Open APIs for Open Minds

FIWARE Data Space Components: Ongoing and Future work

Juanjo Hierro
Chairman
FIWARE Technical Steering Committee
juanjose.hierro@gmail.com

Stefan Wiedemann
Senior Software Engineer
FICodes
swiedemann@ficodes.com

FIWARE

Agenda

- Intro - let’s not forget our overall vision
- Integration with Gaia-X
- Integration with DOME
- Support to IDSA/Eclipse Data Space Protocols
- How to join / follow up

FIWARE

Intro - let’s not forget our overall vision

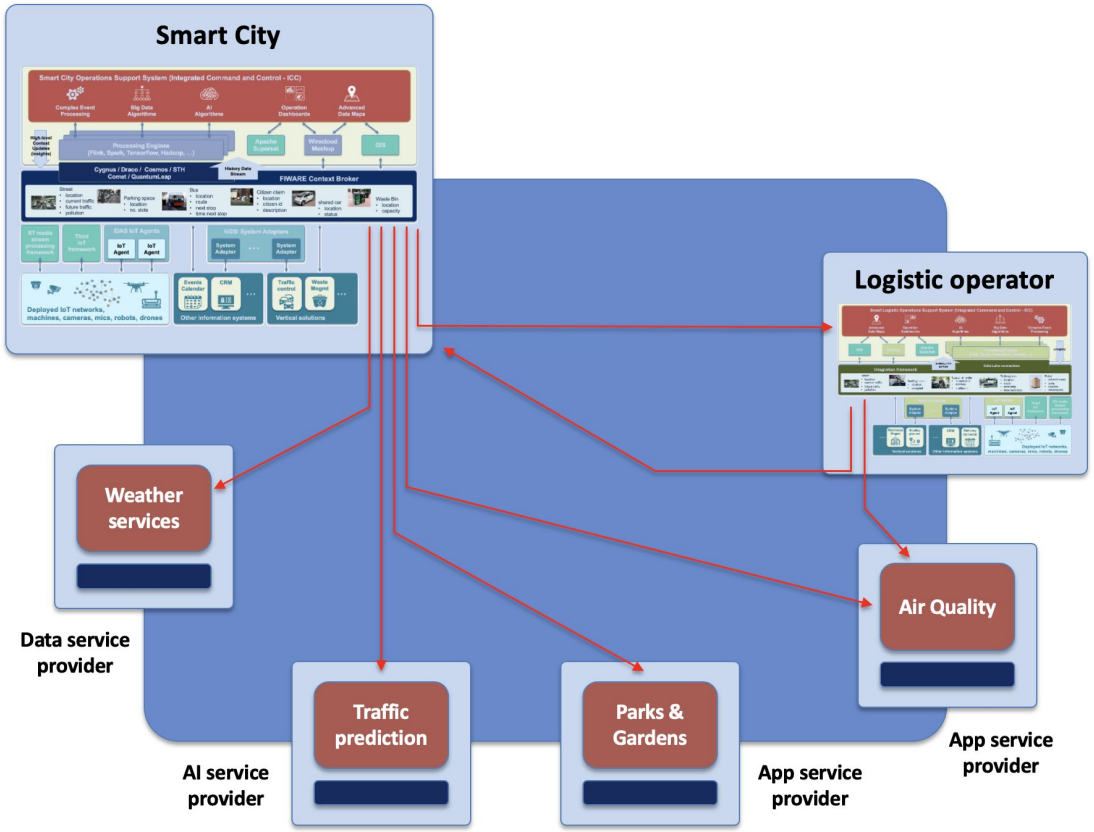
What is a data space?

- A data space can be defined as **an ecosystem** where participants adopt **agreed technology building blocks** for:
  - **Data Interoperability**: participants invoke/integrate data services from others using agreed APIs (protocols and data formats)
  - **Trust and Sovereignty on Data**: trust of parties accessing data services can be verified, digital identity can be managed in a decentralized manner (each organization managing its own users) and there is a common approach how authorization policies can be defined and enforced
  - **Data Value Creation**: Publication and Discovery of data services offerings as well as negotiation of contracts follow common standards
- A data space also requires **agreed governance**: definition of a number of business, operational and organizational agreements every participant adhere to, plus the existence of a governance body
- Many of these **building blocks (technology, governance) can be defined to work for multiple application domains** → data spaces are not only valuable for building an ecosystem around providers of organizations in a given application domain (e.g., smart cities) but an ecosystem where organizations can offer services each other and together develop new data value chains

FIWARE

Position statement

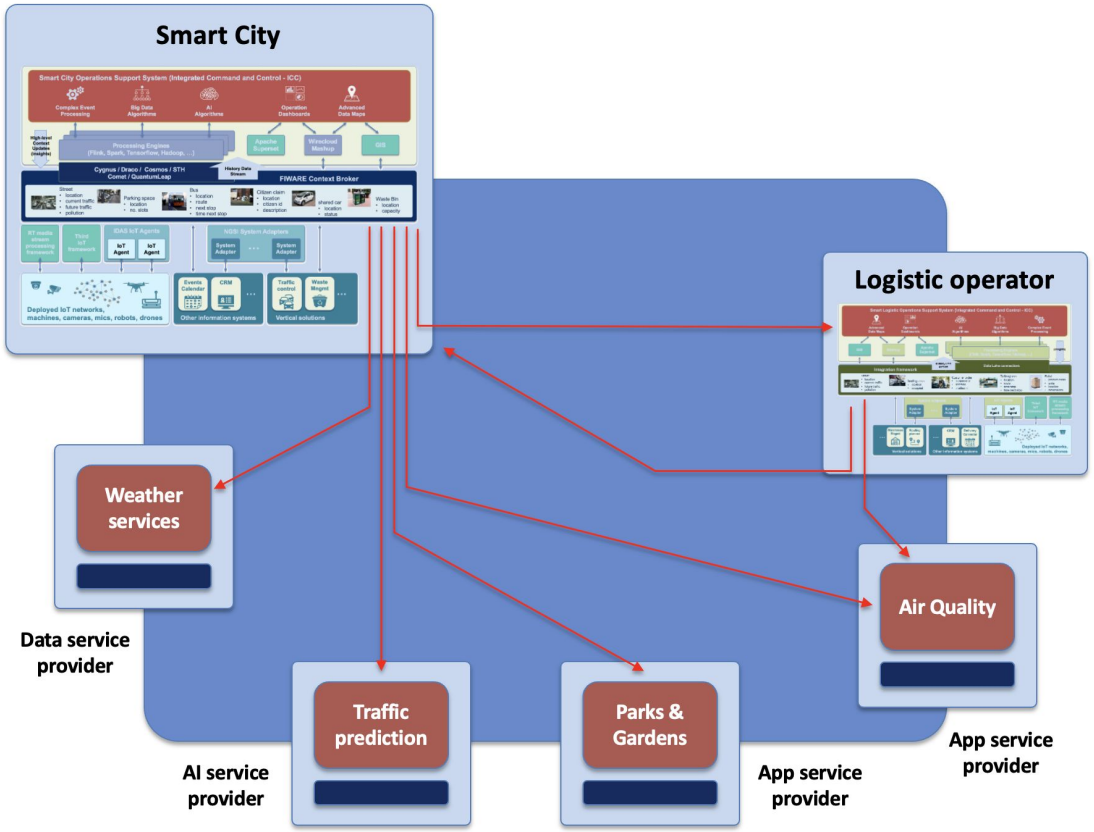
- Data Spaces are not just about peer-to-peer exchange of data / datasets / files !!
- Data Spaces are more about enabling organizations to:
  - seamlessly extend their map of systems by integrating systems from third parties: App providers (including AI services providers), Data Service providers, other organizations
  - easily become system providers (so other organizations can seamlessly integrate their data services)
- Of course, each system offers a collection of:
  - data services (services for accessing data)
  - data processing services (which receive, process and generate data)
- That is why we say data is central in Data Spaces !!



FIWARE

Some key concepts: Products, Services, Resources

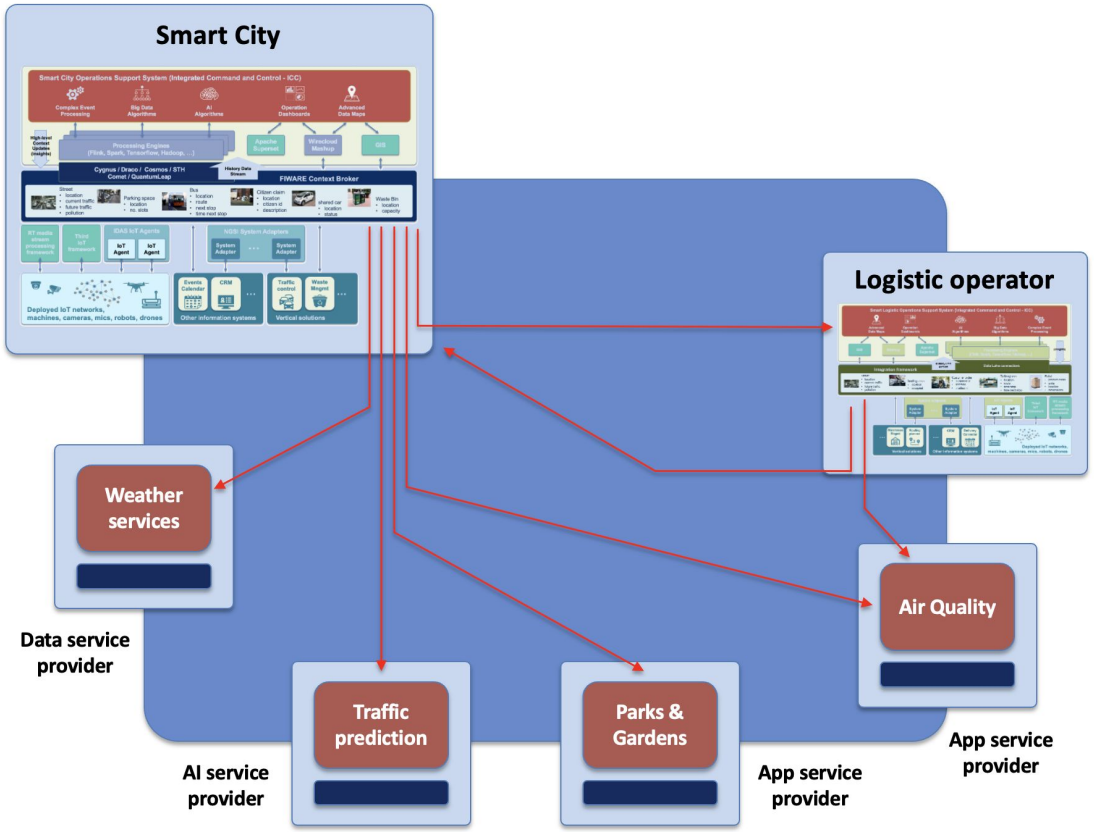
- Each Participant of the Data Space can play the role of a Provider or Customer (or Consumer) of Products
- A Product typically maps to a System that is realized as a combination of Services and/or Resources:
  - Services provide access to data or processing of data
  - Resources are required for the execution of the Services
- A Product (and its corresponding services and resources) are provisioned and activated for a particular Customer when it acquires the right to use the Product:
  - Provision and activation may take days!
  - Not everything runs on the Cloud: cloud-to-edge products
- Example: Air Quality Monitoring Product
  - Comprises services (e.g., web portal, REST services endpoints, etc) some of which bring access to data (air quality measures) or processing of data (air quality predictions)
  - Activation of services for a given customer, requires that some given resources are provisioned and activated - IoT devices in the field and some computing and storage on the backend



FIWARE

Distinguished features of data spaces (1/3)

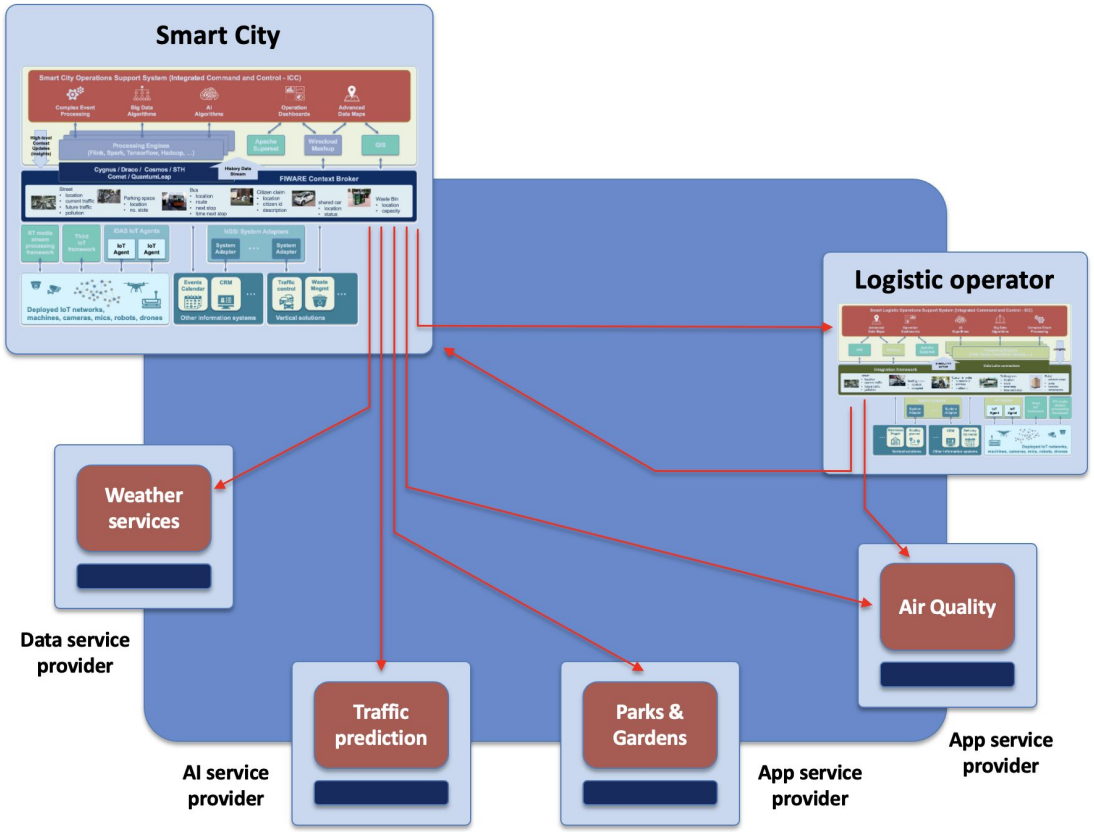
- Commonly agreed Decentralized Identity Management:
  - Each organizations manages its users - no need to register own users in a third identity provider in order to allow them to consume services from system providers they have acquired the right to use
  - System (App/Data service) providers do not need to take care of managing users from consumer organizations - they only need to know what credentials users own that are relevant to the systems business logic and be able to check they were issued by trusted issuers of the credentials
- Commonly agreed global service enabling to verify whether an organization is a trusted participant and issue a credential that accredits such condition
- Commonly agreed Policy Definition Language for specifying authorization policies:
  - expressed as rules that are formulated upon credentials of users, variables of the environment, services invoked, data being accessed or provided for processing, …
  - enabling organizations to understand how authorization is managed and, therefore, what credentials they should issue for each user



FIWARE

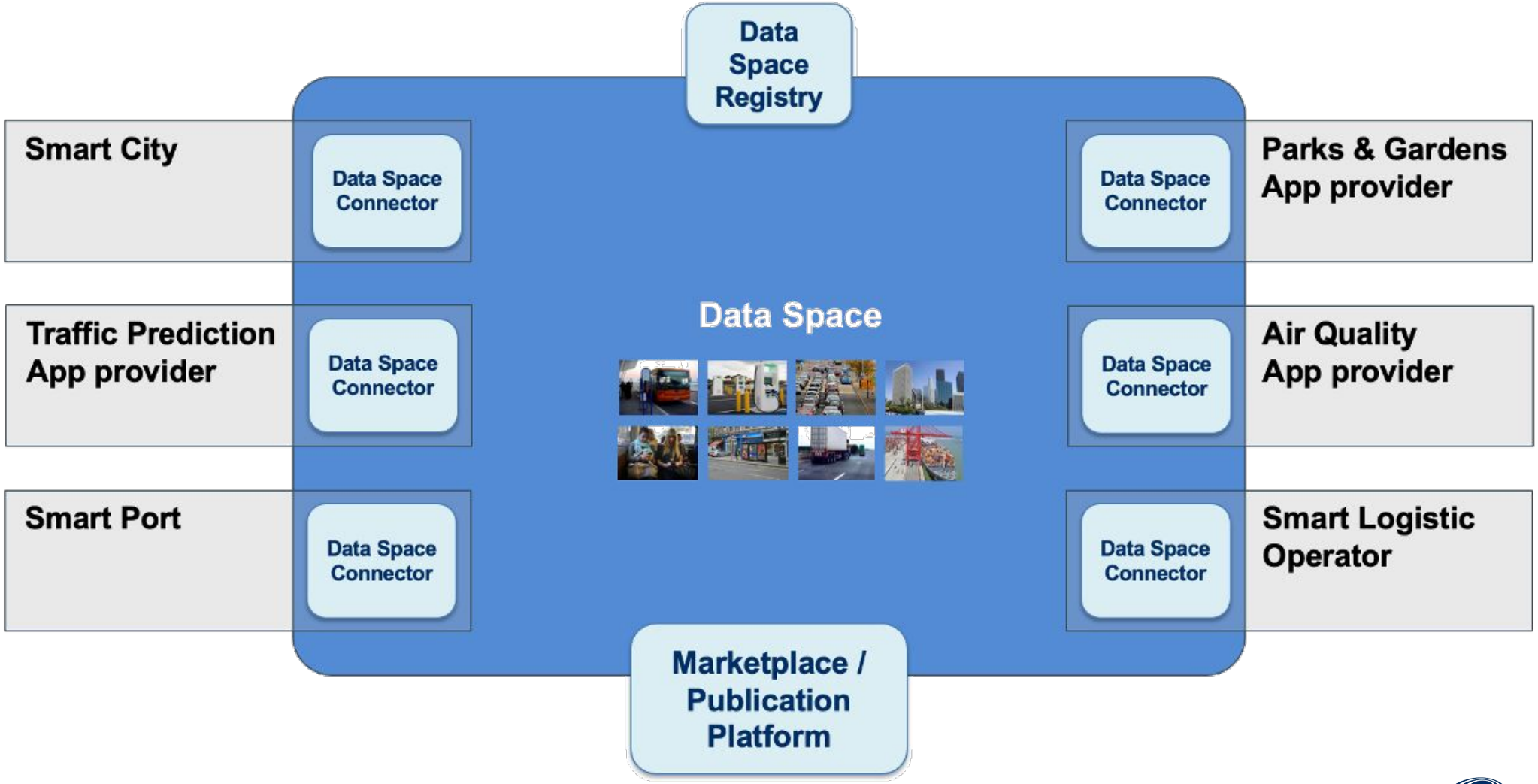
Distinguished features of data spaces (2/3)

- Commonly agreed mechanisms for:
  - publishing product (systems) characteristics: associated data services and their characteristics
  - discovering products (systems): associated data services
- Commonly agreed process to acquire the rights to use products (systems) offered by any provider:
  - standard API for accessing characteristics of a system and managing the process for the acquisition of rights to use it
  - acquiring the rights to use a system implies that the consuming organization becomes a trusted issuers of the credentials that system requires to access to its services
- Commonly agreed mechanisms to invoke services, e.g.:
  - standard APIs for accessing data or request the processing of data
  - mechanisms for exchange of large datasets / files
- Commonly agreed vocabularies to ensure semantic interoperability when invoking services



FIWARE

Data Spaces systems



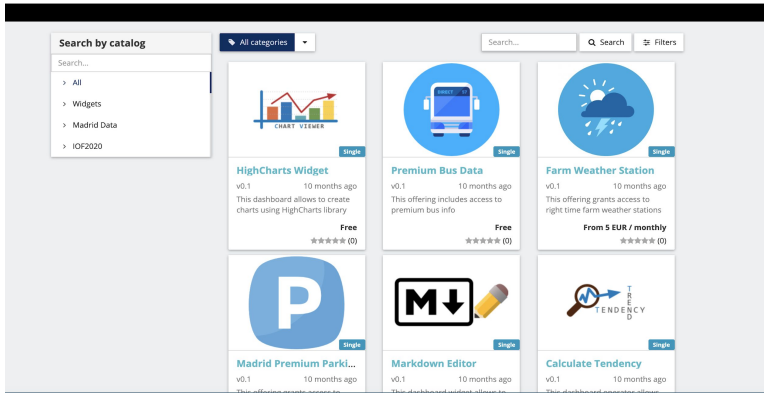
FIWARE

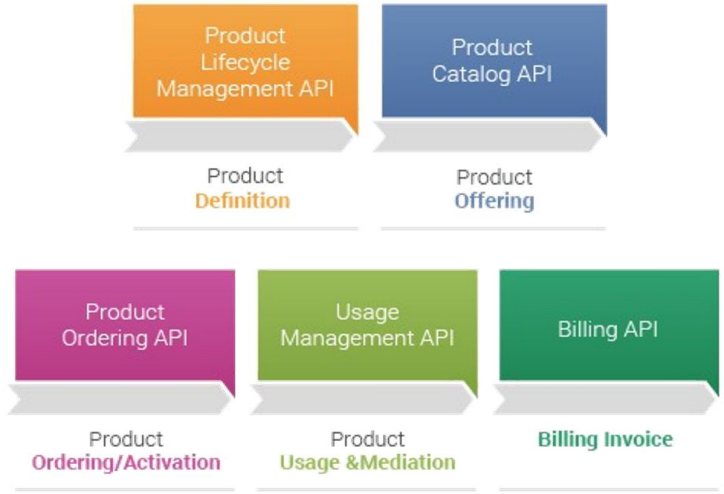
Reference specifications: Data sovereignty and trust

