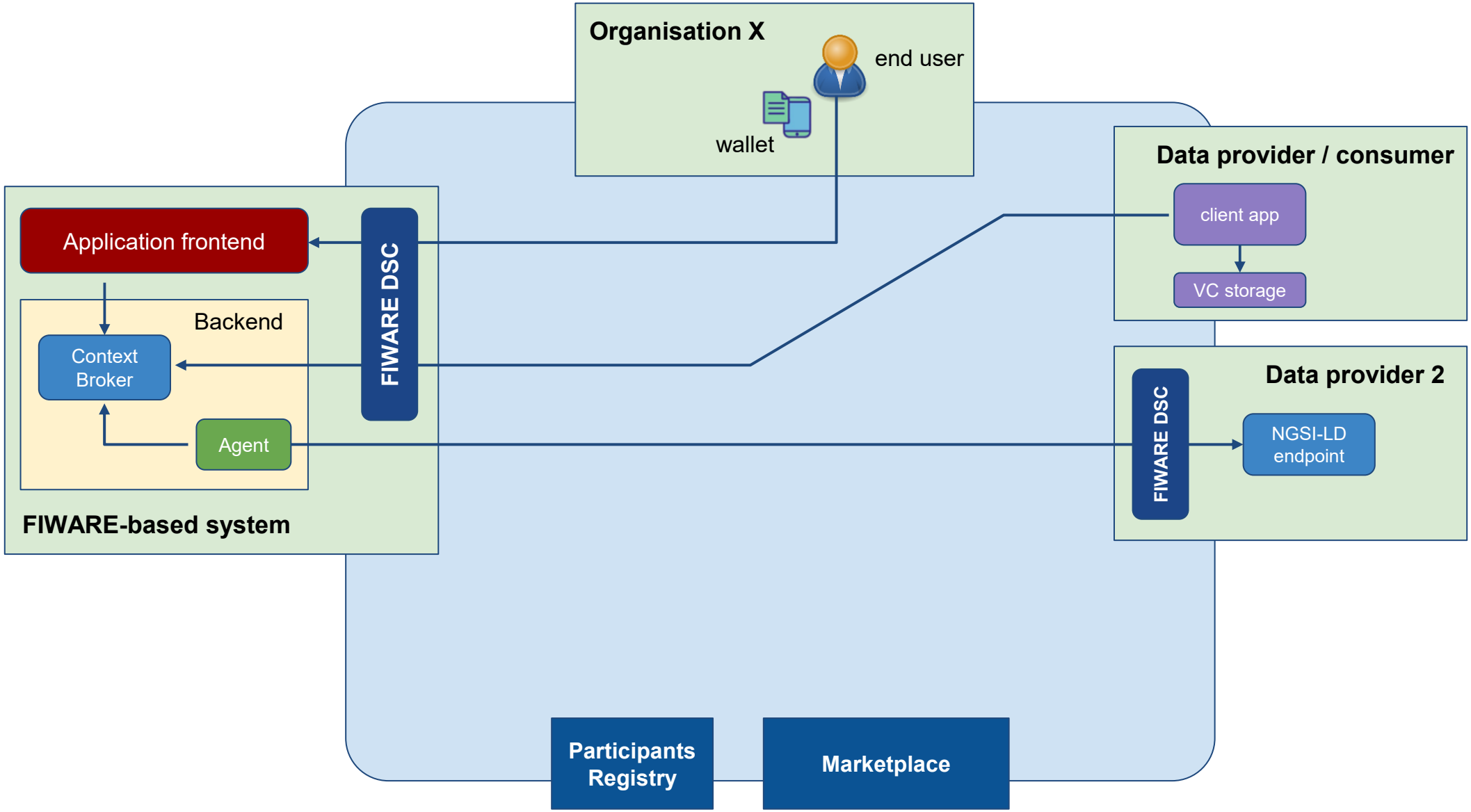
Unique selling proposition brought by FDC