- Any data space requires a Trust Framework bringing
  - Mechanisms for verifying legal identity
  - Mechanisms for verifying compliance with data space participation rules
  - Mechanisms for verifying trustworthiness of credential issuers
- On the other hand, it requires a decentralized Identity and Authorization Management (IAM) framework through which manage authentication and the enforcement of access/usage policies
- Trust framework compatible with Gaia-X Digital Clearing Houses, aligned with the EU DI Wallet Architecture and EBSI
- Decentralized IM based on latest W3C and OIDC standards:
  - W3C DID (Decentralized Identifiers), Verifiable Credentials (VC)
  - Verifiable Credentials Issuance Protocols: OIDC4VCI
  - Self-Issued OpenID Provider: SIOPv2
  - Verifiable Credentials Exchange Protocols: OIDC4VP
- Authorization framework following PEP-PDP-PIP and PRP/PAP architecture for ABAC (attributes ⇔ claims in VCs), and adopting ODRL as Policy Definition Language

Reference specifications: Data value creation

- Creating value out of data based on data sharing is the ultimate goal in data spaces.This follows basically the steps to:
  - Describe data, services, resources, products, offerings in an interoperable manner
  - Include data and service publication services to discover offerings facilitating connection of providers and consumers
  - Support contract negotiation peer-to-peer or through value–added services such as marketplaces
- Providers will be able to self-issue Verifiable Credentials linked to descriptions of their products/services/resources/data → goal is to align on common specifications for future editions
- Descriptions will be available through catalogs at connector level (supporting DCAT v3) or at data space level (Metadata Brokers or Marketplaces)
- TM Forum APIs bring the basis for managing offerings and support contract negotiation via marketplaces → to be supported in DOME, goal is to align on how to support them at connector level





FIWARE

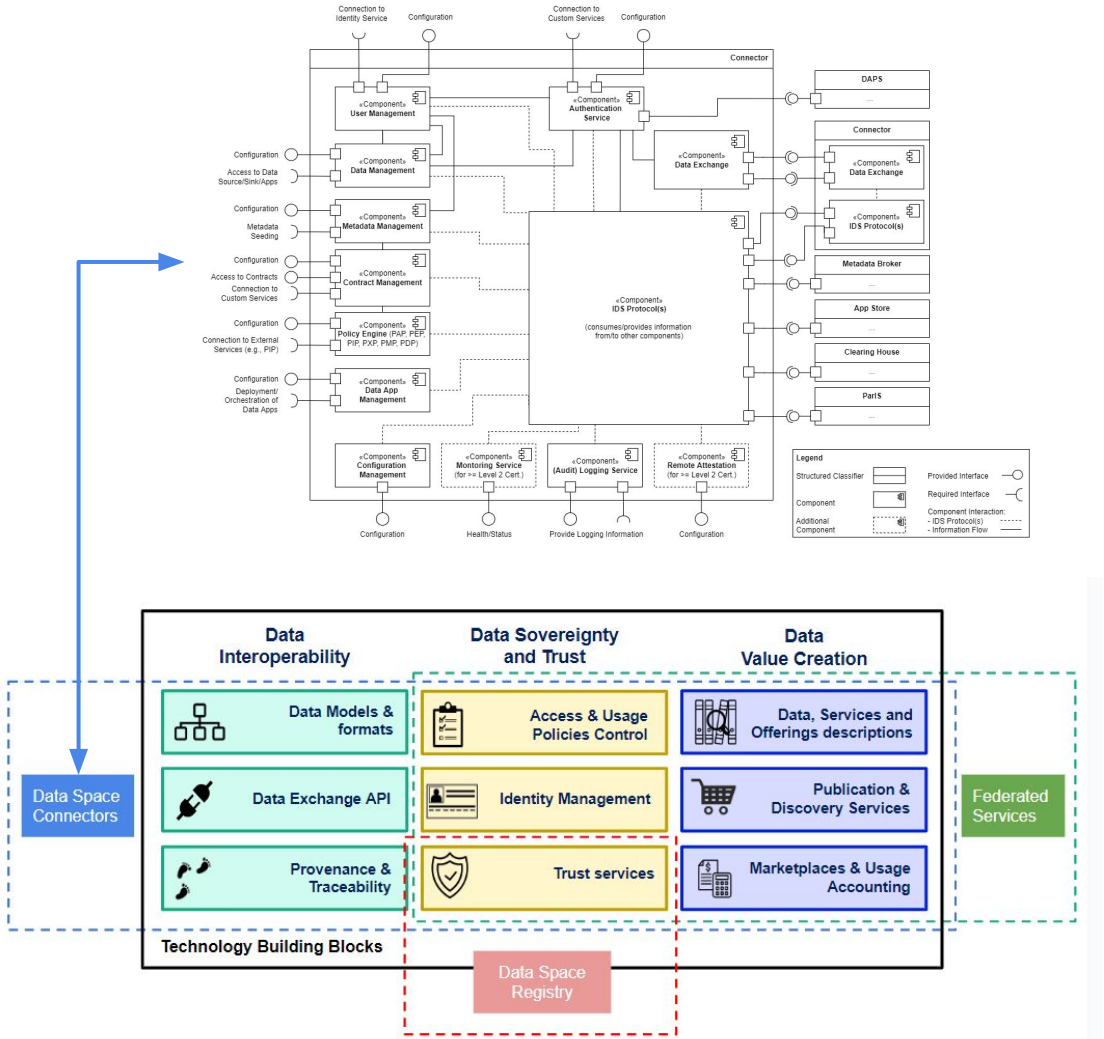
Reference specifications: Data interoperability

- Providers of data products within data spaces must be able to offer data services at well defined endpoints knowing that customers, unknown by them a priori, will know how to consume their data services through those endpoints.
- This means that all participants in data spaces should ‘speak the same language’, addressing interoperability at several levels (see ISO/IEC 21823-1):
  - transport and syntactic level → common APIs
  - semantic level → common data models/vocabularies
- We propose NGSI-LD for transfer of digital twin data and Dataspace Connector Protocols for the Control of data transfer
- Adoption of common data models is encouraged and there are multiple references that may consider (ISO/IEC CIM for Energy, SAREF, …) - the Smart Data Models initiative brings a hub that solves how different data models are mapped into JSON, JSON-LD and other data serialization formats
- In some data spaces, it may be necessary to make the data sharing process observable - to be addressed in future versions

FIWARE

Data Space Connector concept

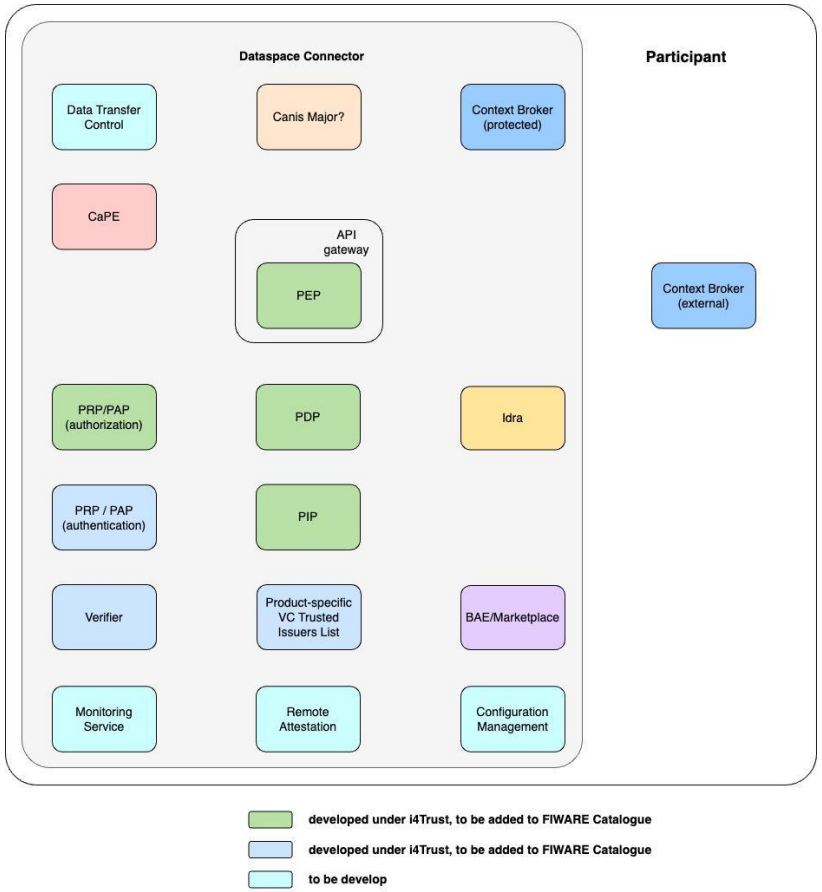
- The concept of Data Space Connector has evolved to match the idea of an integrated suite of components every organization participating in a data space should deploy to “connect” to the data space
- These components would be deployed and configured in controlled environments (e.g., a Kubernetes cluster) and implement a number of services which may be required for an organization to connect in its role as provider of data services, consumer of data services or both:
  - Authentication (including the interface to trust services)
  - Authorization (policy enforcement)
  - Connection to Data Exchange APIs
  - Data resources publication (Metadata Management)
  - Contract Management
  - Logging
  - Remote Attestation
  - …
- The concept of [Data Space Connector in IDS RAM 4.0] evolved to support this vision



FIWARE Data Space Connector

- A first release of FIWARE Data Space Connector components together with recipes for deployment was released September 2023 combining components already aligning with DSBA TC recommendations:
  - Context Broker technology for Data Exchange/Transfer
  - Trust and IM components implementing W3C DID + VC/VP standards and SIOPv2/OIDC4VP protocols, interface to trust services based on extended EBSI APIs (Trusted Issuers Registry)
  - PDP enforcing policies specified in ODRL
  - Modules implementing TM Forum APIs for marketplace functions (BAE marketplace components may be configured on top to contract via portal)
- Coming soon:
  - Support to IDS Transfer Process Dataspace Protocol
- For future releases, following modules will be incorporated:
  - DCAT-compliant data resources catalog for Metadata Management → aligning with IDS Catalog Dataspace Protocol
  - Logging modules based on either BAE/marketplace functions for logging or, if we want to rely on blockchain, Cannis Major
- The FIWARE Data Space Connector is the best aligned with DSBA recommendations or EU DI directives available in the market

https://github.com/FIWARE/data-space-connector

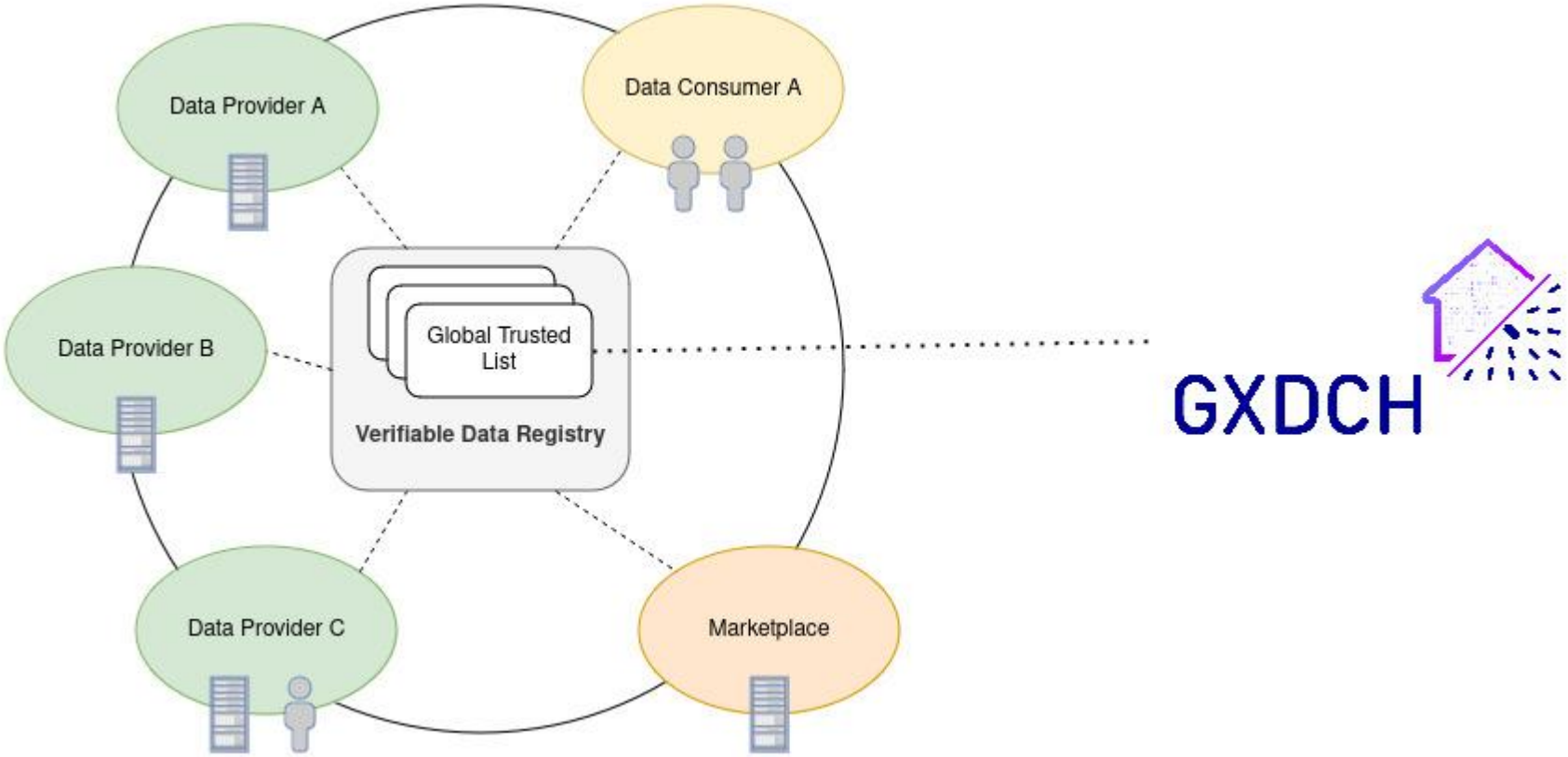


Integration with Gaia-X

Integration with Gaia-X

- Gaia-X is a European initiative aimed at developing a federated and secure data infrastructure to ensure data sovereignty, interoperability and transparency
- the Gaia-X Trust Framework is a set of rule that defines the minimum baseline to be part of the ecosystem
- Verifiable Credentials and Link Data representations as cornerstones, providing trust information in a machine readable format
    - defined schemas and formats to be used
- Gaia-X Digital Clearing Houses to ensure compliance, trust and interoperability within the federated data infrastructure
    - act as neutral “trust anchors”, validating and certifying participants, services and data exchanges

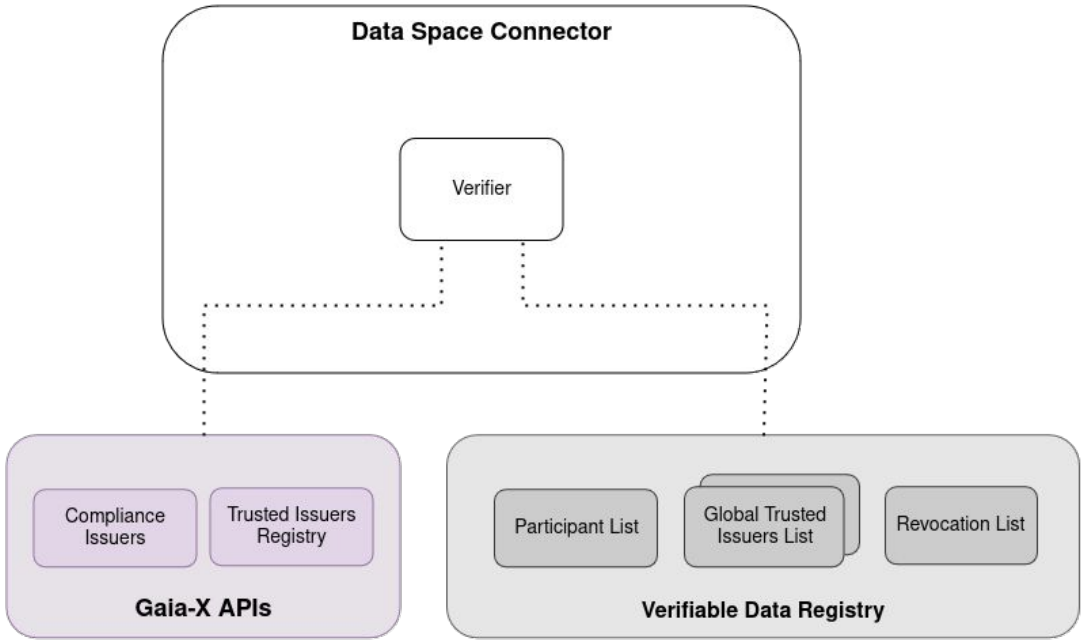
Integration with Gaia-X



FIWARE

Integration with Gaia-X

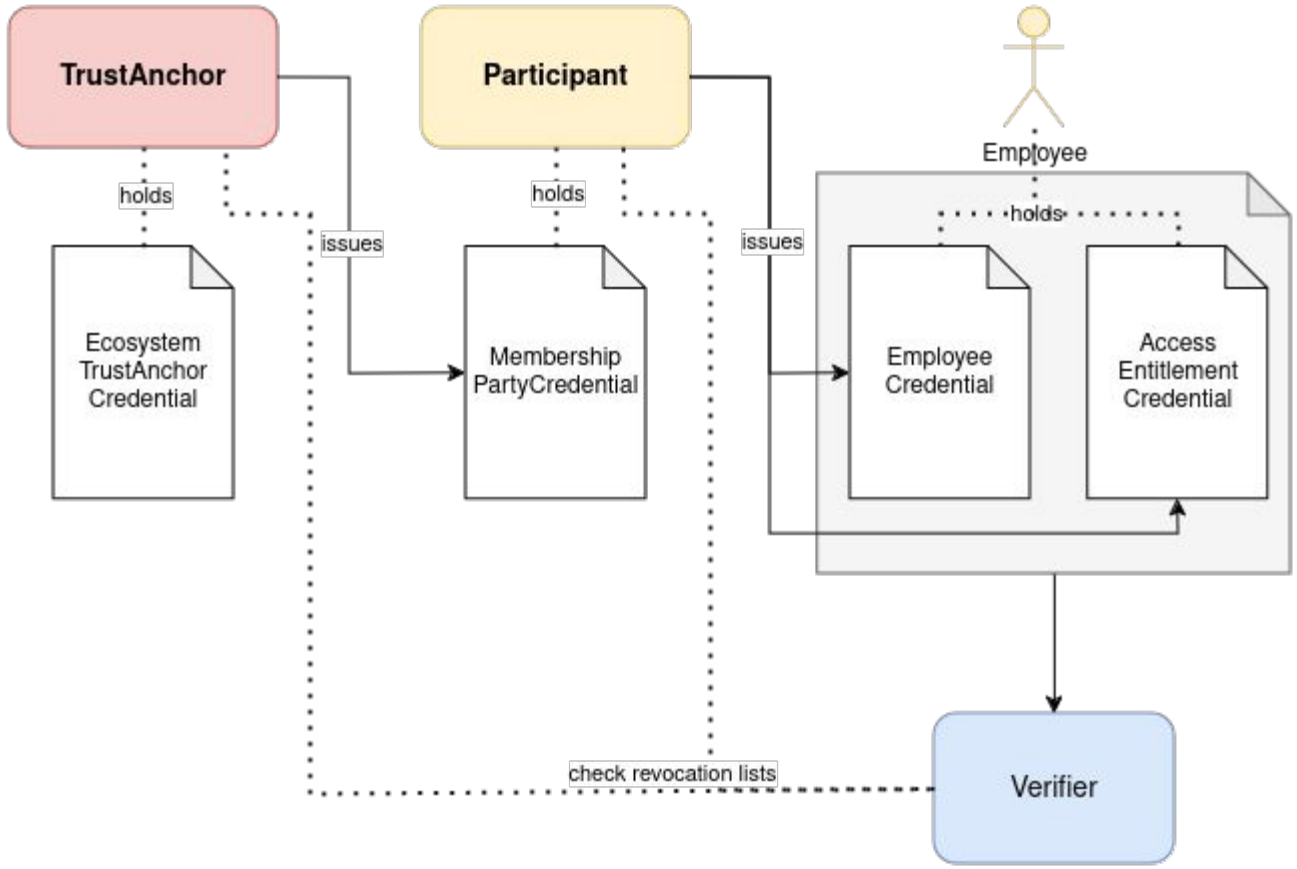
- Gaia-X Digital Clearing Houses as Trust Anchor for FIWARE Data Spaces
  - extension of the VCVerifier to support the Gaia-X Registry APIs as Verifiable Data Registry



FIWARE

Integration with Gaia-X

- Support of the Gaia-X Verifiable Credentials Formats:
  - TrustAnchorCredentials as base of the Data Space Trust Anchor
  - MembershipPartyCredentials for Participants
  - PartyCredentials and their specializations(f.e. Employee Credential) to be used by Legal and Natural Persons
- Authentication through VerifiablePresentations containing the Gaia-X Credentials
  - Gaia-X compliant checks at revocation lists of TrustAnchor and Participant
  - support Revocation Lists in the Data Space Connector