- Providers can offer sophisticated products comprising services (e.g., accessible via APIs) and end applications, not just data
- Users (natural persons, devices, robots, AI and software agents) within consumer organizations can get direct access to services and applications without a connector
- Compatibility with EU DI wallet and Keycloack VCI
- Enforcement of policies through solid and mature open source framework based on APISIX and OPA
- Compatibility with Gaia-X ICAM and ODRL profile for VC
- Compatibility with EBSI APIs (global registries)
- Translation of ODRL to Rego for evaluation of policies via open policy agent, instead of hard coding policies
- Compatibility with marketplaces, including DOME
- Support to monetization



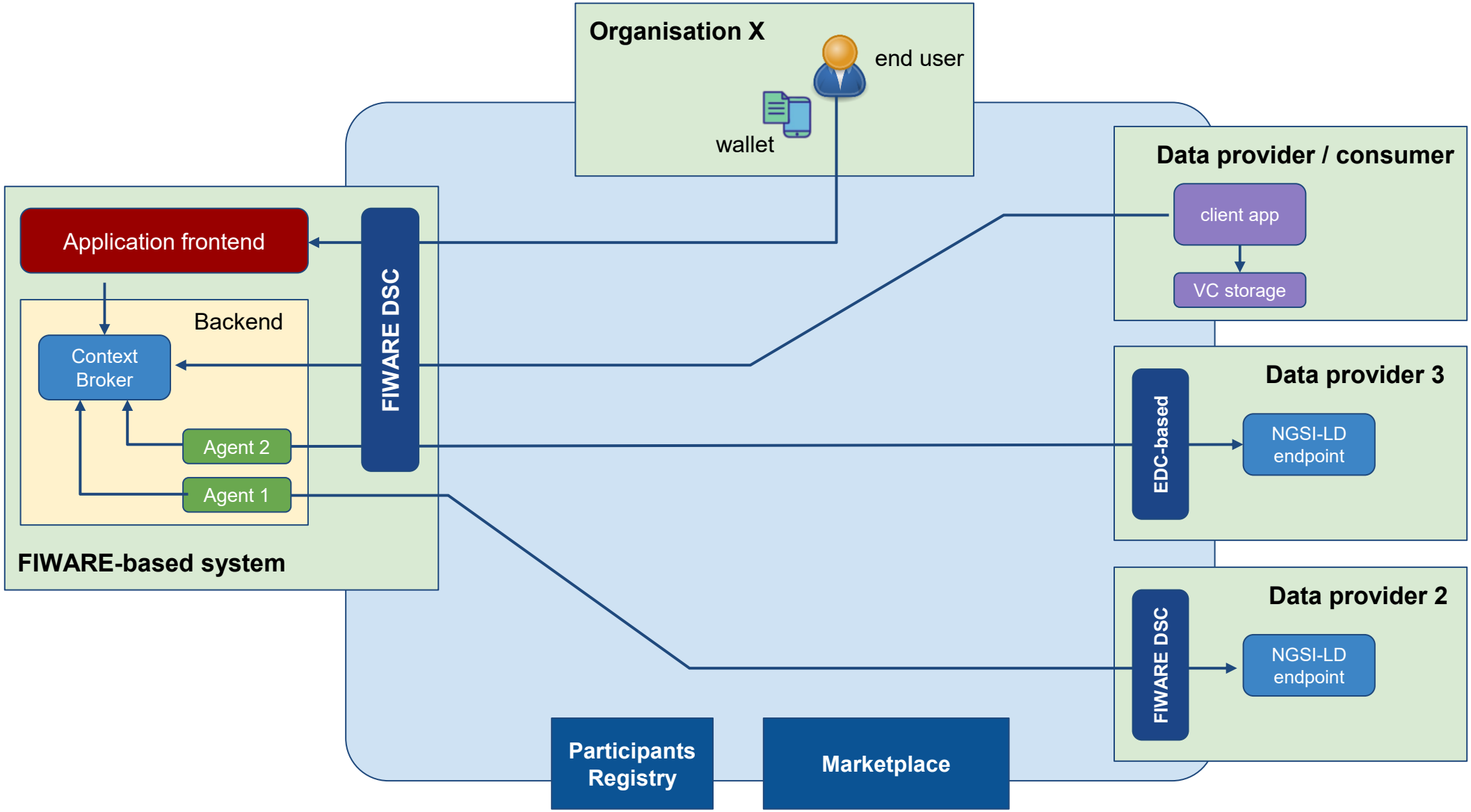
FIWARE

Proposed MVDS



FIWARE

Extended MVDS

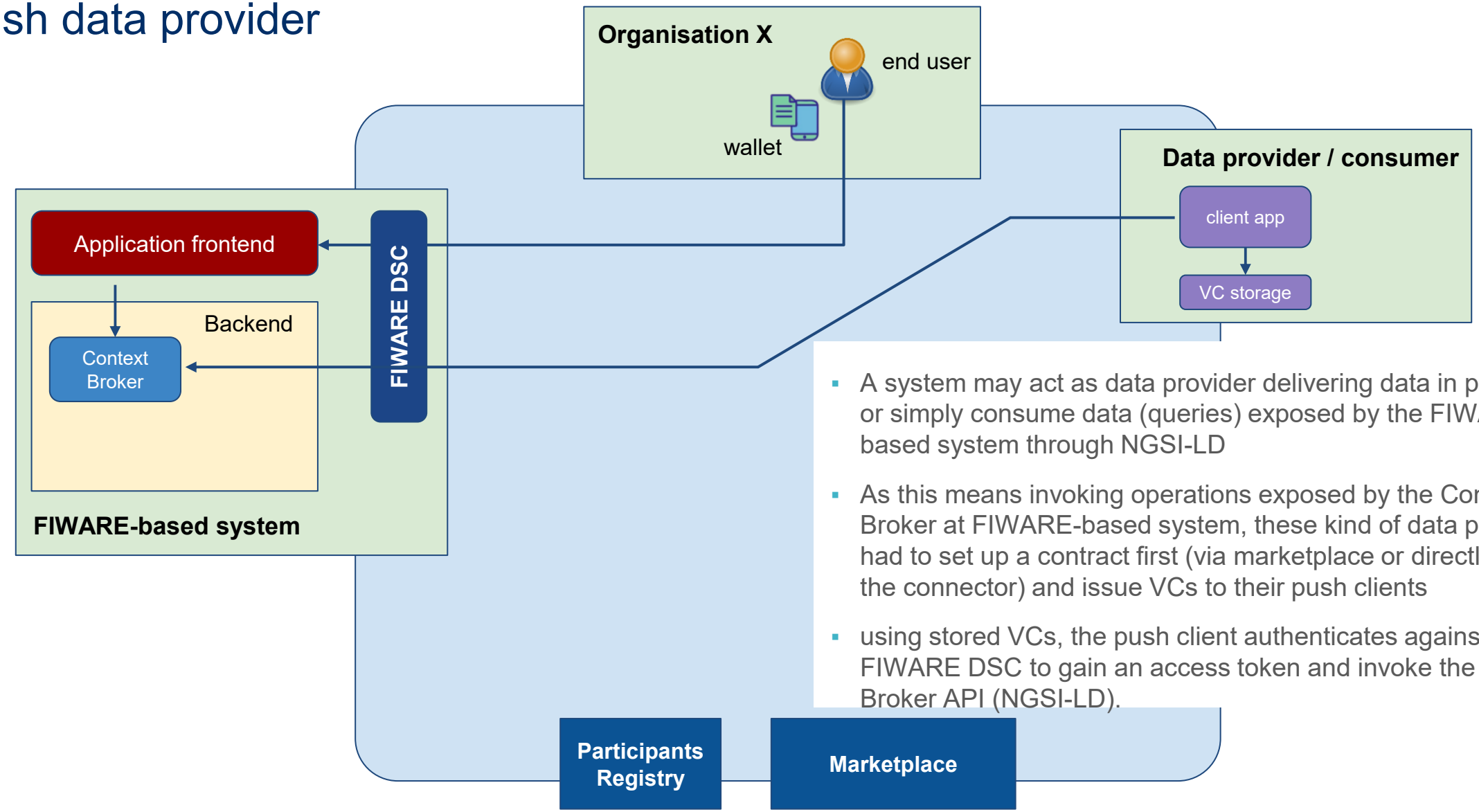


Potential challenges for a hackathon

- Challenge 1: create example client application which can query (acting as consumer) from, or push data (acting as data provider) into, the FIWARE-based system using the NGSI-LD API it offers