FIWARE

Integration with Gaia-X

- Support the Gaia-X ODRL VC Profile in the ODRL-PAP
- Intention of the profile: refer VerifiableCredentials claims in a clear and precise way within ODRL Policies
- Example Policy:

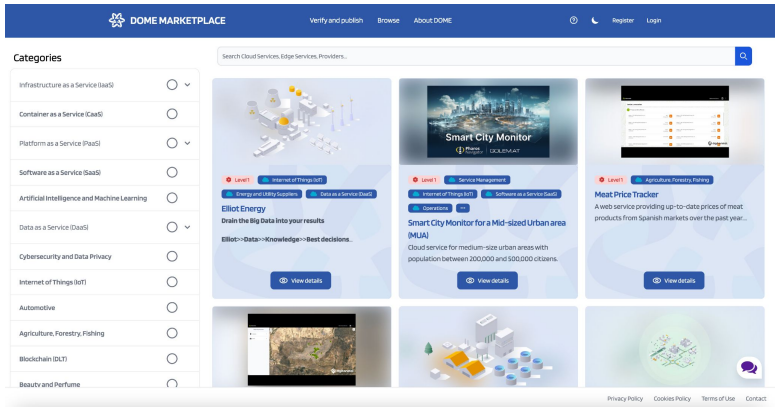
```
{
        “@context”: {…},
        …
        “odrl:permission”:  [
                “odrl:target”: “urn:ngsi-ld:entity:1”,
                “odrl:action”: “odrl:read”,
                “odrl:assigner”: “did:web:my-data-provider.org”,
                “ovc:constraint”: [
                        {
                                “ovc:leftOperand”: “$.credentialSubject.gx:legalAddress.gx:countrySubdivisionCode”,
                                “odrl:operator”: “odrl:isAnyOf”,
                                “odrl:rightOperand”: [“FR-HDF”, “BE-BRU”],
                                “ovc:credentialSubjectType”: “gx:LegalParticipant”
                        }
                ]
        ]
}
```

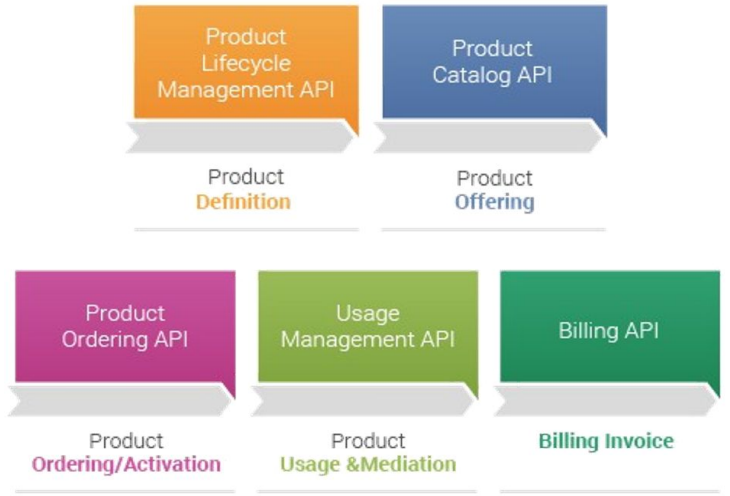

FIWARE

Integration with DOME

DOME: Distributed Open Marketplace for Europe

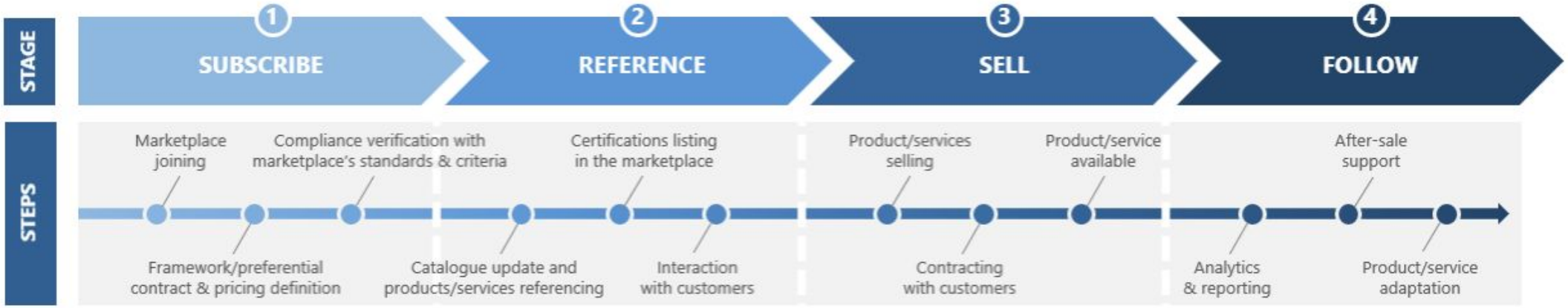
- DOME will take the form of a **shared digital catalogue of cloud and edge services made available through**:
  - the **global DOME portal**; or
  - **federated marketplaces**
- DOME relies on TM Forum Open API specifications with regards to the definition of its underlying information model as well as APIs supporting:
  - storage of info about products, product specifications and product offerings
  - storage of logs during procurement and usage of products
- Product specifications and product offering descriptions are made available as Verifiable Presentations (= set of Verifiable Credentials) defined according to Gaia-X specifications
  - VCs issued by certification agencies describing compliance with certain regulations/recommendations (e.g., GDPR, low carbon)
  - VCs issued by certification agencies on compliance with certain standards (e.g., NGSI-LD, support of standard data models)
  - VCs describing roles (claims) that are meaningful to assign to service users and policy rules that are defined on roles and other environment attributes
  - etc
- Marketplaces for Data Spaces can federate with DOME or use DOME as base marketplace



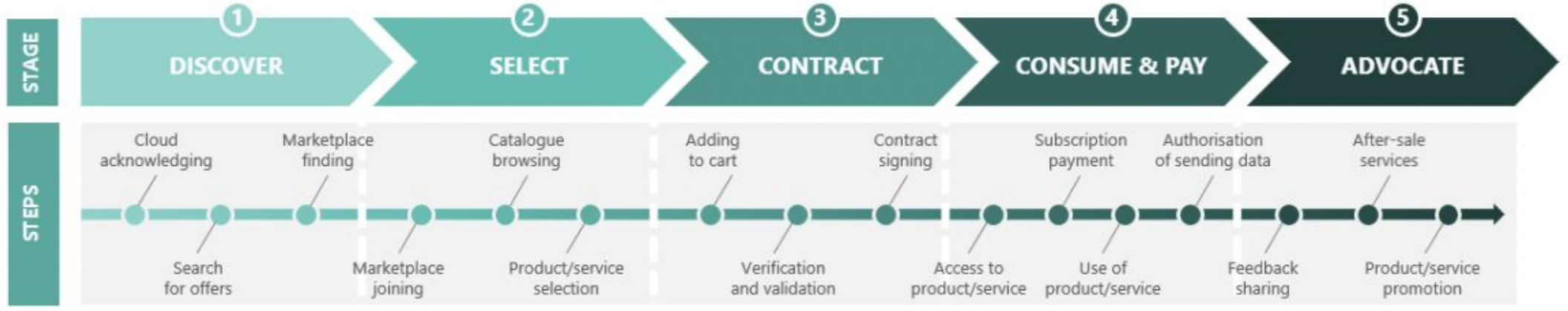


Service Provider and Customer journeys

Cloud and Edge Service Provider journey*

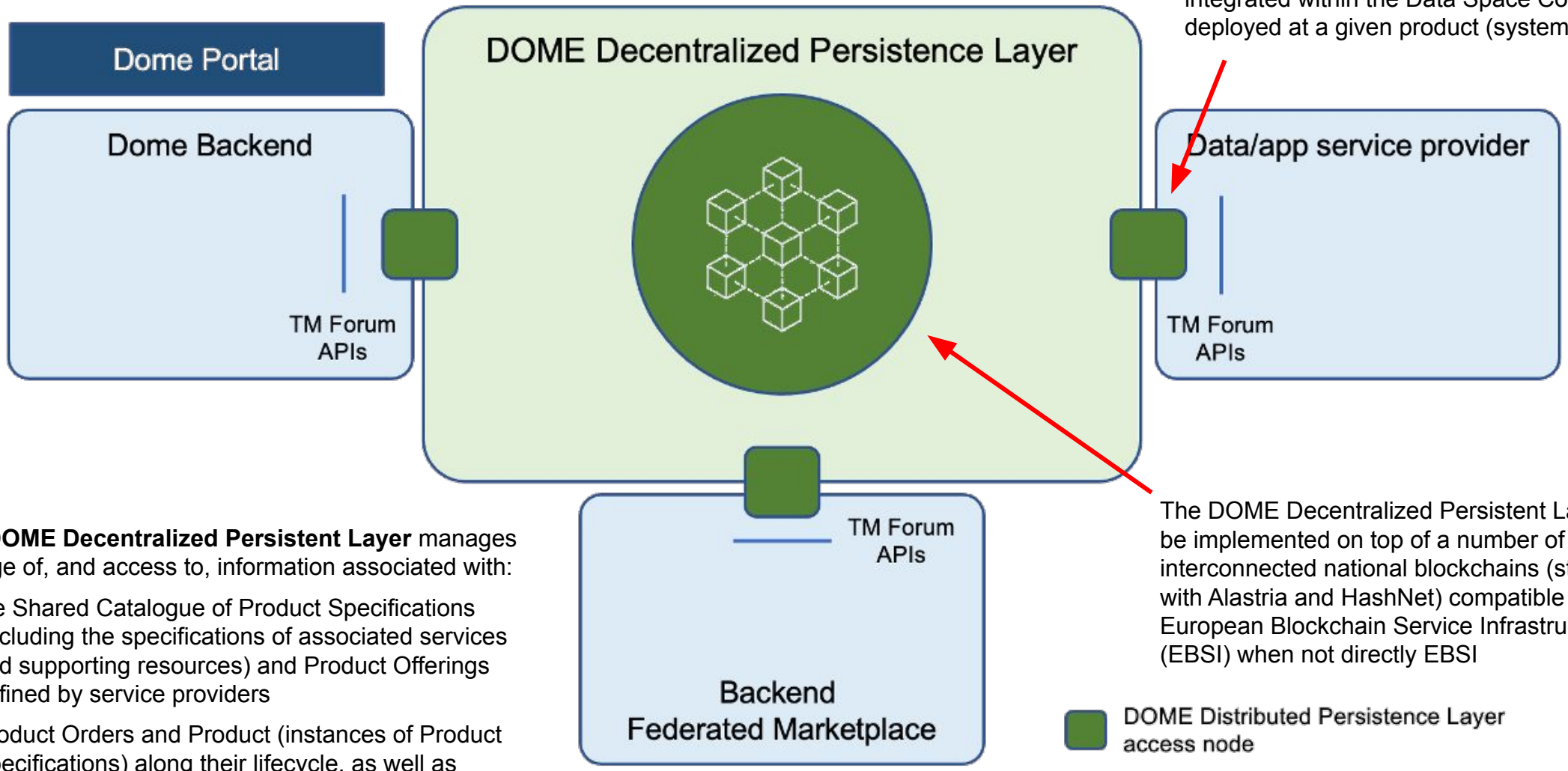


Customer journey*



* source: “conceptualization study on the European cloud marketplace” - Cap Gemini

Marketplaces federation + Shared Catalogue (Architecture)

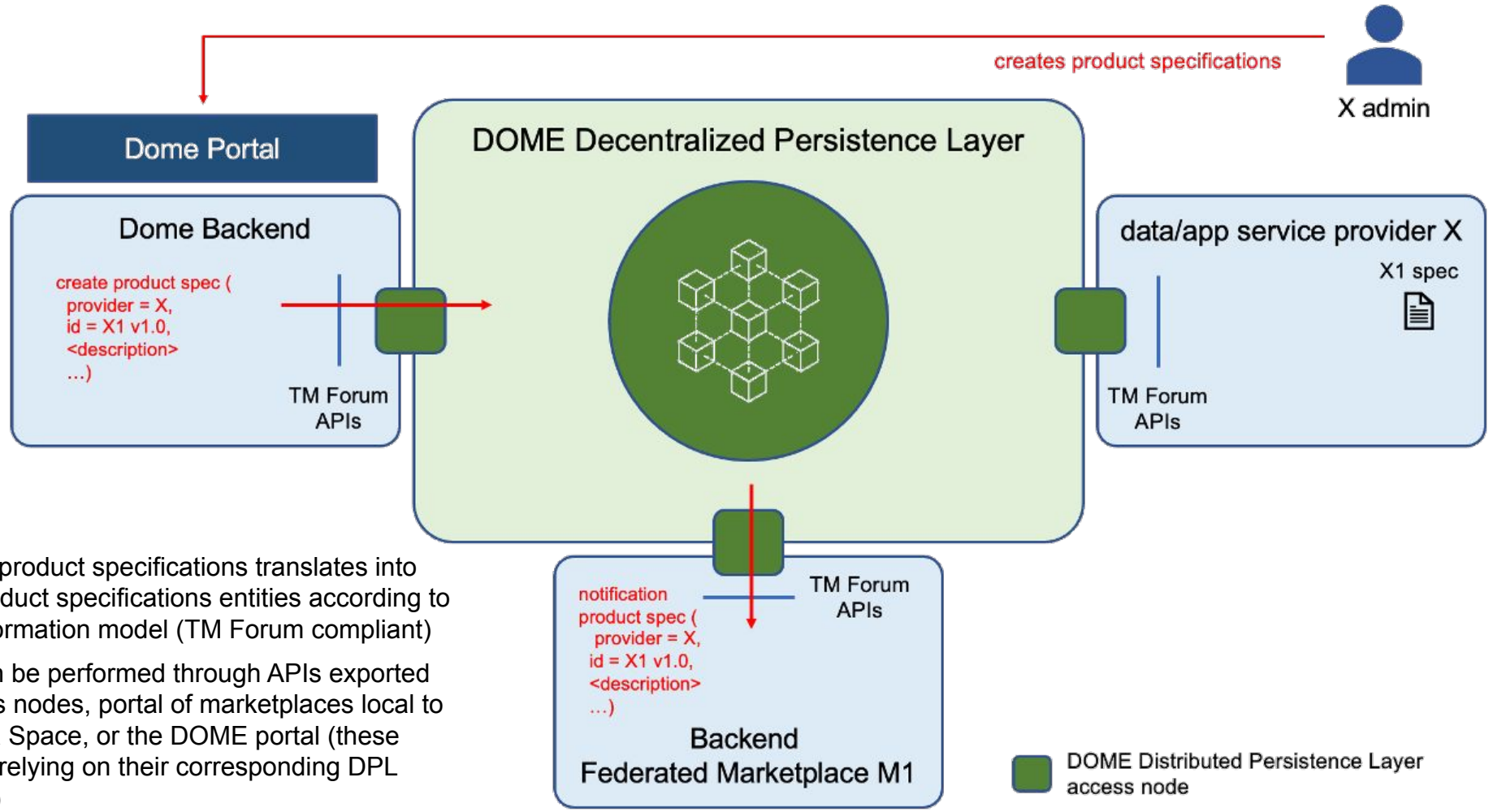


The **DOME Decentralized Persistent Layer** manages storage of, and access to, information associated with:

- the Shared Catalogue of Product Specifications (including the specifications of associated services and supporting resources) and Product Offerings defined by service providers
- Product Orders and Product (instances of Product Specifications) along their lifecycle, as well as information about actual Usage of Products

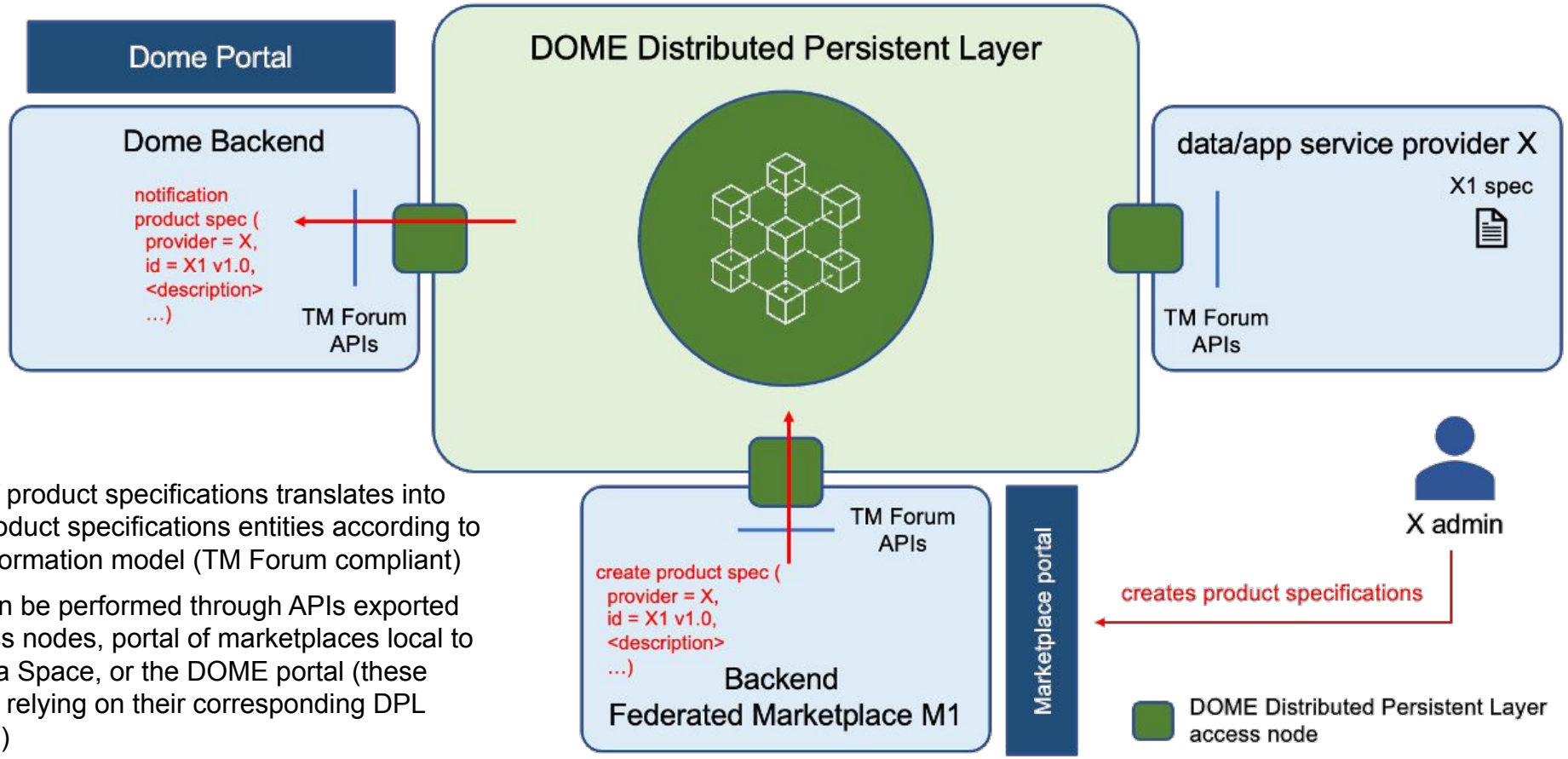
FIWARE

Registration of product specifications



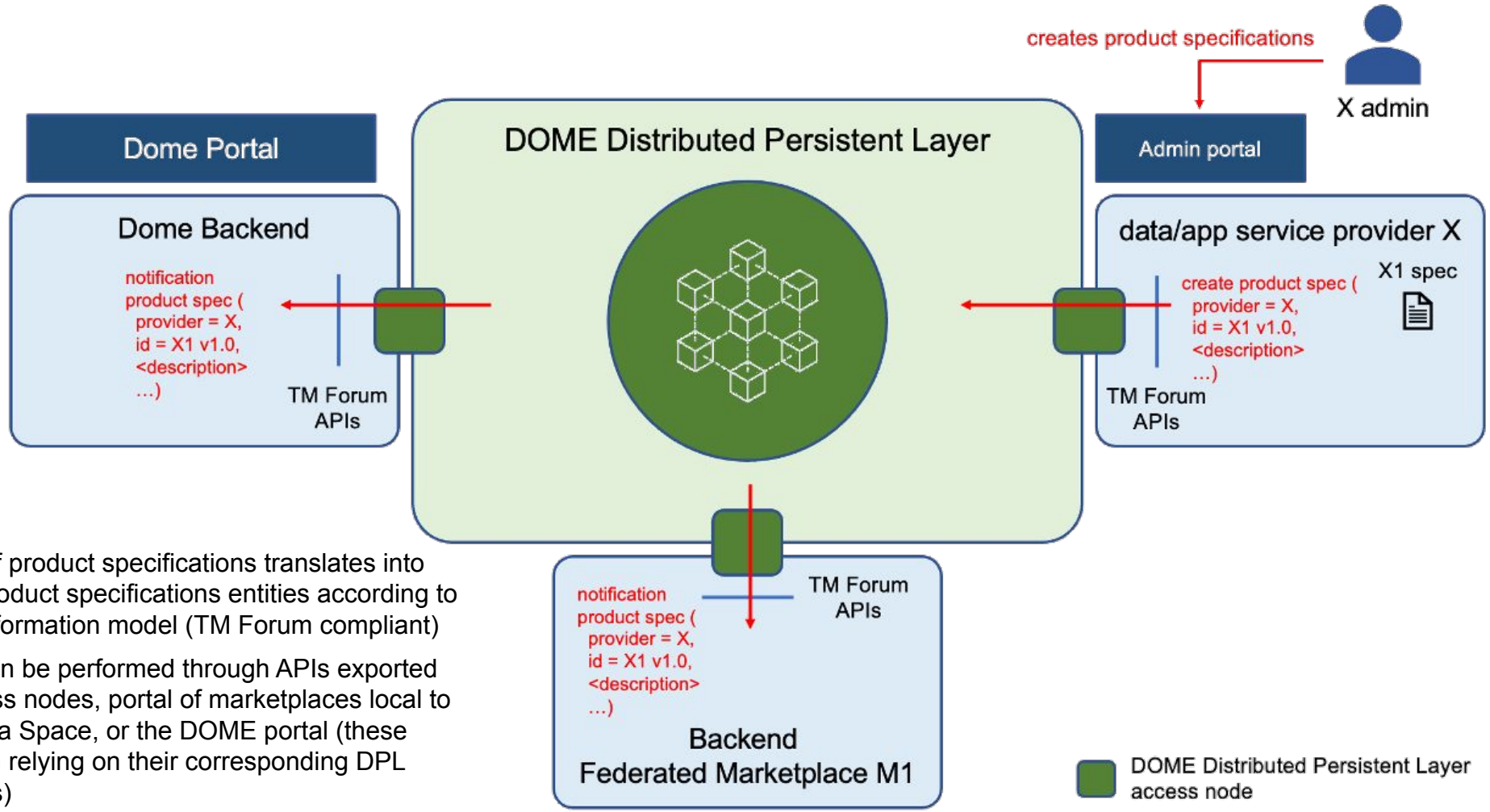
- registration of product specifications translates into creation of product specifications entities according to the DOME information model (TM Forum compliant)
- operations can be performed through APIs exported by DPL access nodes, portal of marketplaces local to the given Data Space, or the DOME portal (these portals in turn relying on their corresponding DPL access nodes)