- Challenge 2: within an organization that has acquired the right to access the FIWARE-based system, manage the issuance of verifiable credentials for users linked to the organization (employees or customers) so they can access the web application associated with the FIWARE-based system
- Challenge 3: create data provider which offers near real-time data or datasets (may be synthetic data) that can be exposed through the FIWARE Data Space Connector, develop a client agent to be deployed in the FIWARE-based system that can query data offered by this data provider and inject it in local Context Broker
- Challenge 4: same as challenge 3 but using a EDC-based connector (may be the FIWARE Data Space Connector or some other connector like Tractus-X or Eona-X) in the data provider side so that DSP (Data Space Protocol) is used for contract negotiation and management of transfer

FIWARE

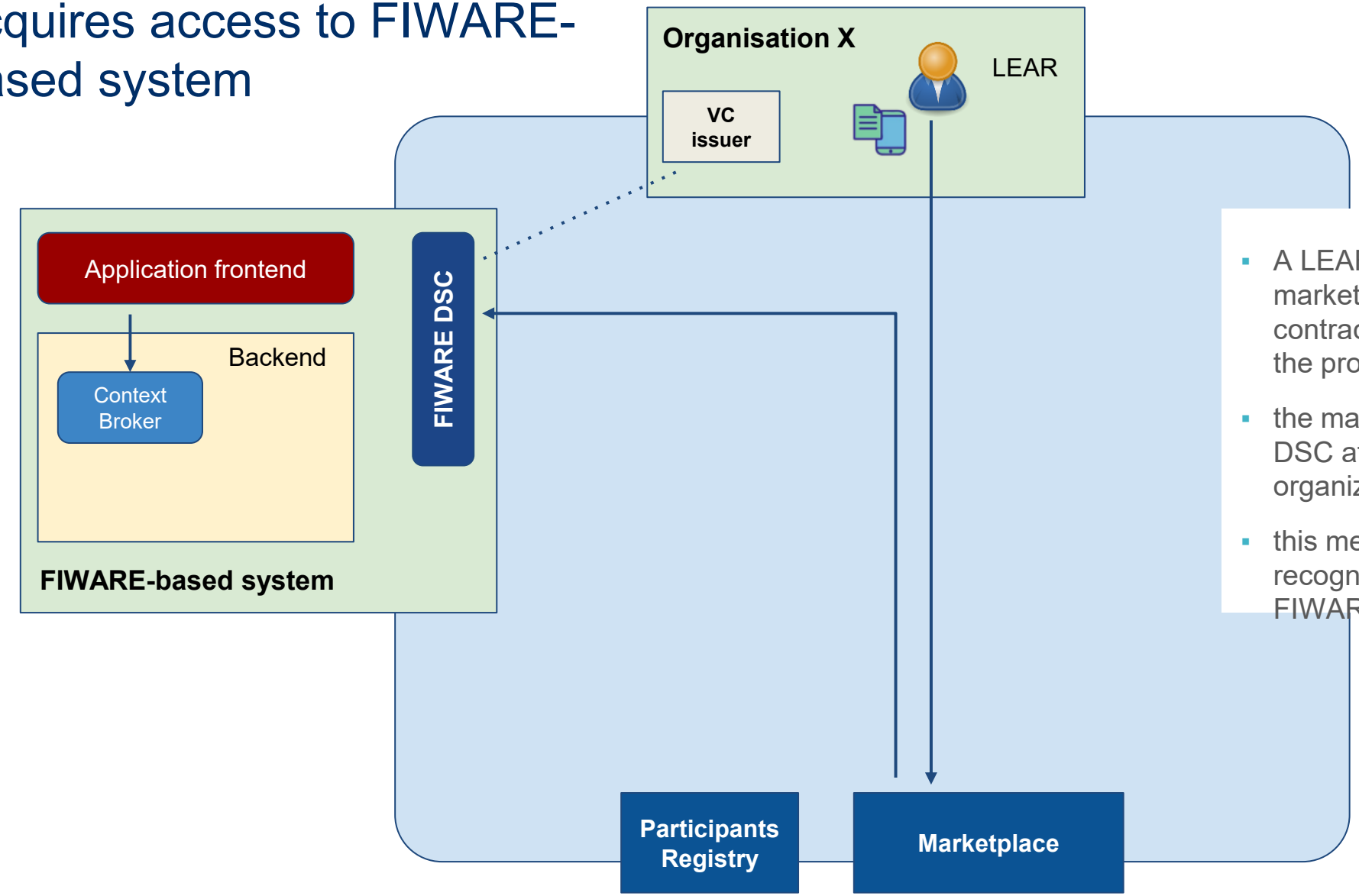
Challenge 1: example of push data provider