Registration of product specifications



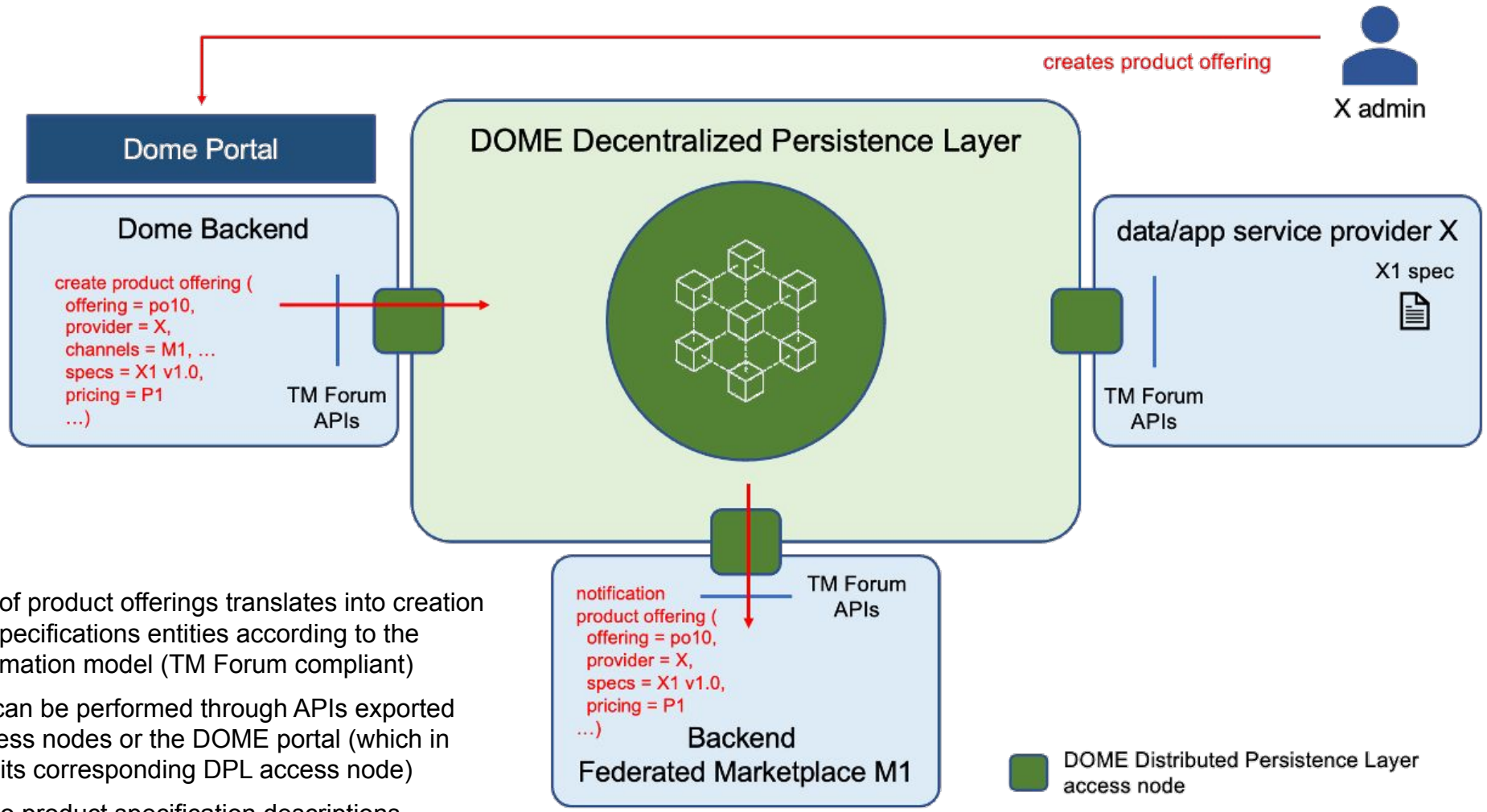
- registration of product specifications translates into creation of product specifications entities according to the DOME information model (TM Forum compliant)
- operations can be performed through APIs exported by DPL access nodes, portal of marketplaces local to the given Data Space, or the DOME portal (these portals in turn relying on their corresponding DPL access nodes)

Registration of product specifications



- registration of product specifications translates into creation of product specifications entities according to the DOME information model (TM Forum compliant)
- operations can be performed through APIs exported by DPL access nodes, portal of marketplaces local to the given Data Space, or the DOME portal (these portals in turn relying on their corresponding DPL access nodes)

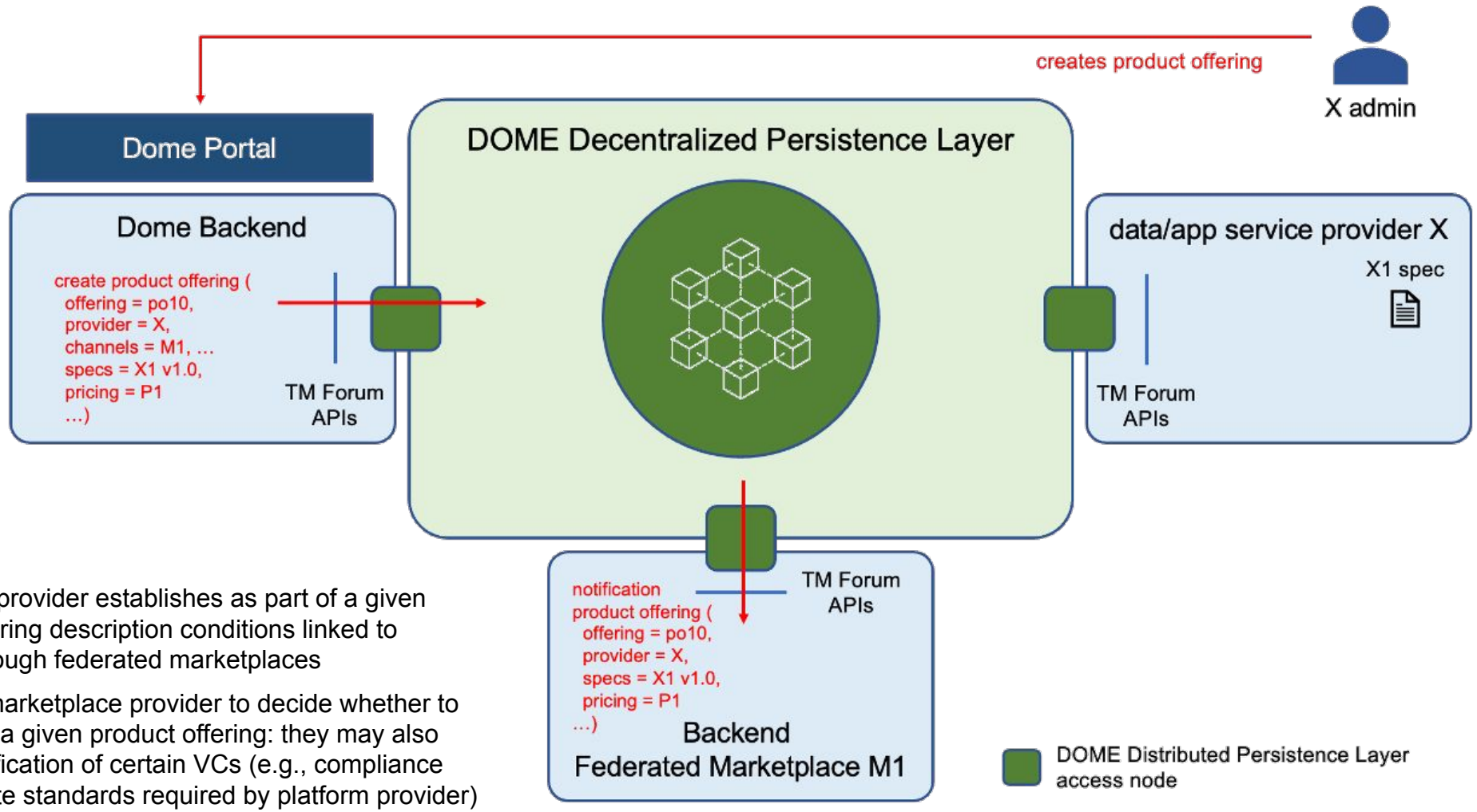
Creation of Product Offering



- registration of product offerings translates into creation of product specifications entities according to the DOME information model (TM Forum compliant)
- operations can be performed through APIs exported by DPL access nodes or the DOME portal (which in turn rely on its corresponding DPL access node)
- VPs linked to product specification descriptions following Gaia-X specifications are also generated and stored on the blockchain

FIWARE

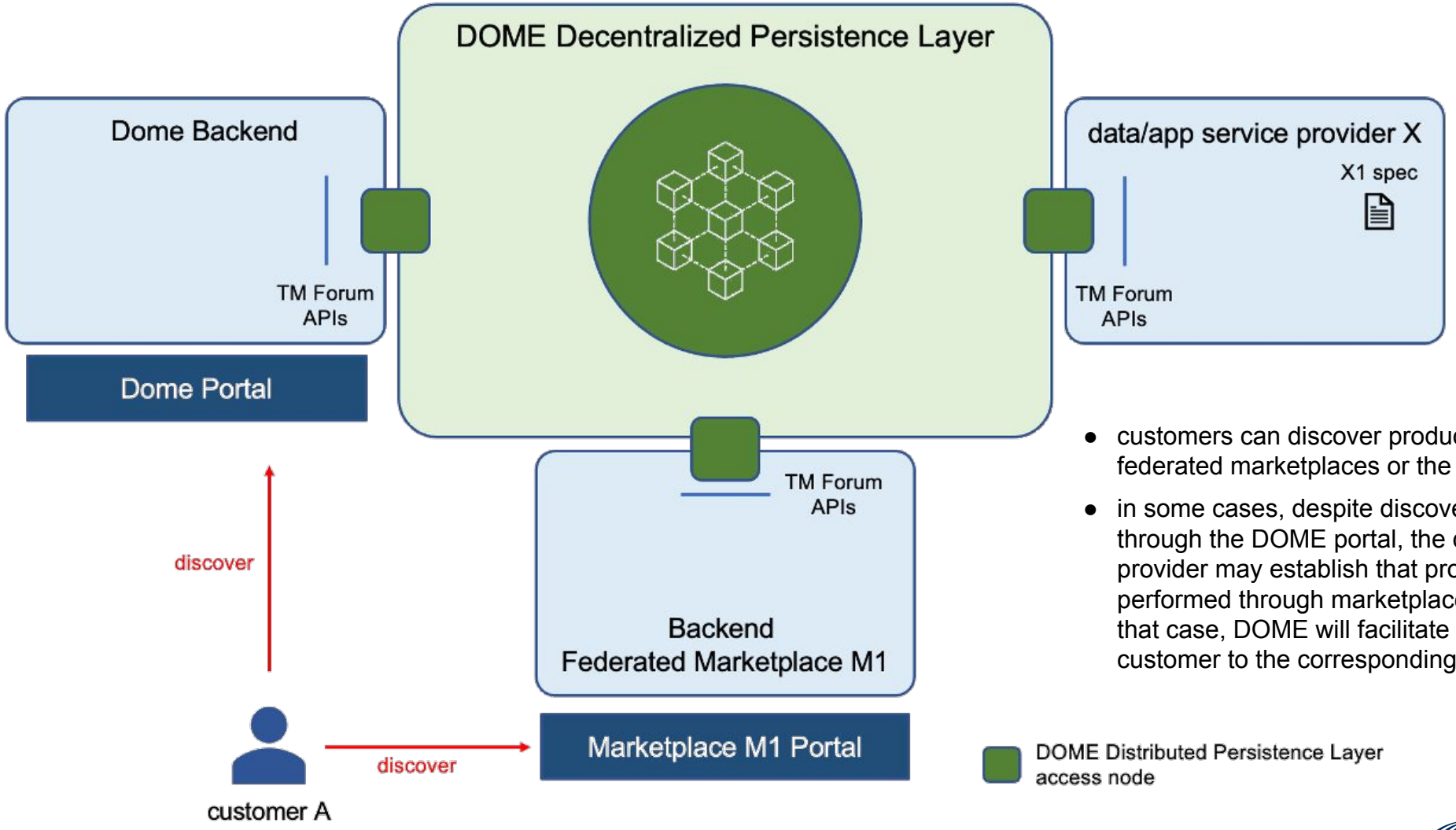
Creation of Product Offering (cont.)



- the service provider establishes as part of a given product offering description conditions linked to visibility through federated marketplaces
- its up to a marketplace provider to decide whether to incorporate a given product offering: they may also require verification of certain VCs (e.g., compliance with concrete standards required by platform provider) beyond those that are mandatory for DOME

FIWARE

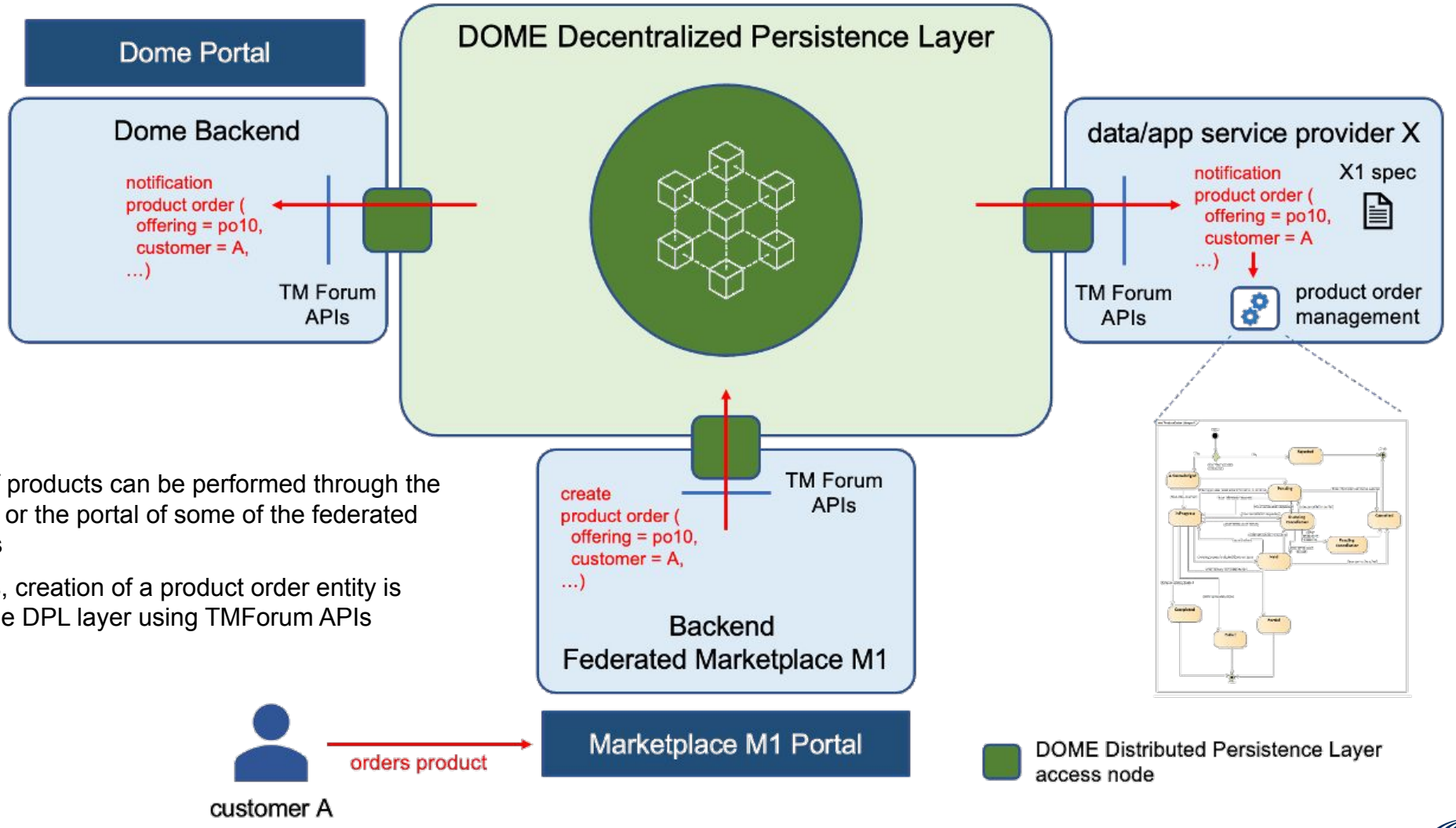
Product offering discovery



- customers can discover product offerings through a federated marketplaces or the DOME portal
- in some cases, despite discovery can take place through the DOME portal, the data/app service provider may establish that procurement has to be performed through marketplaces of its choice - in that case, DOME will facilitate navigation of the customer to the corresponding portal

FIWARE

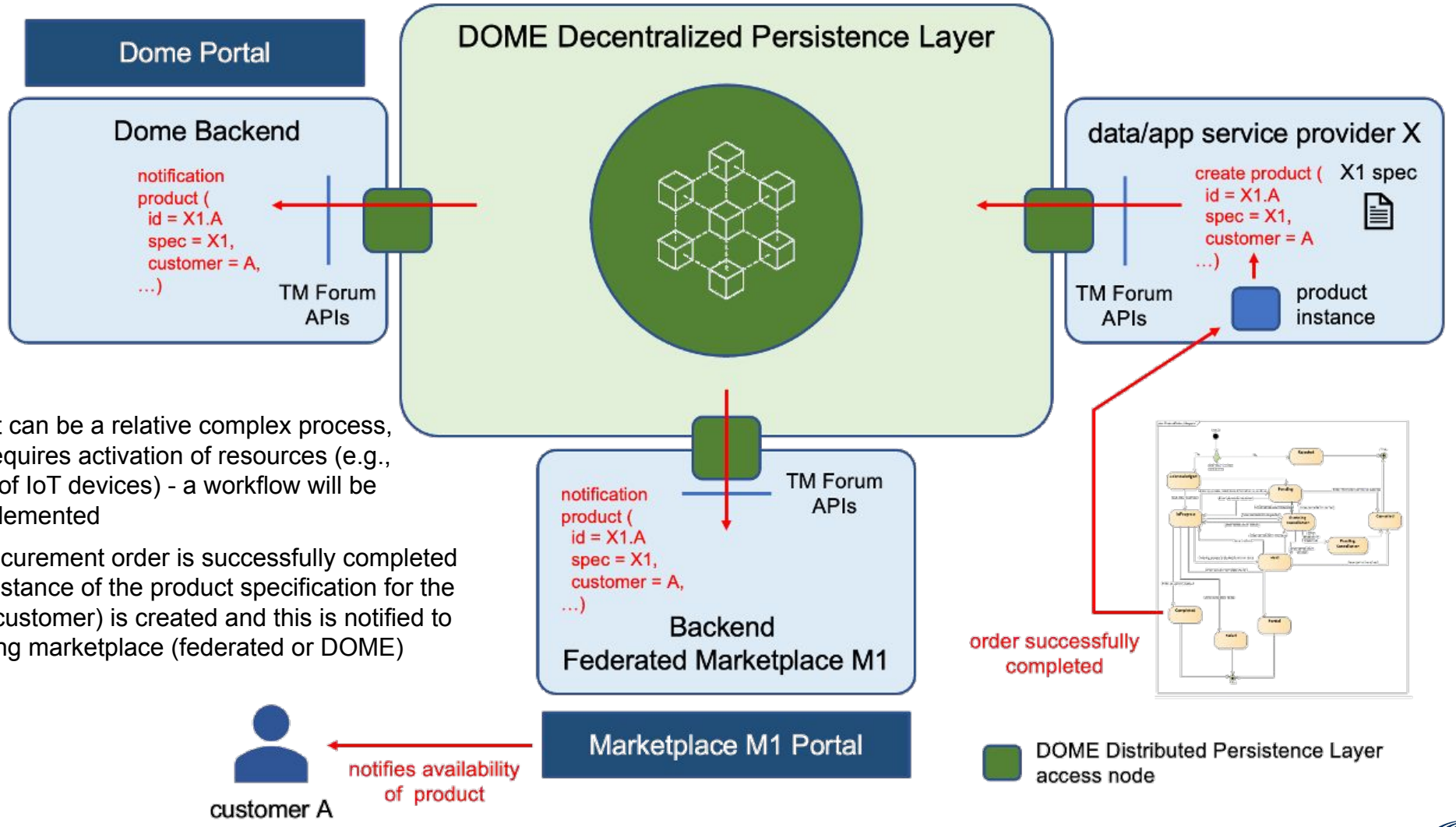
Product acquisition (through federated marketplace)



- acquisition of products can be performed through the DOME portal or the portal of some of the federated marketplaces
- in both cases, creation of a product order entity is issued into the DPL layer using TMForum APIs

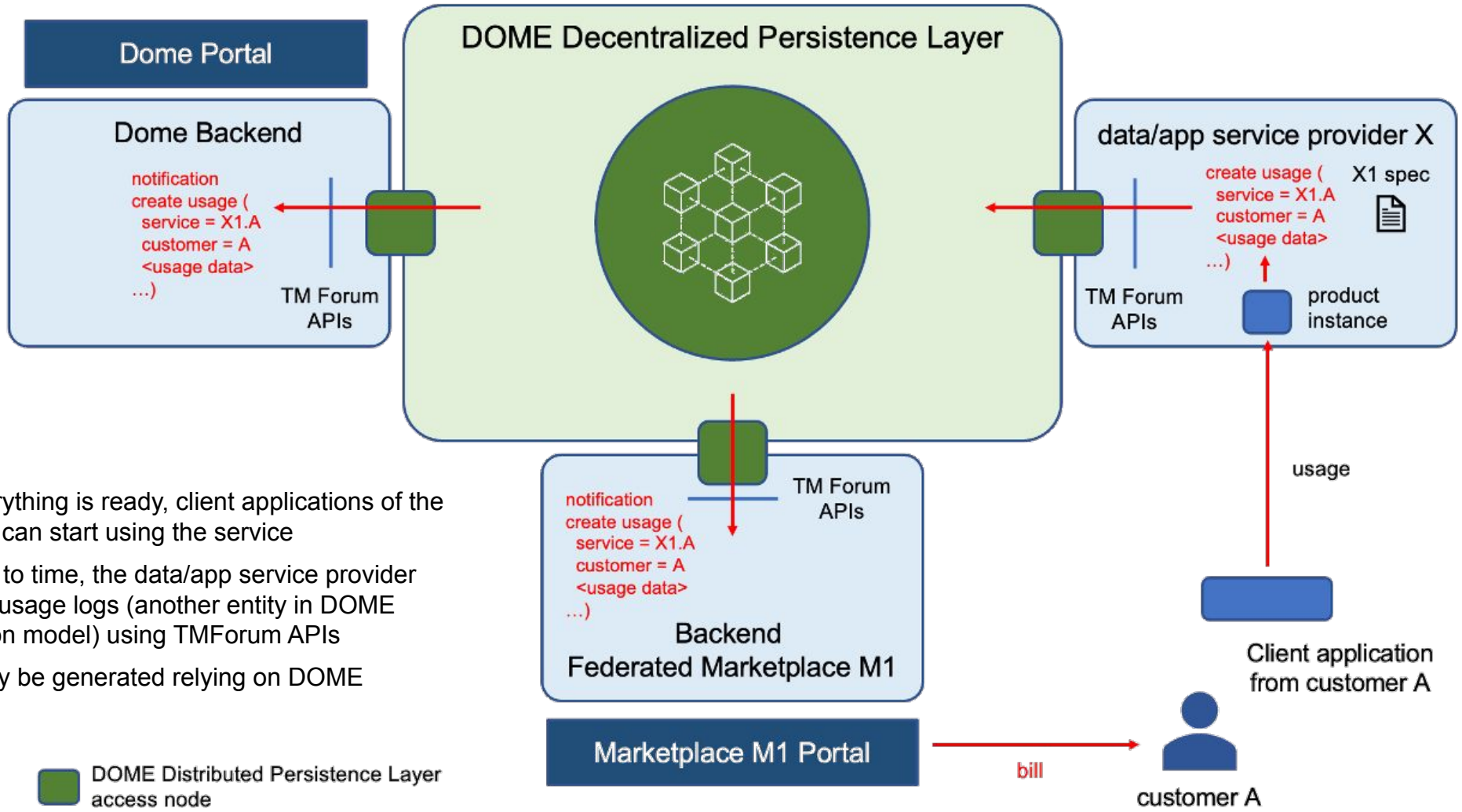
FIWARE

Product activation (product becomes available for use)



- procurement can be a relative complex process, overall if it requires activation of resources (e.g., deployment of IoT devices) - a workflow will be typically implemented
- once the procurement order is successfully completed a product (instance of the product specification for the demanding customer) is created and this is notified to the generating marketplace (federated or DOME)

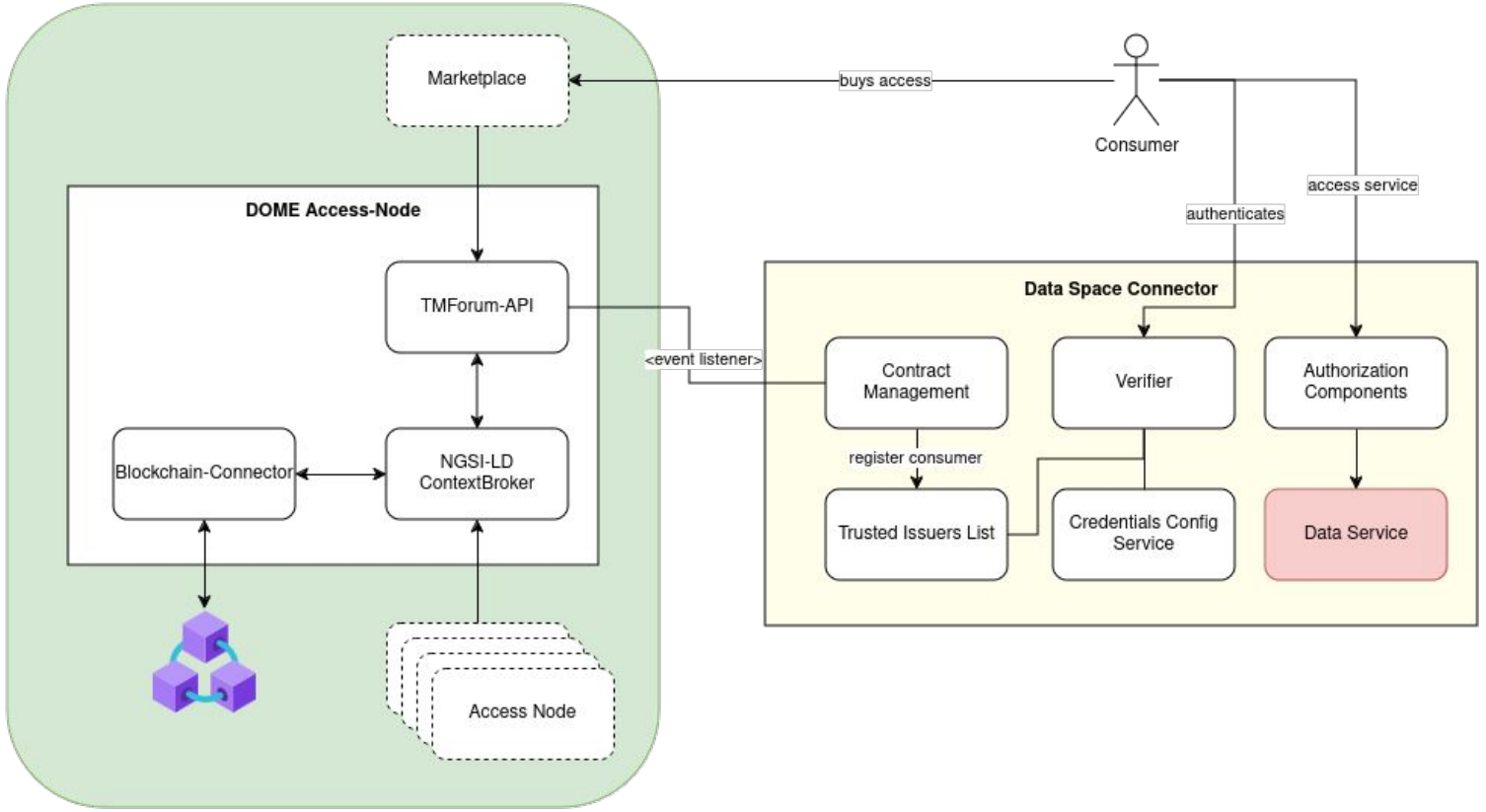
Product usage



- once everything is ready, client applications of the customer can start using the service
- from time to time, the data/app service provider generate usage logs (another entity in DOME information model) using TMForum APIs
- billing may be generated relying on DOME

Data Space Connector - Access Node Integration

- Data Service is offered at the Marketplace and can be purchased by a Consumer
- Data Space Connector integrates through TMForum-EventListeners
- Contract Management reacts on purchase, registers the new consumer
- Consumer is now allowed to authenticate for the service
- Consumer can access the service

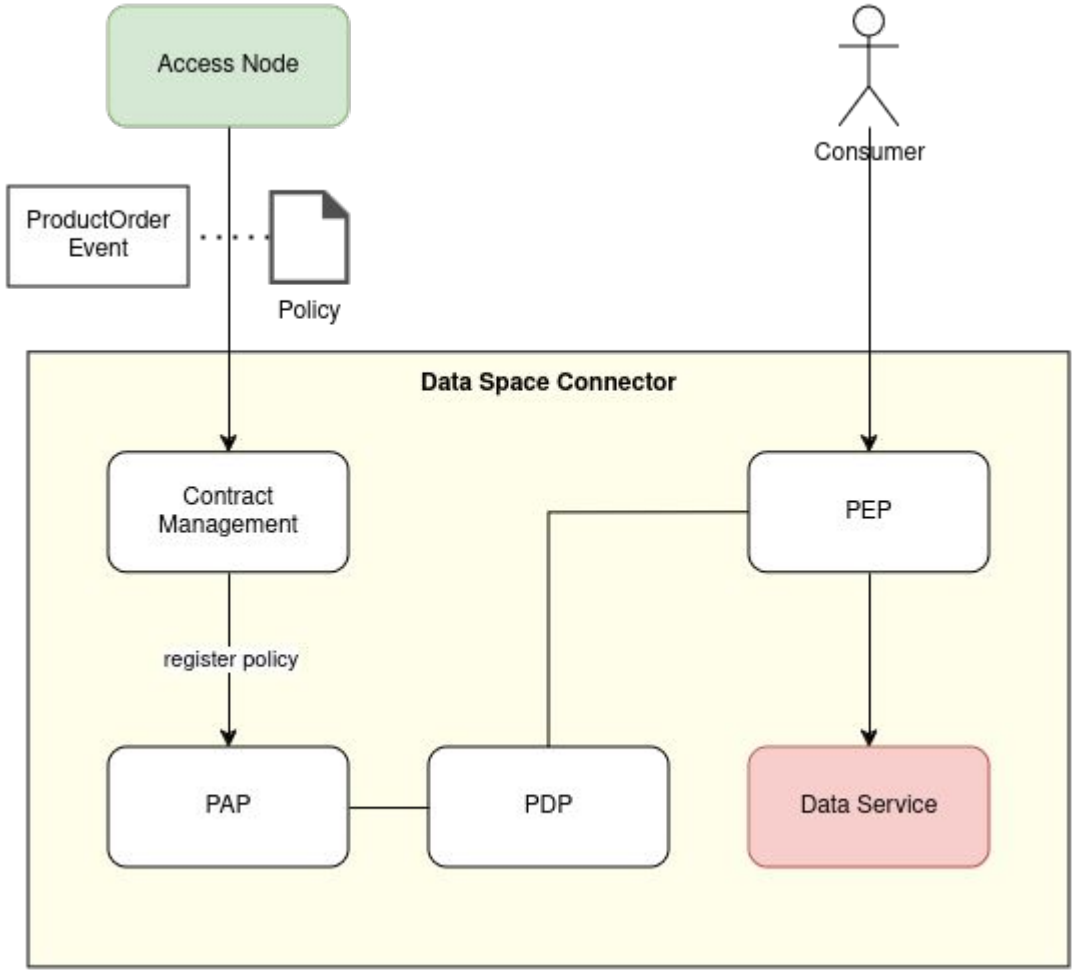


FIWARE

Policy Integration

- ODRL-Policies can be attached to Offerings and might differ on the concrete purchase
- concrete Policy to be provided as part of the Order-Event
- registered through Contract Management at the PAP
- Automatically enforced through the Data Space Connector Authorization Framework

- Status in DOME:
  - Concrete Policy Implementation in DOME still under discussion
  - Decisions expected in Q1/2025, ODRL was agreed on in principle

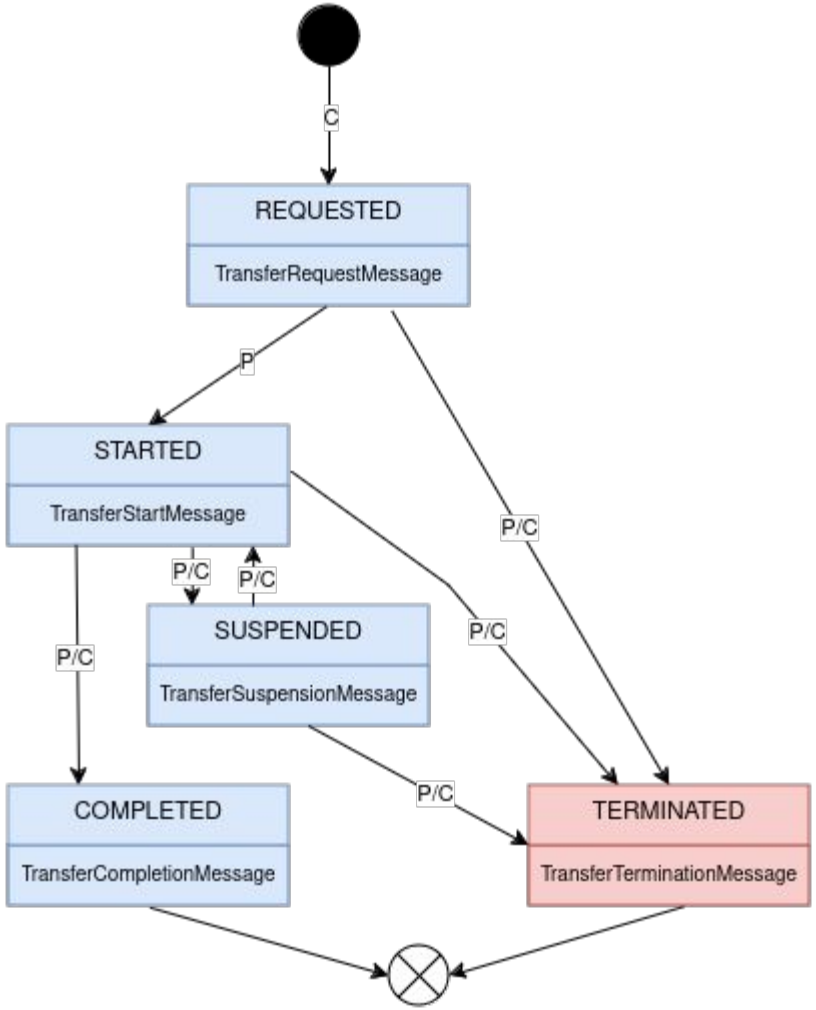


FIWARE

Support to IDSA/Eclipse Data Space Protocols

Integration of the IDSA Transfer Process Protocol

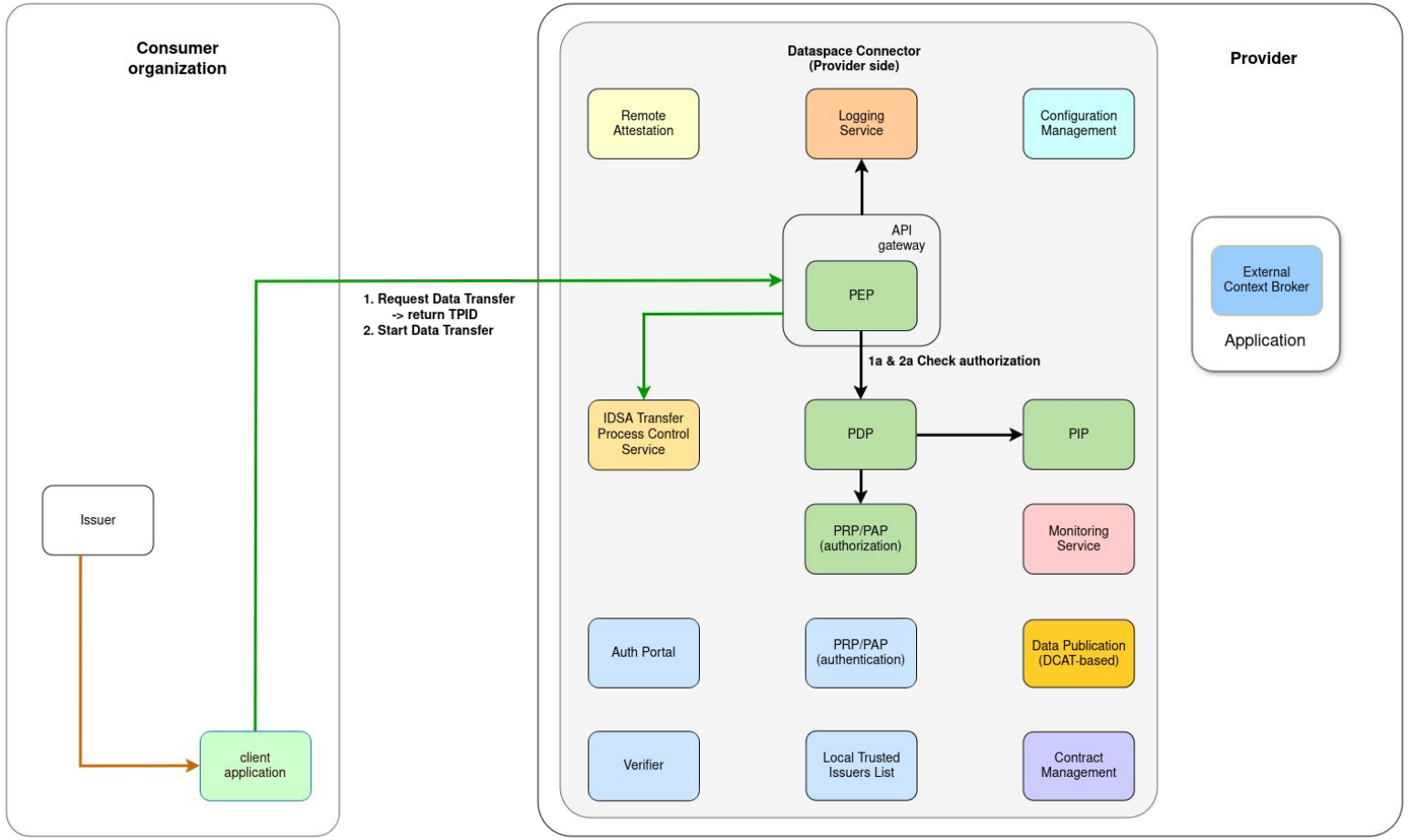
- The IDSA Dataspace Protocol is a set of specifications intended to facilitate interoperable data sharing
  - implementation of the protocols will allow the FIWARE Data Space Connector to be interoperable with alternative Data Space Connector implementations
- The Transfer Process Protocol is a state-machine, that defines the data transfer between two participants