- A system may act as data provider delivering data in push mode or simply consume data (queries) exposed by the FIWARE-based system through NGSI-LD
- As this means invoking operations exposed by the Context Broker at FIWARE-based system, these kind of data providers had to set up a contract first (via marketplace or directly through the connector) and issue VCs to their push clients
- using stored VCs, the push client authenticates against the FIWARE DSC to gain an access token and invoke the Context Broker API (NGSI-LD).

FIWARE

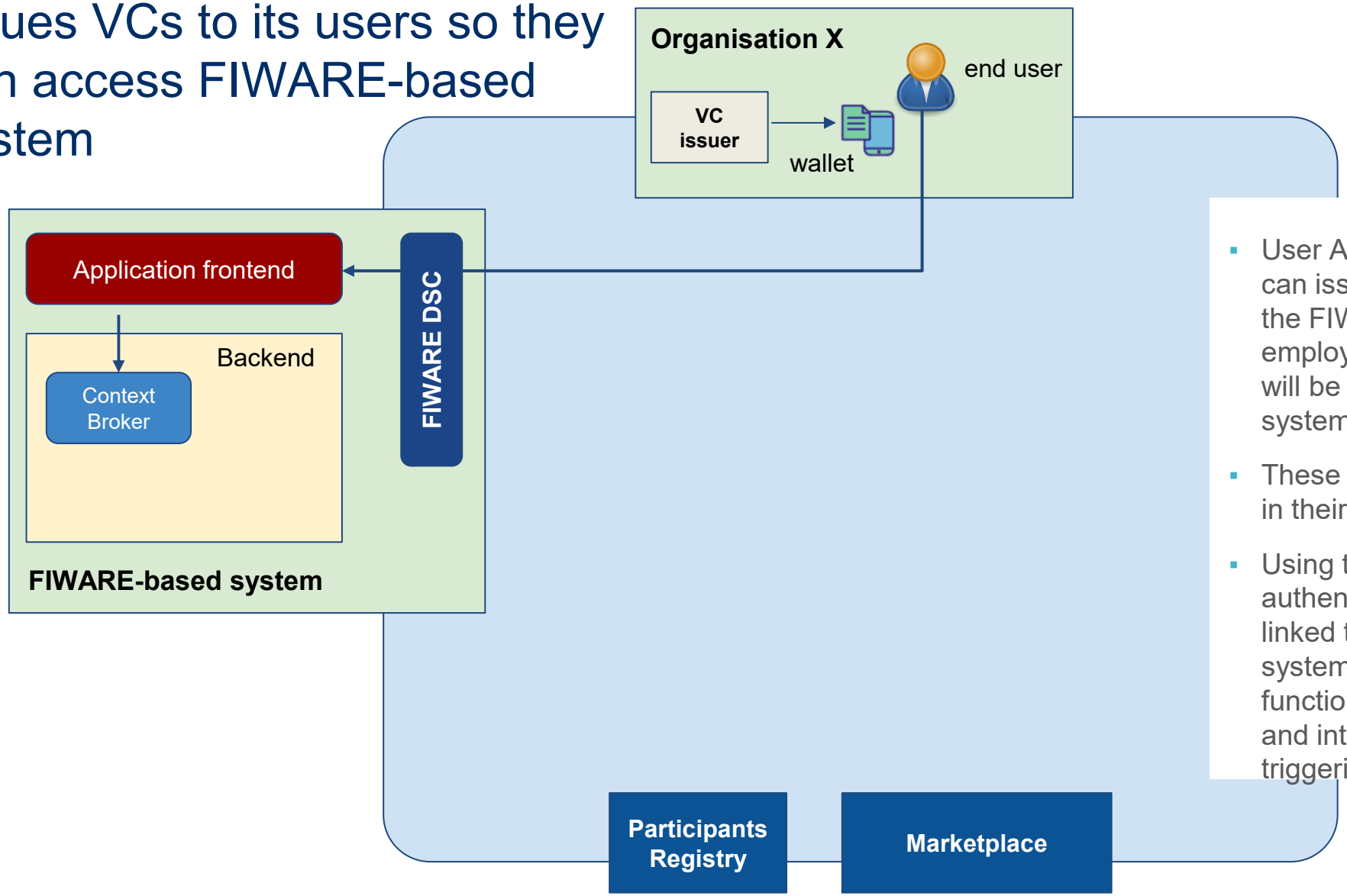
Challenge 2: organization X acquires access to FIWARE-based system