FIWARE

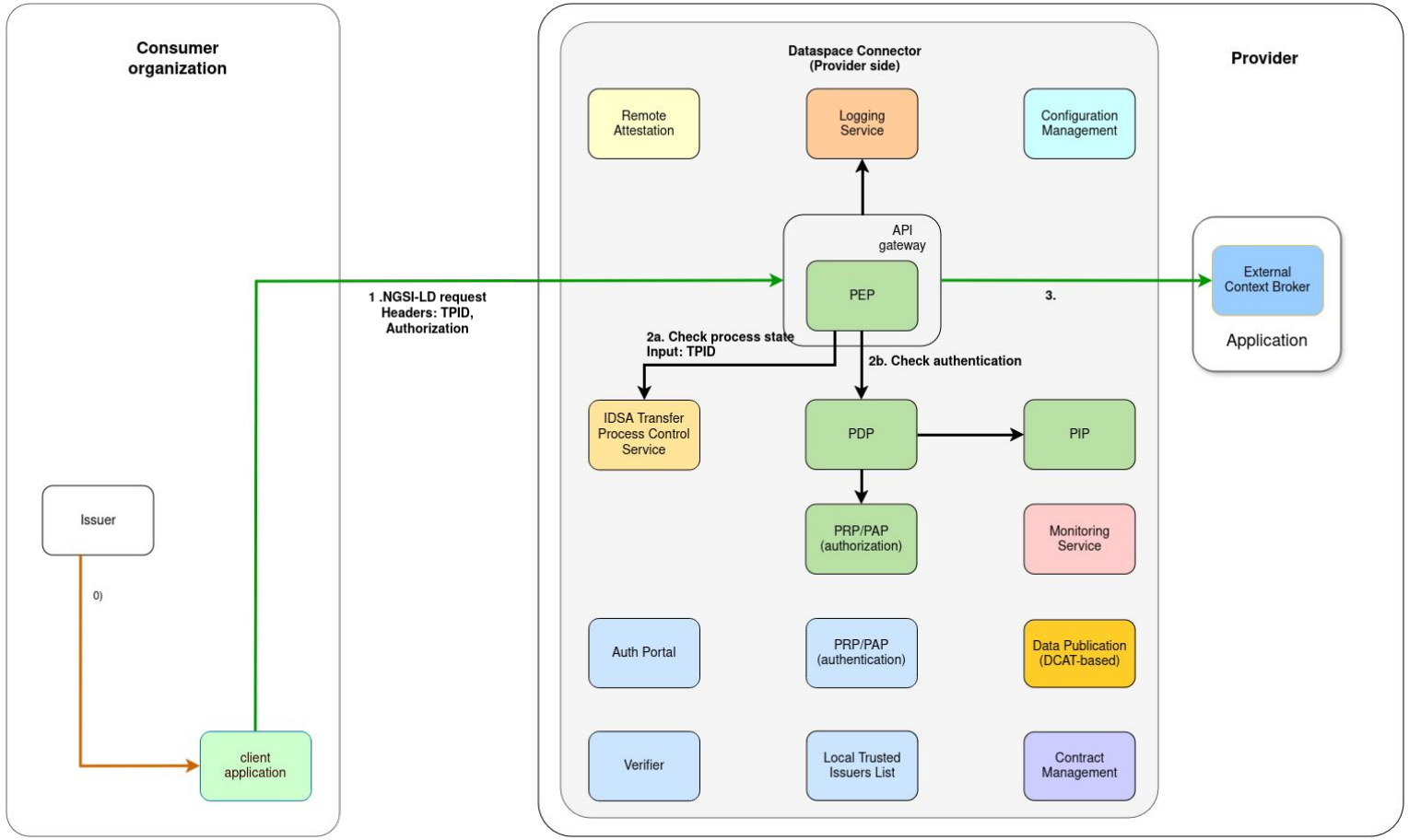
Integration of the IDSA Transfer Process Protocol

- IDSA Transfer Process Control Service(by UPM) integrated with the authorization components(PEP)
- Consumer connects the TPC-Service through the PEP
  - ➢ integrates with existing Authn/z Framework
  - ➢ Service is only available to participants
- Consumer requests a Data Transfer
  - ➢ State “REQUESTED”
  - ➢ TPID returned to the consumer
- Consumer requests to start the data transfer
  - ➢ State “STARTED”



Integration of the IDSA Transfer Process Protocol

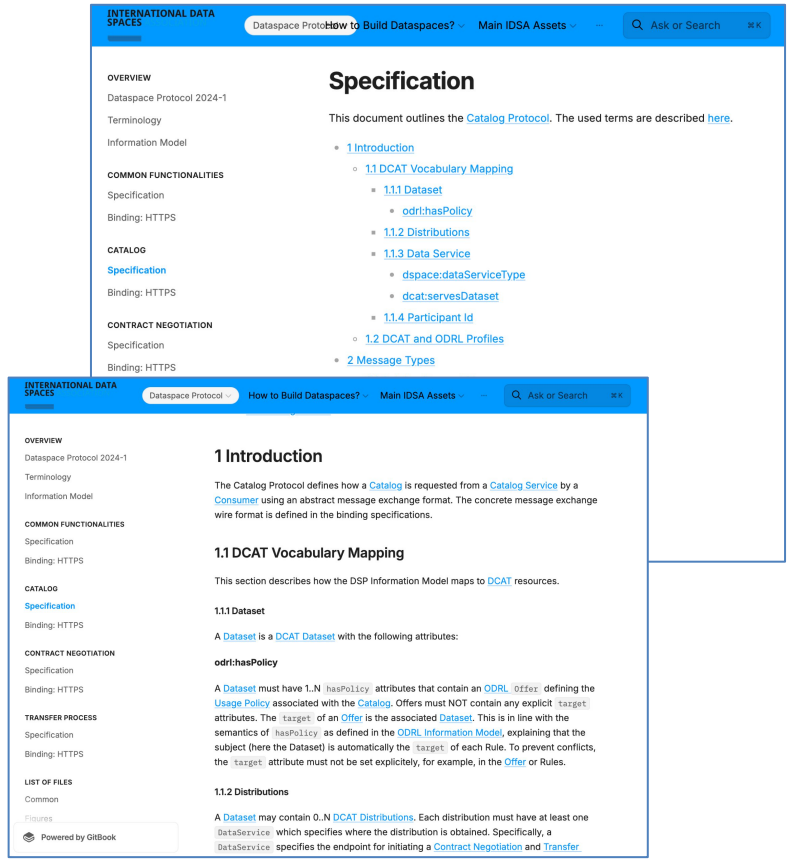
- Consumer sends request to the PEP
  - ➢ includes TPID as header
  - ➢ includes authorization header
- PEP checks:
  - ➢ process state at the Transfer Process Control Service
  - ➢ existing policies at the PDP
- If authorization is granted and state==”STARTED”, request is forwarded
- both participants can suspend, complete or terminate the process at the Transfer Process Control Service
  - ➢ subsequent requests with the TPID will be rejected



FIWARE

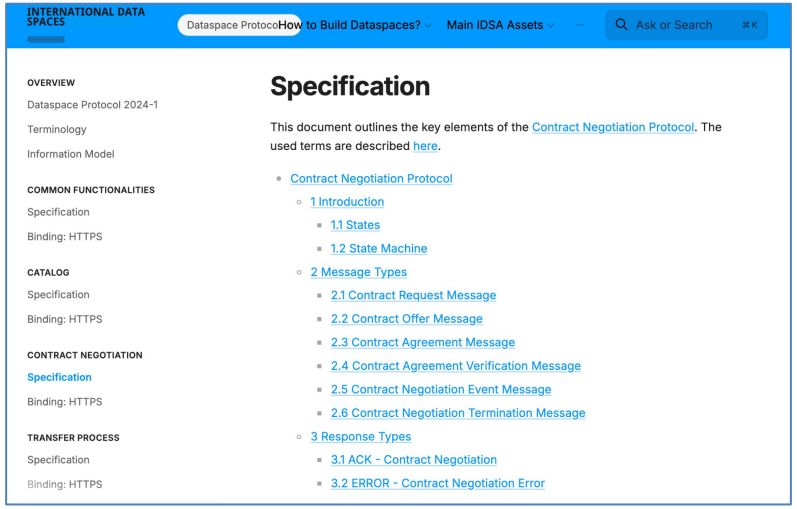
Catalog Protocol

- Our vision:
  - Data services exposed and linked to systems connected to the data space can be published on DCAT-compliant catalogs, easing their discovery
  - Entries in DCAT-compliant catalogs should come with metadata identifying end points through which rights to access data services exposed by the systems connected to the data space can be acquired (essentially, end points exposing TM Forum APIs)
  - In FIWARE, we have experience developing extensions to existing data publication platforms so they can support the processes associated to acquisition of access rights (including eventual monetization)
  - Data Space Connectors may incorporate modules implementing catalogs exposing DCAT-compliant interfaces enabling discovery by applications using DCAT APIs and harvesting from global data publication portals that support the referred extensions
- The FIWARE Data Space Connector will evolve to incorporate modules implementing DCAT-compliant interfaces enabling the above described vision
- IDSA Data Space Catalog Protocol bring a bit limited vision, need to be extended to support key aspects mentioned above - from FIWARE we will implement a catalog module that is compatible with the IDSA/Eclipse Catalog Protocol but incorporates the necessary extensions to support these key aspects - we will contribute to evolution of the Catalog Protocol based on our implementation experience



Contract Negotiation Protocol

- Adoption of TM Forum APIs for managing registration of product specifications, product offerings and the lifecyle associated to the acquisition of rights to use data services ensures compatibility with DOME and means relying on mature industry-tested global open standard specifications
- TM Forum API specifications already addresses aspects related to the monetization of services as well as the support to all kind of scenarios linked to the acquisition of rights to use services or the provisioning and activation of services
- We will work towards contributing to the IDSA/Eclipse Contract Negotiation Protocol in order to incorporate everything that is needed and ensure compatibility with TM Forum APIs and DOME



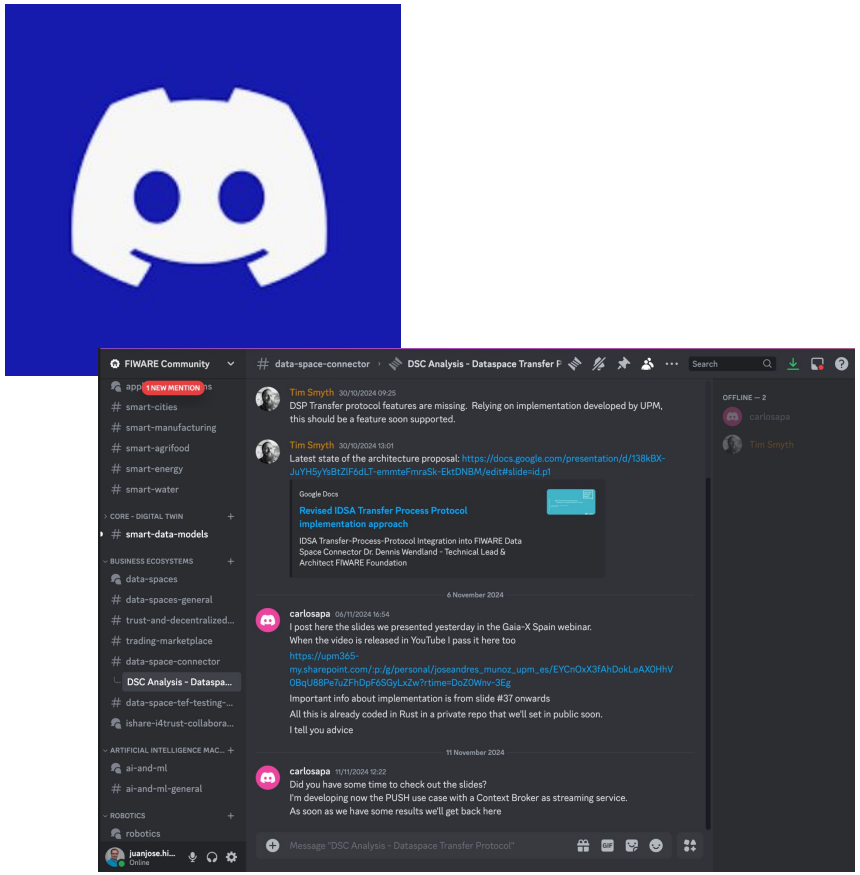
FIWARE

How to join / follow up

FIWARE

Wish to follow or join us?

- A Data Space WG was created under the umbrella of FIWARE TSC activities to follow up on all activities related to development of FIWARE Data Space components
- The WG meets regularly on a weekly basis - wish to join us? contact us (Juanjo Hierro, Stefan Wiedemann)
- A FIWARE Community on Discord has been configured (still in testing mode) for enabling instant exchange and discussion with the experts - don’t hesitate to join us on Discord channels linked to data spaces:
  - #data-space-connector
  - #trust-and-decentralized-iam



FIWARE

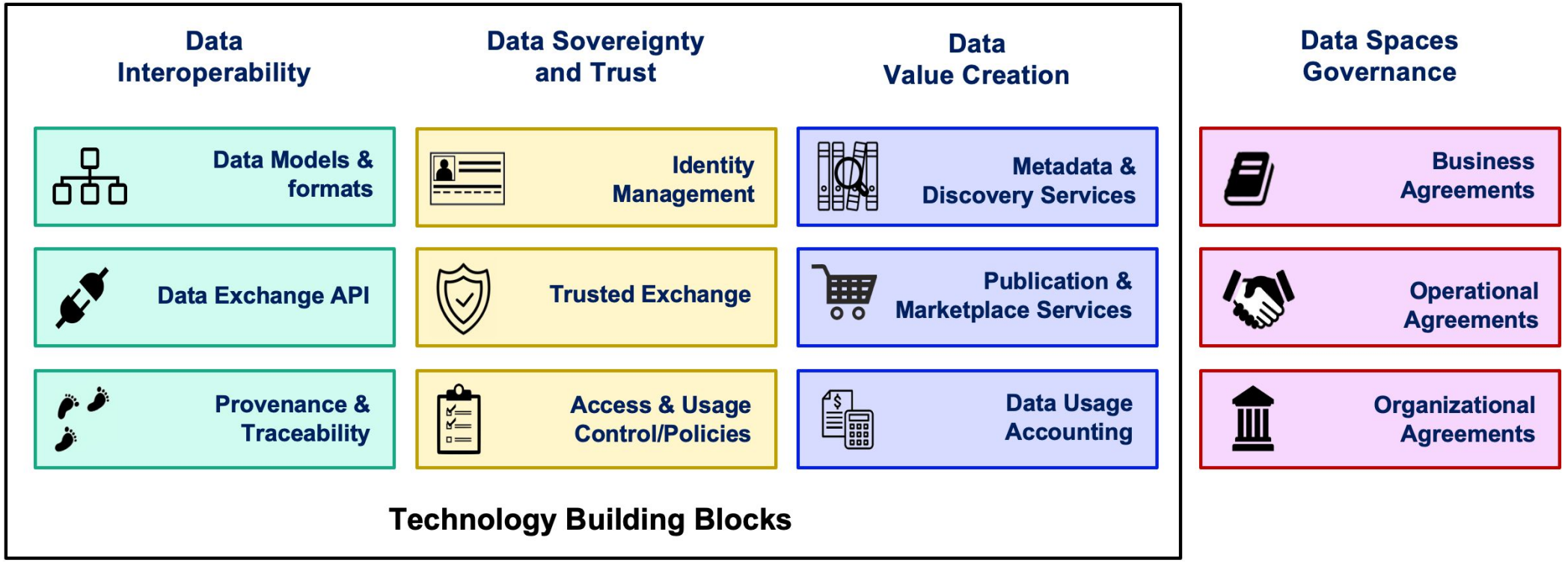
Sounds nice? - Contact us!

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

Juanjo Hierro
chairman
FIWARE Technical Steering Committee
juanjose.hierro@gmail.com

FIWARE

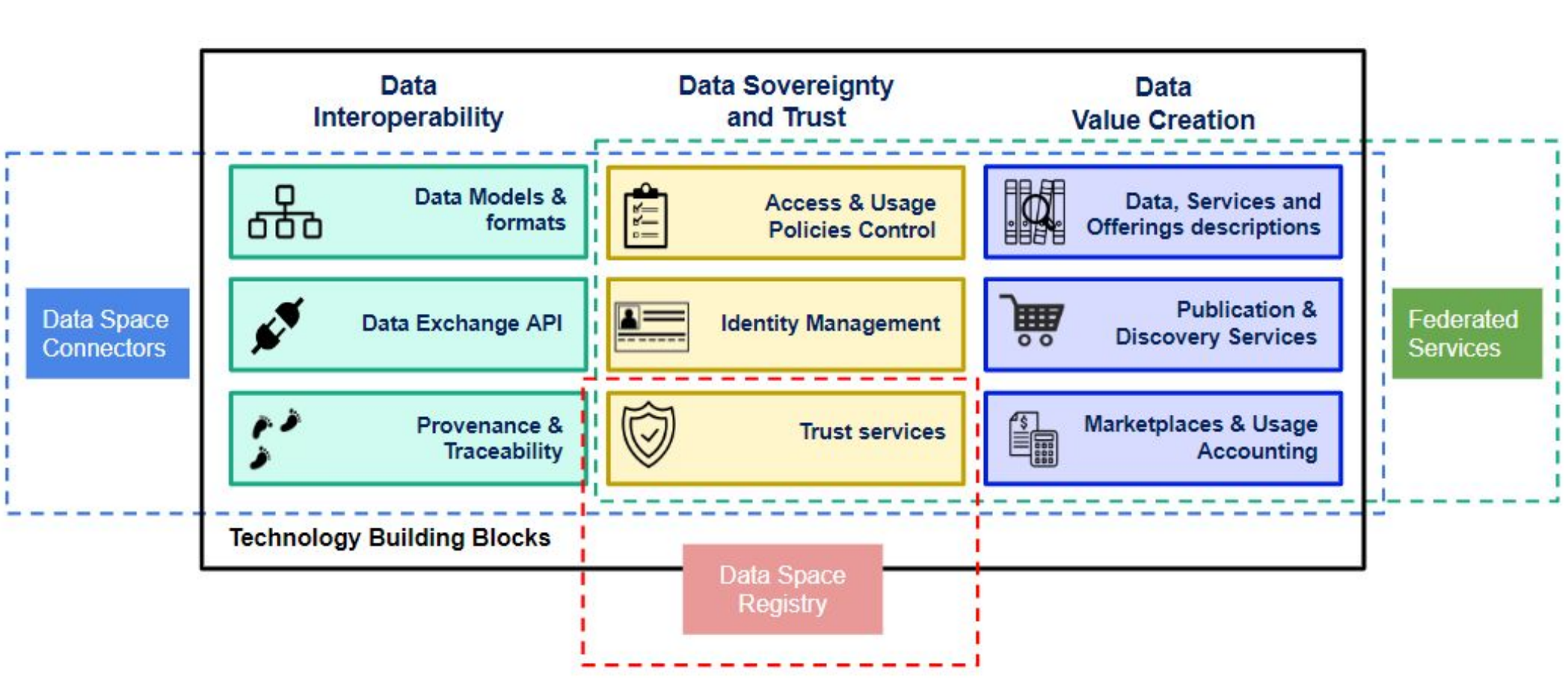
Data Spaces Building Blocks



MATERIALIZING DATA SPACES REQUIRES TO TAKE OPTIONS AND ADOPT A MINIMUM BUT ENOUGH SET OF TECHNOLOGY STANDARDS

FIWARE

Mapping of Technology Building Blocks and Systems



FIWARE

FIWARE helps to make things happen: transfering results of research to the market … we commit to do it for data spaces

Collaboration with iSHARE Foundation under the umbrella of [i4Trust program] and active participation in Gaia-X IAM WG (co-chairs)

- Trust Services APIs aligned with EBSI
- Support to DID+VC/VPs + SIOPv2 and OIDC4VP

Driving fast-growing library of smart data models for developers ([website], [github]) following open agile approach

- 1000+ data models,
- 21K+ terms
- 150+ contributors

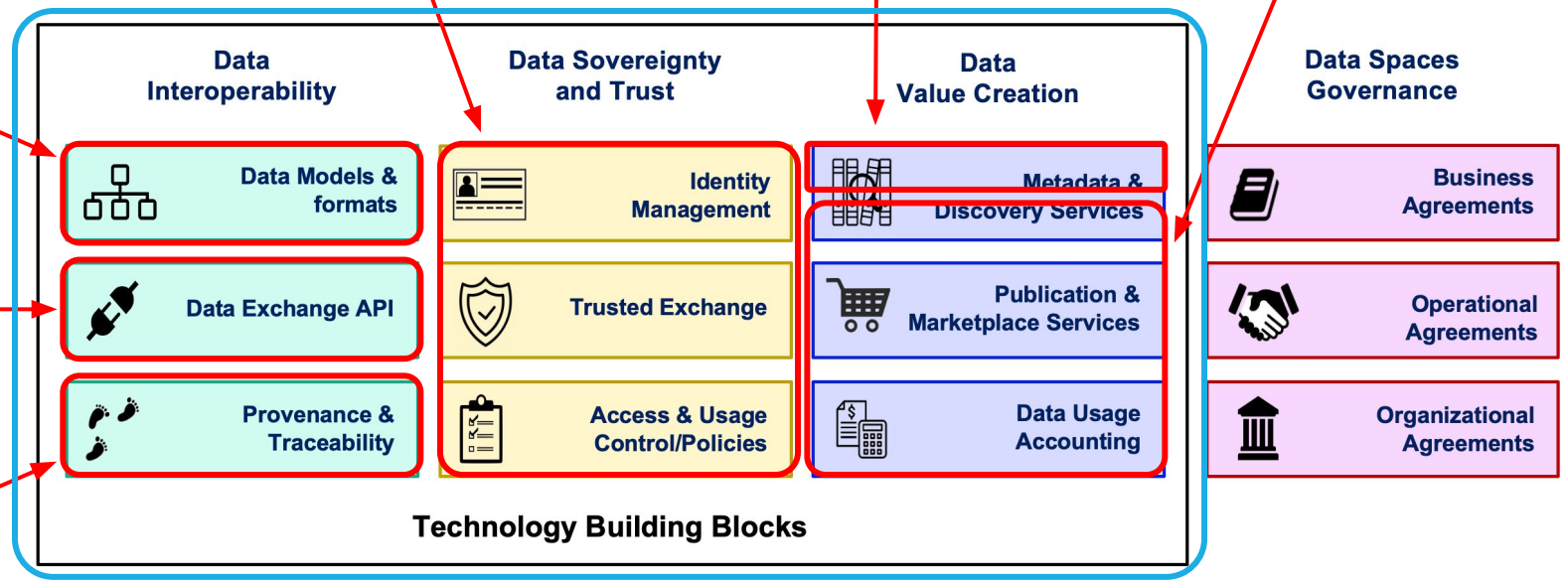
Experience implementing IDS Connector functions (TRUE Connector)

DCAT-compliant Idra component used in several market solutions

Marketplace Services open source components based on TM Forum industry standards used in i4Trust and now in DOME

Driving standardization of API for context / digital twin data exchange: [ETSI NGSI-LD]:

- de-facto for cities, growing adoption in other domains
- adopted beyond Europe



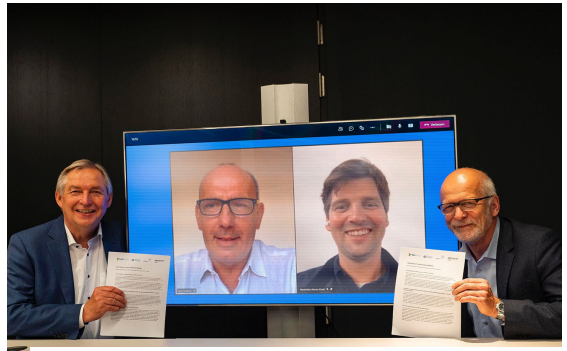
[Collaboration with Alastria] towards EBSI-compatible no-code approach for storing logs on context / digital twin data transactions on blockchain networks

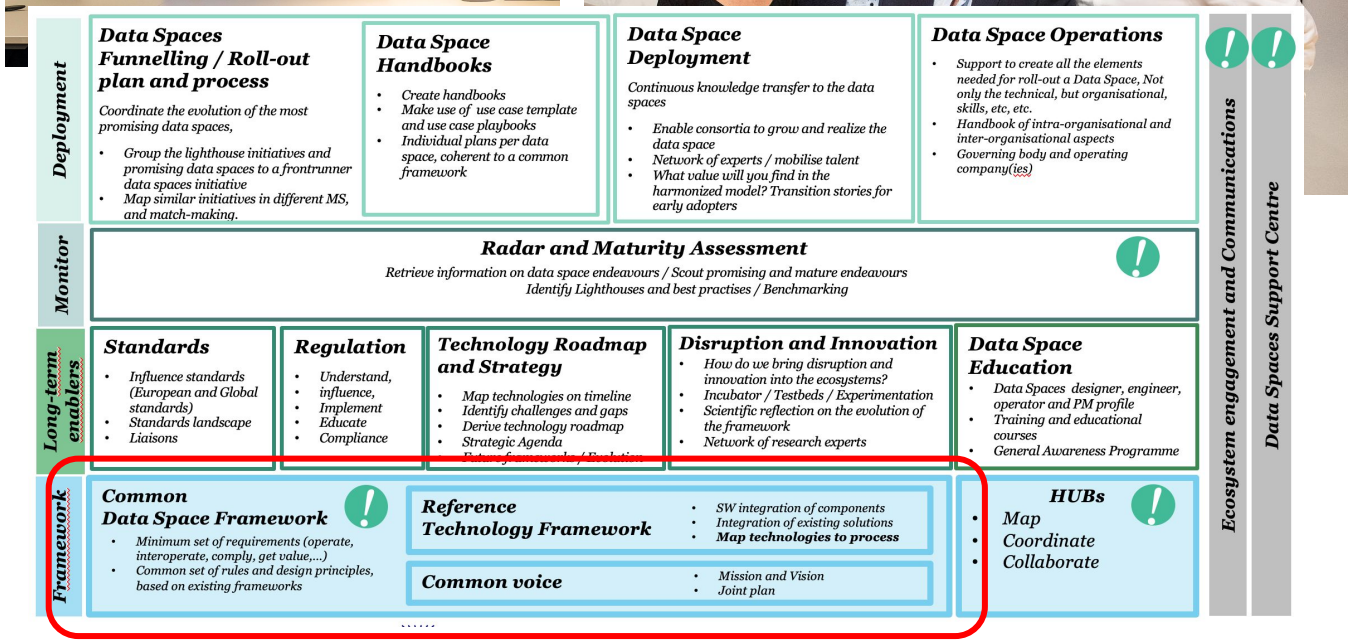
FIWARE

Data Spaces Business Alliance (DSBA): joining forces

BDVA, FIWARE, GAIA-X and IDSA launched the [Data Spaces Business Alliance (DSBA)] to accelerate Business Transformation in the Data Economy (Sep 23rd, 2021)

- **One voice and a common framework** to make **interoperable Data Spaces** happen;
- Together, **the Alliance's founding organisations represent 1,000+ leading key industry players**;
- With its combined **cross-industry expertise, resources and know-how**, the Alliance drives awareness and rely on **more than 100 Hubs** for dissemination
- **Technical Convergence discussions** towards common reference technology framework for creation of Data Spaces:
  - Agile approach based on delivery of subsequent versions of a Minimum Viable Framework (MVF) specification where we do not only identify standards and target components but how to integrate them
  - Once alignment on relevant topics within several of the ongoing workstreams is achieved, the publication of a new version of the DSBA Technology Convergence document will be published to incentivize development of compliant implementations

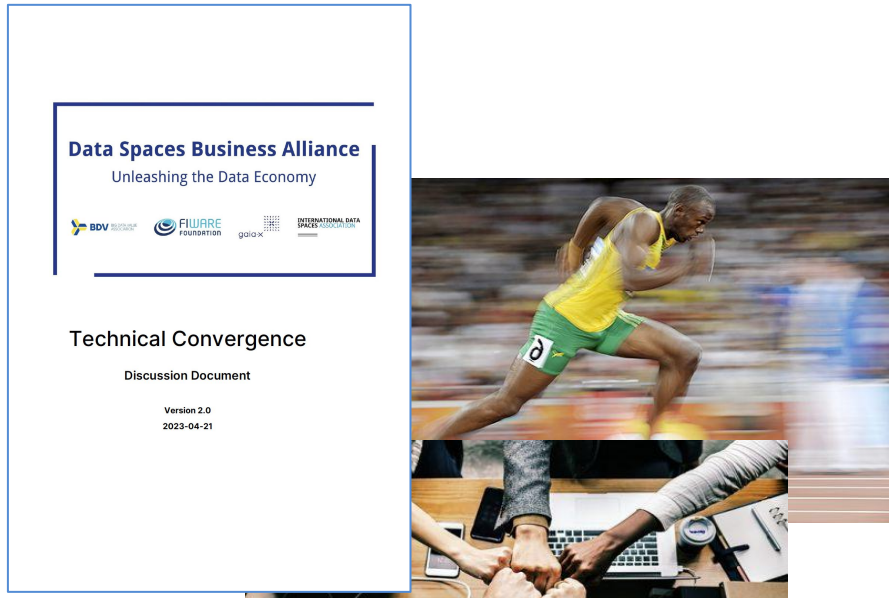




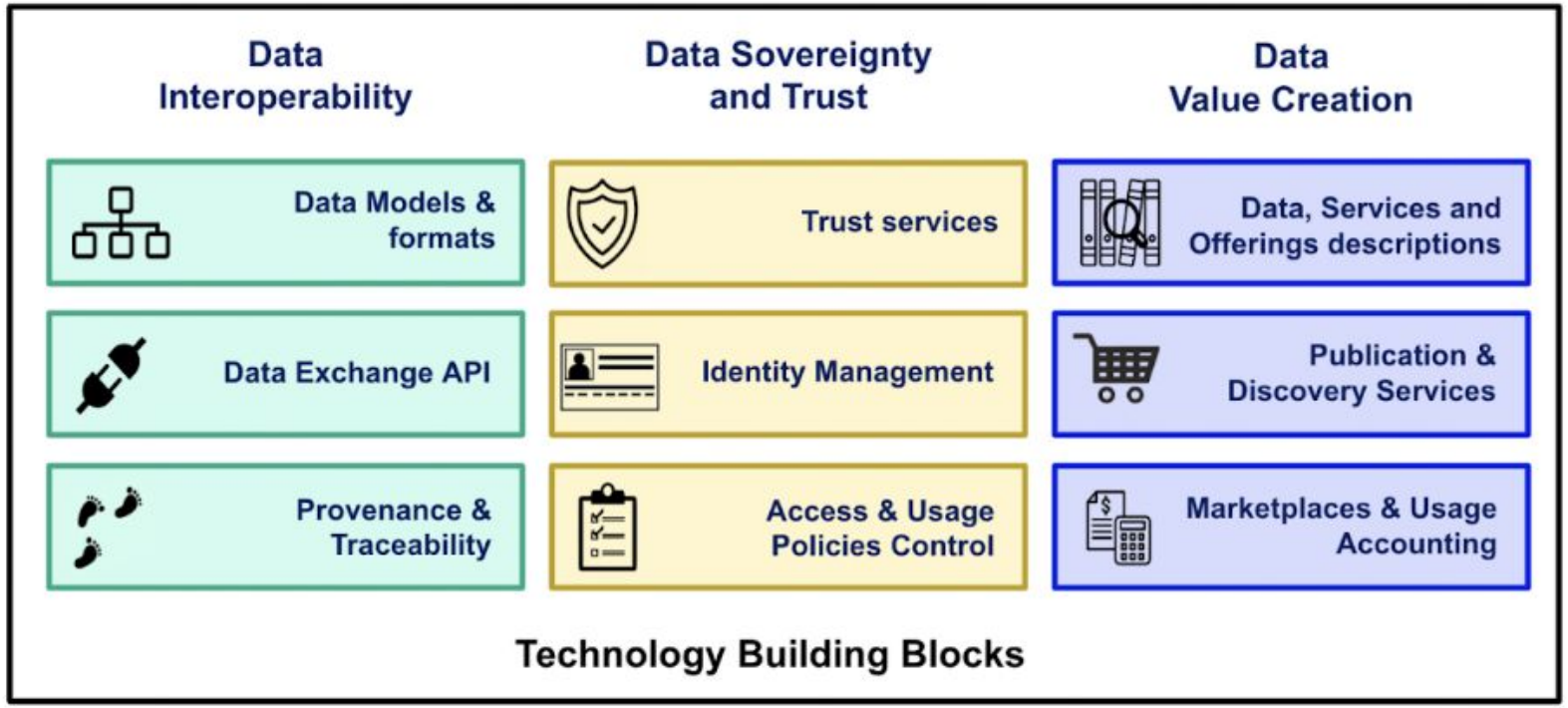
DSBA Technical Convergence version 2.0

- The DSBA Technical Convergence (TC) delivers a Minimum Viable Framework (MVF) enabling the creation of data spaces
- This MVF is based on the convergence of existing architectures and models, leveraging each other's efforts on specifications and implementations.
- A new edition of the DSBA TC (version 2.0) was released on April 21st - Major highlights
  - Description of common vision and conceptual model
  - Identification of major standards per technology pillar and specifications of how they get integrated
- Some initiatives committed to follow DSBA technical recommendations (others welcome to do the same!):
  - FIWARE Data Space Connector
  - iSHARE Trust Framework

  Working to integrate results under i4Trust collaboration program
  - DOME project under Digital Europe Programme



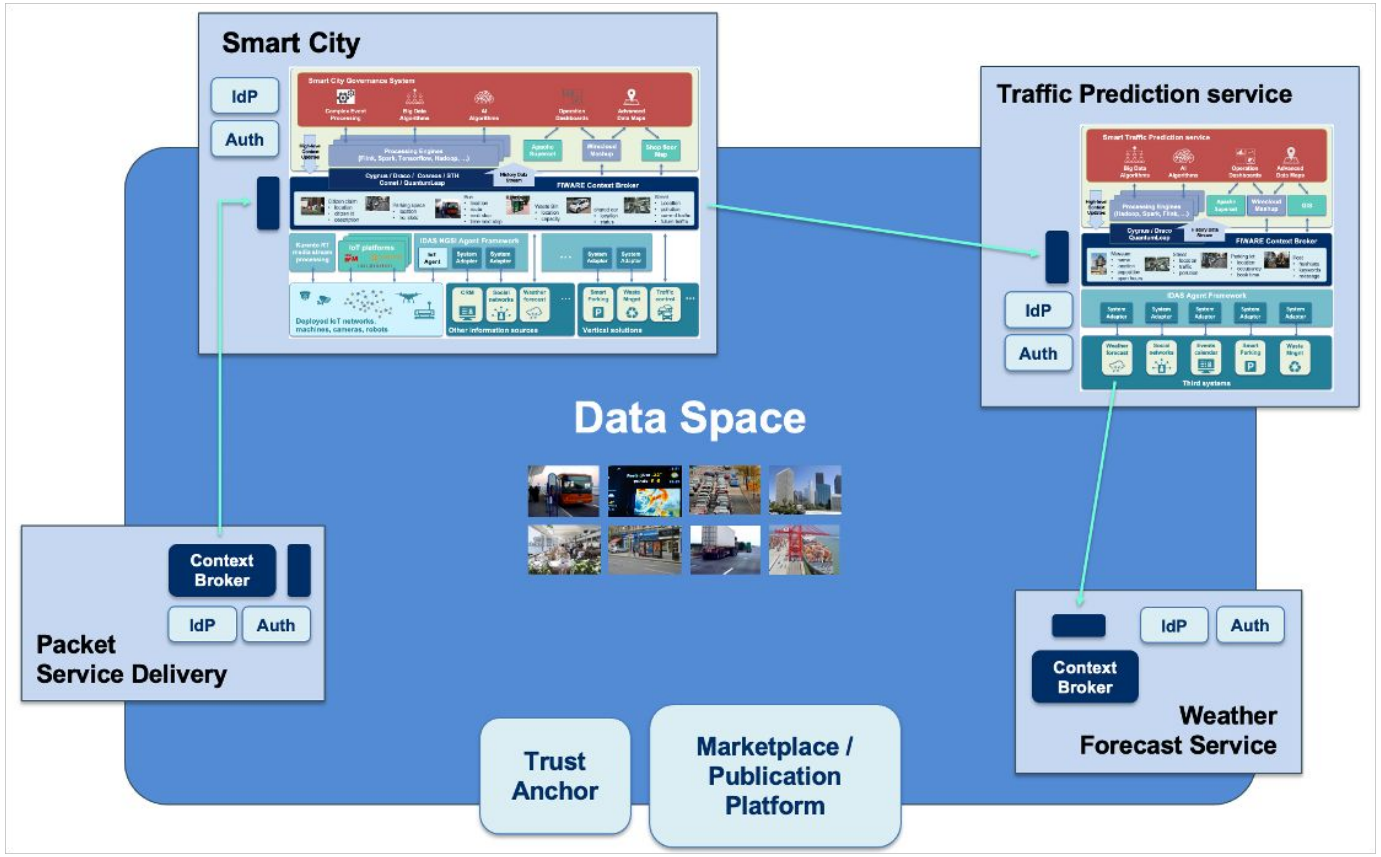
DSBA Technology Convergence: Technical Building Blocks



FIWARE

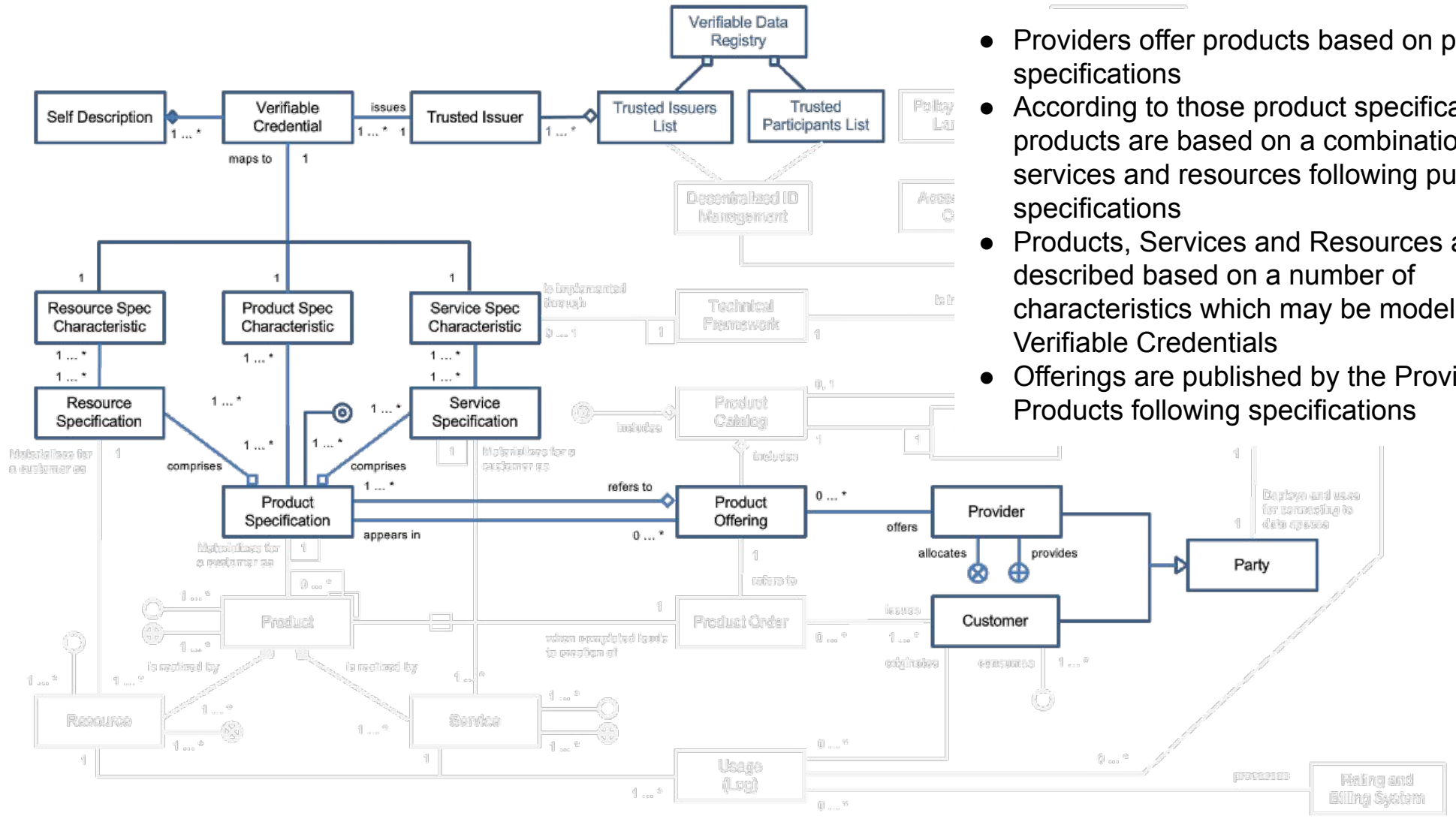
Some key concepts: Verifiable Credentials

- VCs will be used to describe participants in data spaces
- VCs will be used to describe products offered by participants, e.g.:
  - issued by certification agencies, describing compliance with certain regulations (e.g., GDPR compliance) recommendations (e.g., low carbon emissions) or technical compliance (e.g., NGSI-LD compatible interface).
  - provided by the own service provider describing aspects of the service (e.g., access policies, technical standards supported, etc)



FIWARE

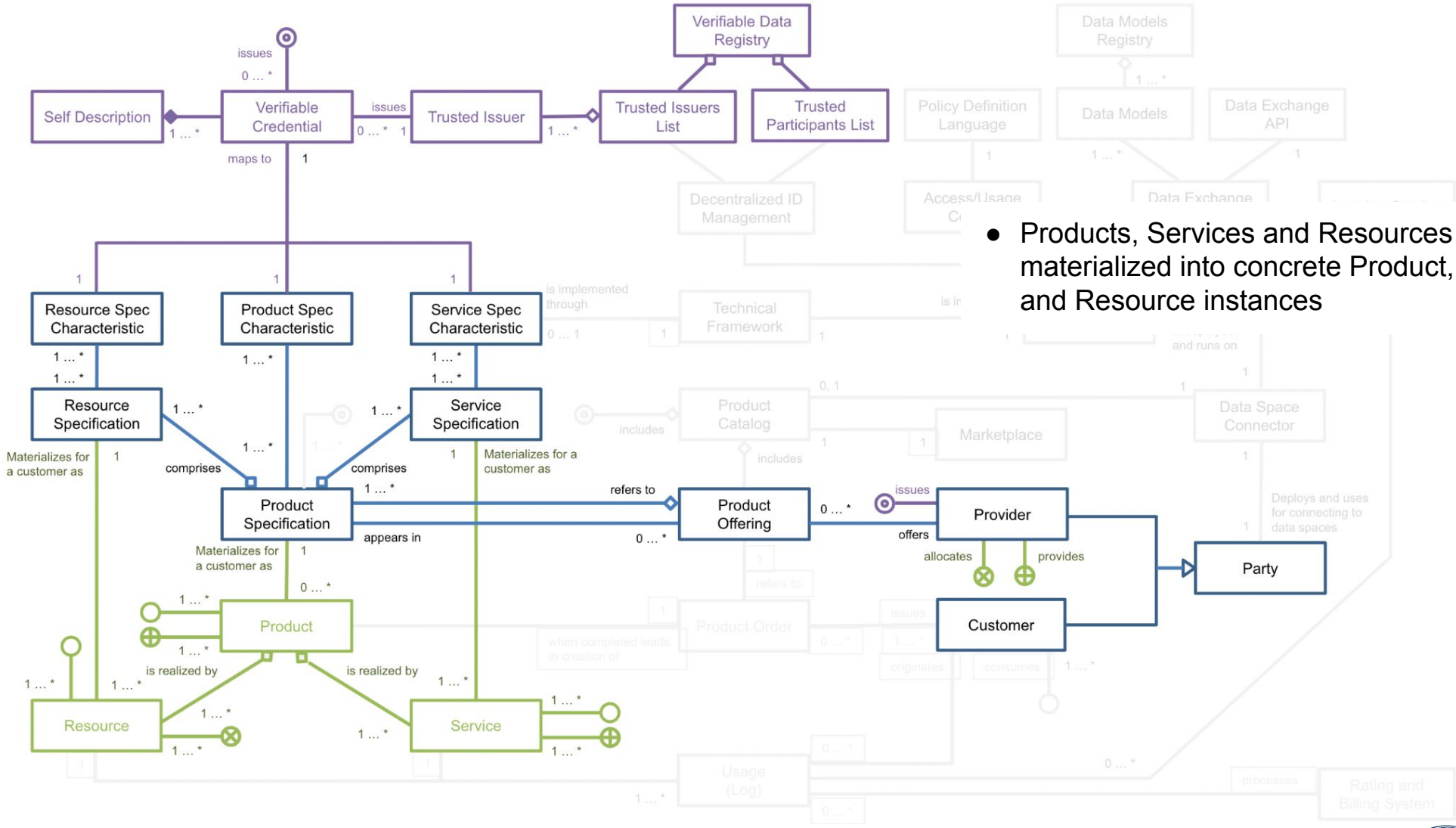
DSBA Technical Convergence: Conceptual Model