- A LEAR of organization X goes to the marketplace in order to set up a contract (adquire) enabling it to access the product (FIWARE-based system)
- the marketplace notifies the FIWARE DSC at the FIWARE-based system that organization X acquired the product
- this means organization X will be recognized as trusted issuer of VCs the FIWARE-based system requires

FIWARE

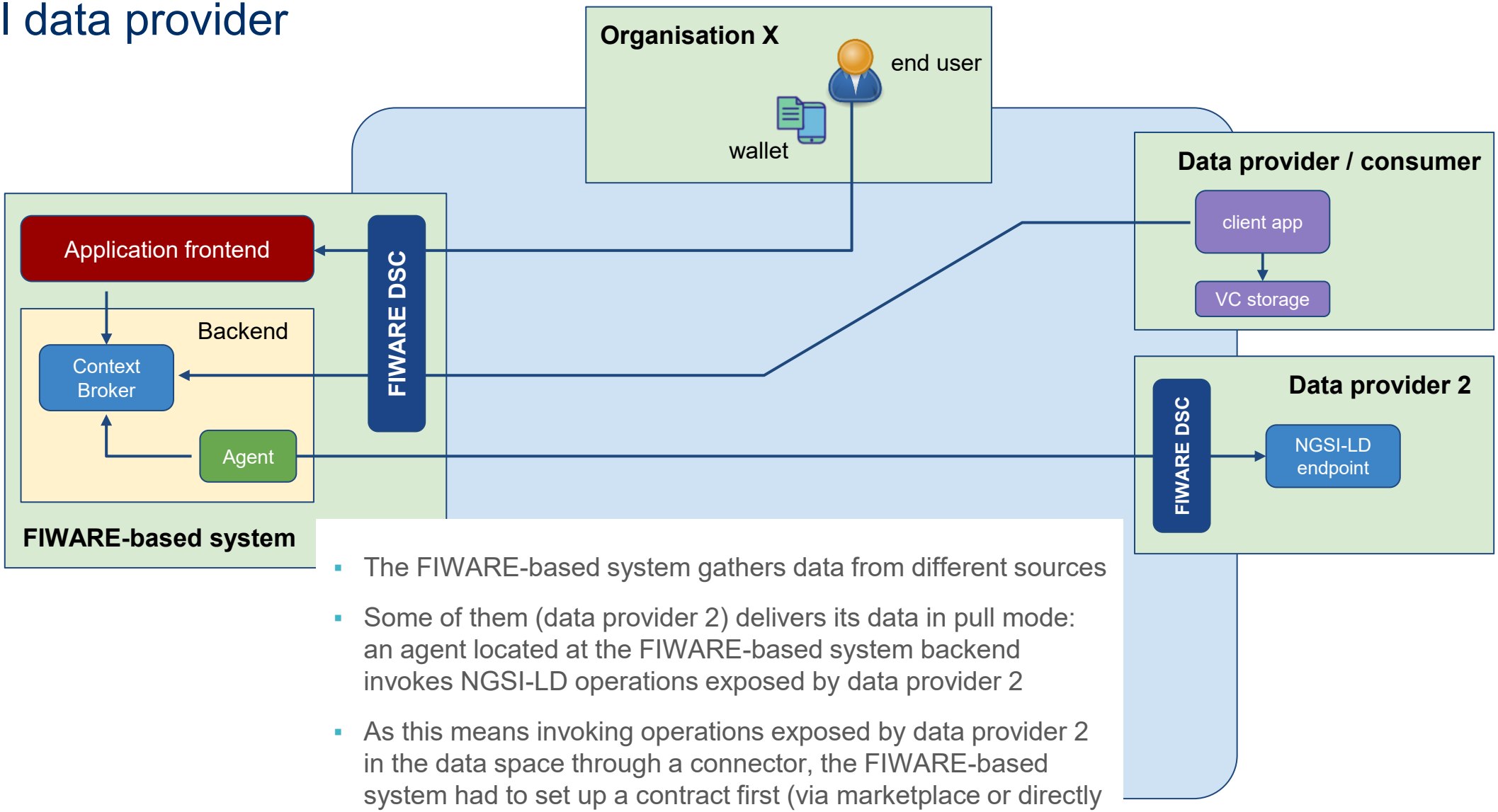
Challenge 2: organization X issues VCs to its users so they can access FIWARE-based system



- User Admins at organization X can issue VCs required to access the FIWARE-based system (e.g., employees) at organization X who will be using the FIWARE-based system
- These users will store issued VCs in their digital wallets
- Using these VCs they can authenticate to the application linked to the FIWARE-based system and enjoy end user functionality (e.g., visualization and interpretation of data, triggering actions, etc)

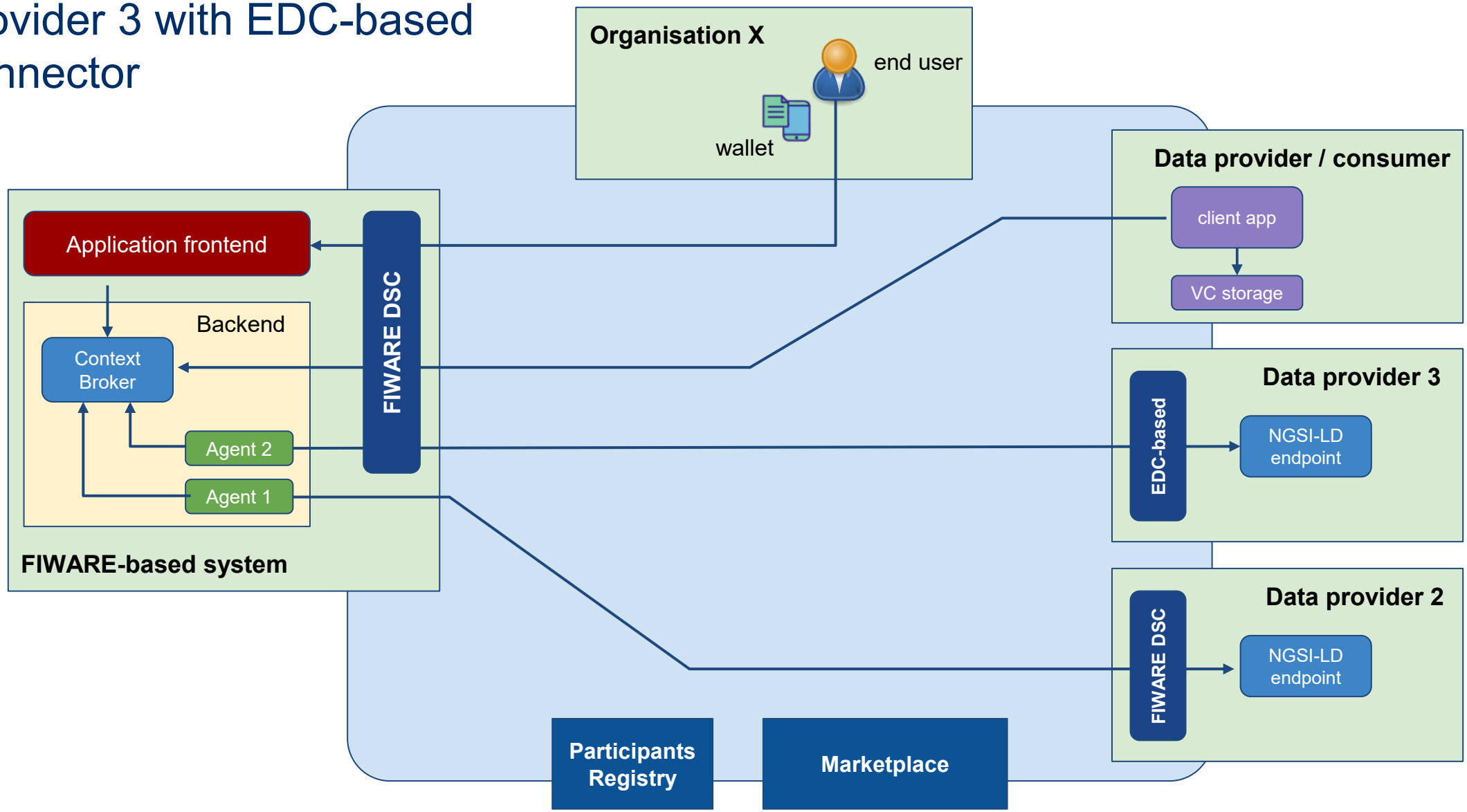
FIWARE

Challenge 3: example of pull data provider



- The FIWARE-based system gathers data from different sources
- Some of them (data provider 2) delivers its data in pull mode: an agent located at the FIWARE-based system backend invokes NGSI-LD operations exposed by data provider 2
- As this means invoking operations exposed by data provider 2 in the data space through a connector, the FIWARE-based system had to set up a contract first (via marketplace or directly through the connector of data provider 2) to acquire the rights to issue VCs the agent can use to access the endpoint

Challenge 4: inclusion of data provider 3 with EDC-based connector



FIWARE

Benefits of the approach

- Value proposition for Data Spaces become more attractive for solution providers and intermediaries:
  - They can make their full offer (applications, APIs, data) available on data spaces
  - Transitioning web-based applications to support authentication based on verifiable credentials is a relatively low-cost path, thus enabling quick-wins for providers delivering their SaaS solutions
  - Providers can set up a roadmap where they first bring their SaaS solution (user interface only) and later they deliver APIs, data
  - Intermediaries can offer catalog/marketplaces of applications that can be integrated relying on data spaces technology stacks
- Value proposition for Data Spaces become more attractive for consumer organizations, particularly small ones:
  - Their users can enjoy web applications offered in the data space without the need of deploying a connector (and they need apps more than plain data!) - relying on use of digital wallets is enough
  - They can manage what users (e.g., employees, customers) linked to their organization can access what functions, without the need to develop applications that take care of authorization

FIWARE

Thanks!

FIWARE