- Providers offer products based on published specifications
- According to those product specifications, products are based on a combination of services and resources following published specifications
- Products, Services and Resources are described based on a number of characteristics which may be modeled as Verifiable Credentials
- Offerings are published by the Provider around Products following specifications

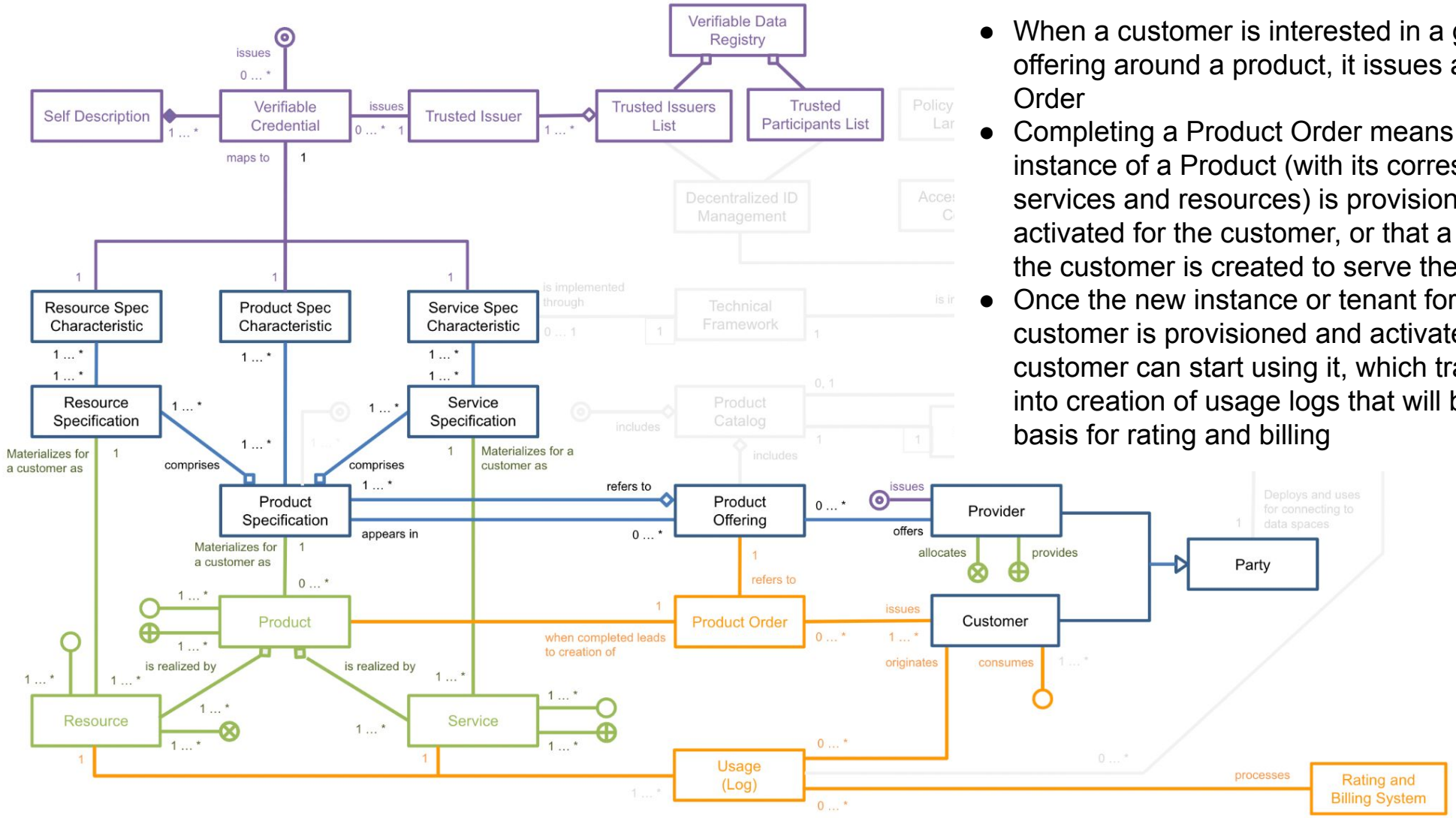
FIWARE

DSBA Technical Convergence: Conceptual Model



- Products, Services and Resources specs get materialized into concrete Product, Service and Resource instances

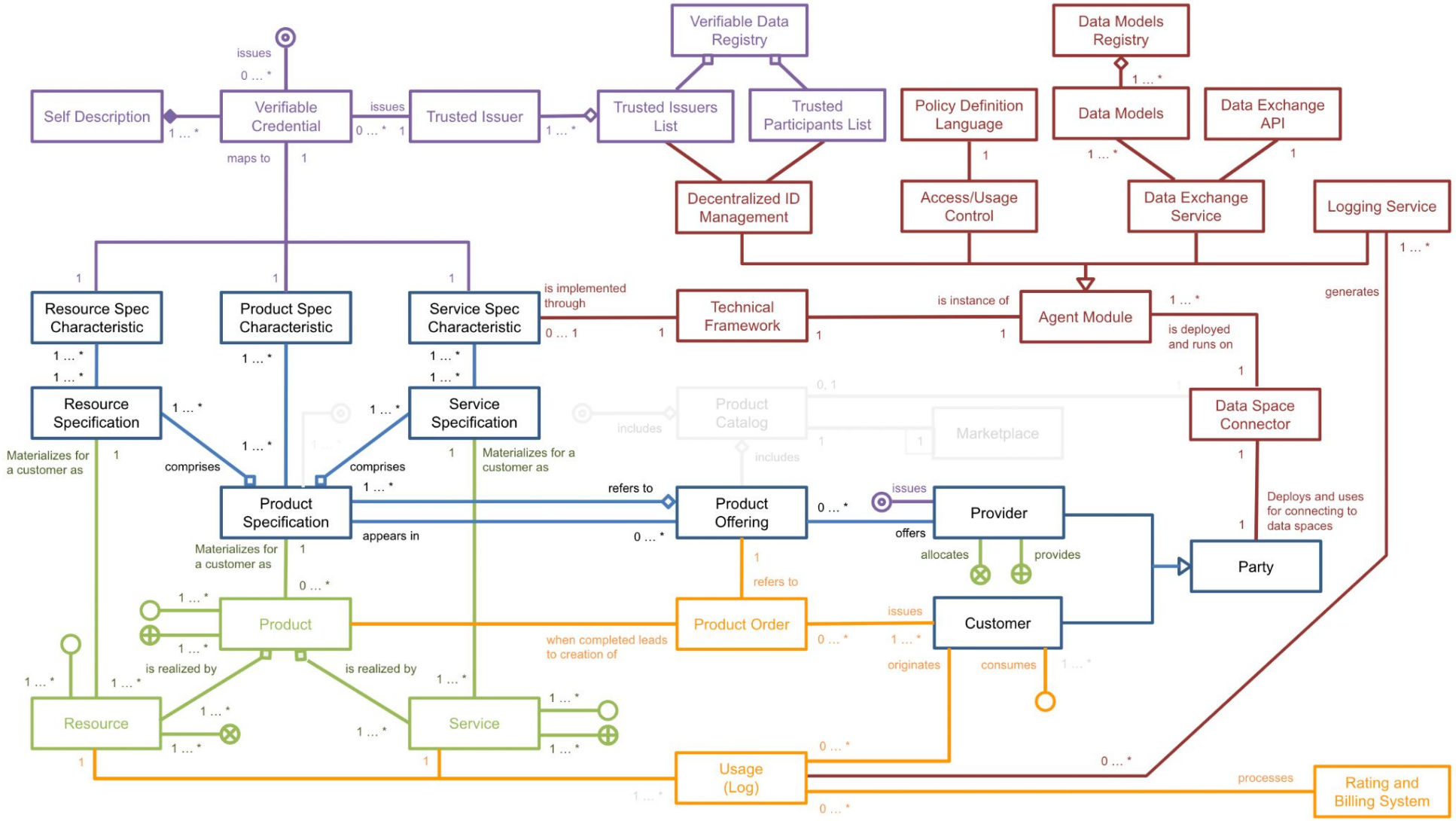
DSBA Technical Convergence: Conceptual Model



- When a customer is interested in a given offering around a product, it issues a Product Order
- Completing a Product Order means that a new instance of a Product (with its corresponding services and resources) is provisioned and activated for the customer, or that a tenant for the customer is created to serve the customer
- Once the new instance or tenant for the customer is provisioned and activated, the customer can start using it, which translates into creation of usage logs that will bring the basis for rating and billing

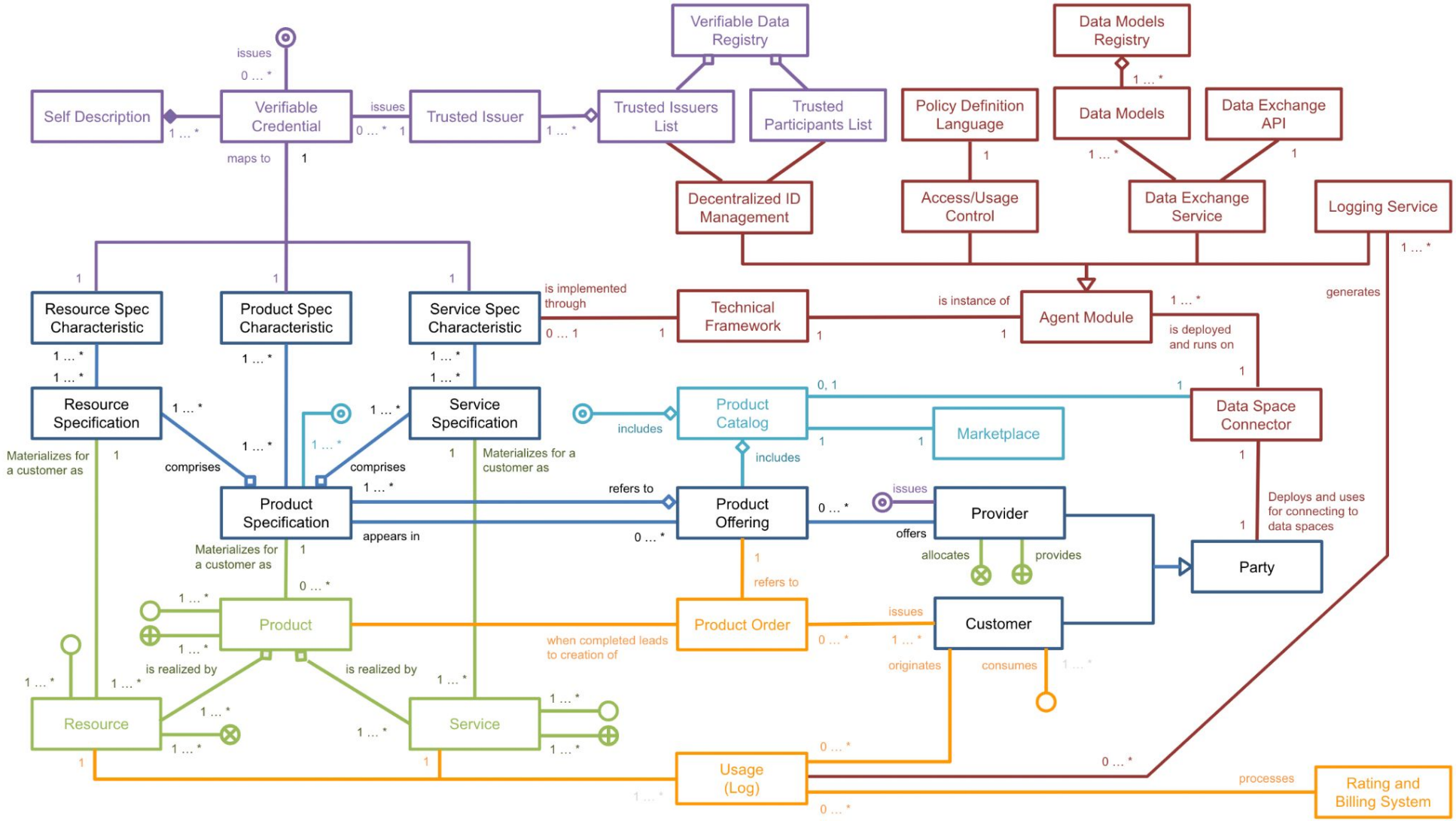
FIWARE

DSBA Technical Convergence: Conceptual Model



FIWARE

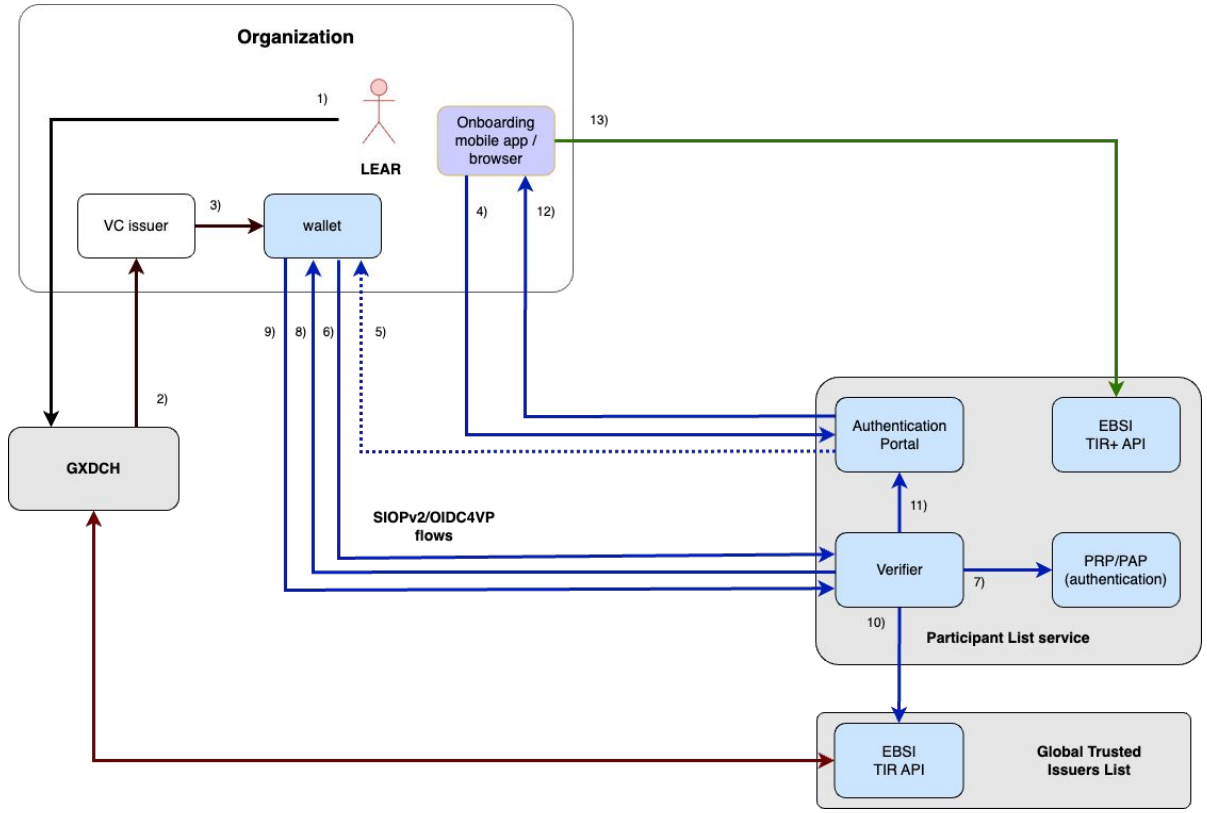
DSBA Technical Convergence: Conceptual Model



FIWARE

Onboarding of an organization in the data space

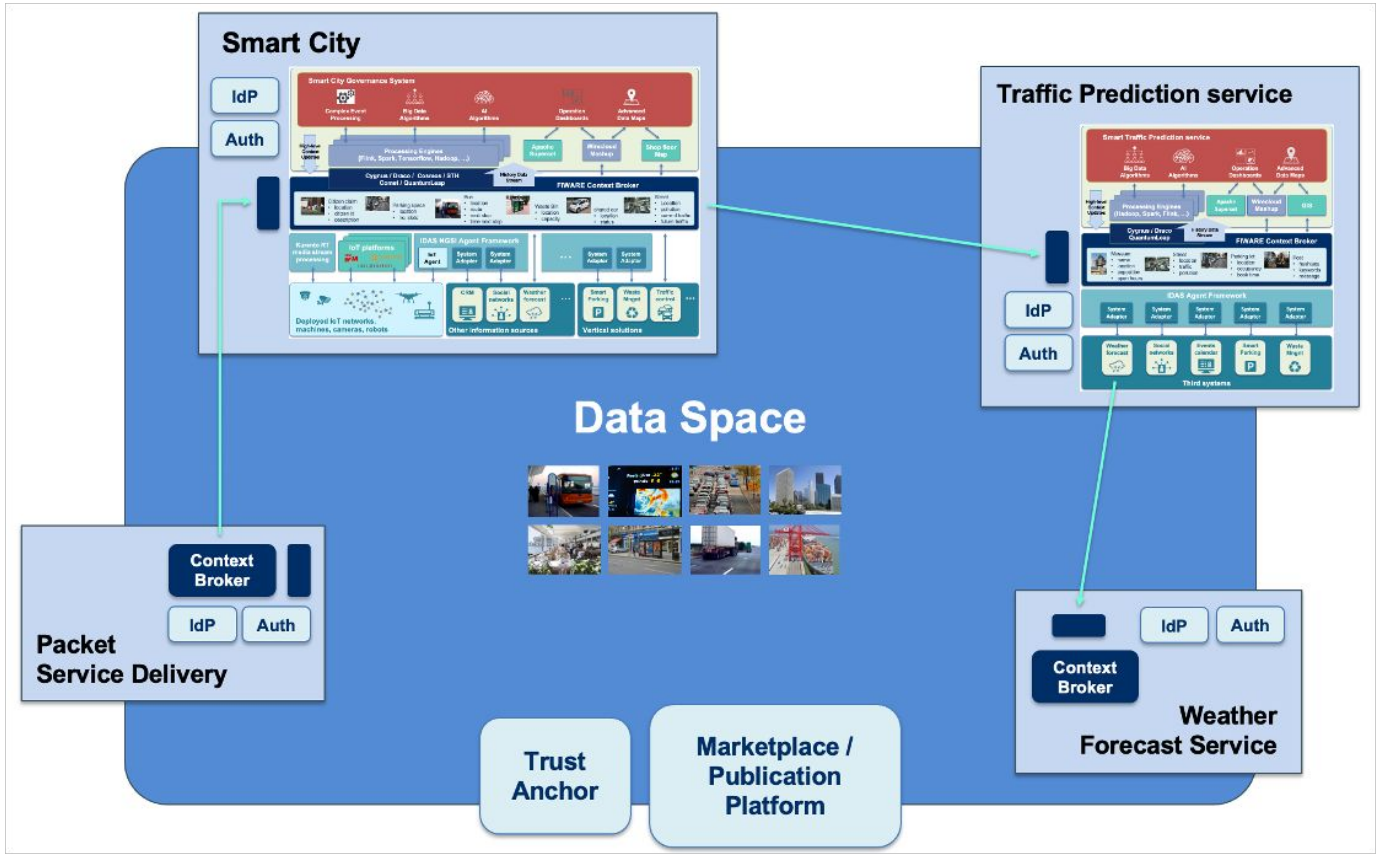
- The organization validates that the VC containing its description as organization is compliant with Gaia-X specifications using the services of a Gaia-X Digital Clearing House (GXDCH) - as a result, a VC is issued by the GXDCH (steps 1-2). That VC will end stored in the wallet of the LEAR either as part of the same process (once the GXDCH implements the OIDC4VCI) or via an issuer of VCs that exists inside the organization (step 3)
- The API for registering the organization is inspired in the TIR API defined by EBSI but extending it to allow:
  - creation, update and deletion of entries beyond read(ing) of entries
  - authentication with VCs (including the VC issued by a GXDCH)
- Using an onboarding application (or a web portal) the organization's LEAR requests the authentication into the Participant Lists service which ultimately translates into a request to the Verifier (step 4-6)
  - a page is accessed where a QR for authentication is displayed (step 4)
  - the QR code is scanned through the wallet (step 5) which translates
  - into a request to the verifier (step 6)
- The verifier checks in the PRP/PAP what VCs it has to request to the wallet (step 7). In principle it will find the following VCs to be requested: a) the LEAR VC accrediting the user as LEAR of the organization, b) the VC containing the description of the organization, and c) the VC issued by some GXDCH acredditing that the previous VC is Gaia-X compliant
- The verifier responds to the previous request sending a VP request to the wallet which responds with the requested VCs (steps 8-9)
- The verifier checks that the LEAR VC has been signed using proper eIDAS certificates and that the GXDCH VC has been issued by a trusted GXDCH (step 10). It finally produces an access token (steps 11-12) which the onboarding application can then use to invoke the EBSI TIR+ API in order to register the organization as data space participant (step 13)



FIWARE

What it means acquiring rights to use a product/service?

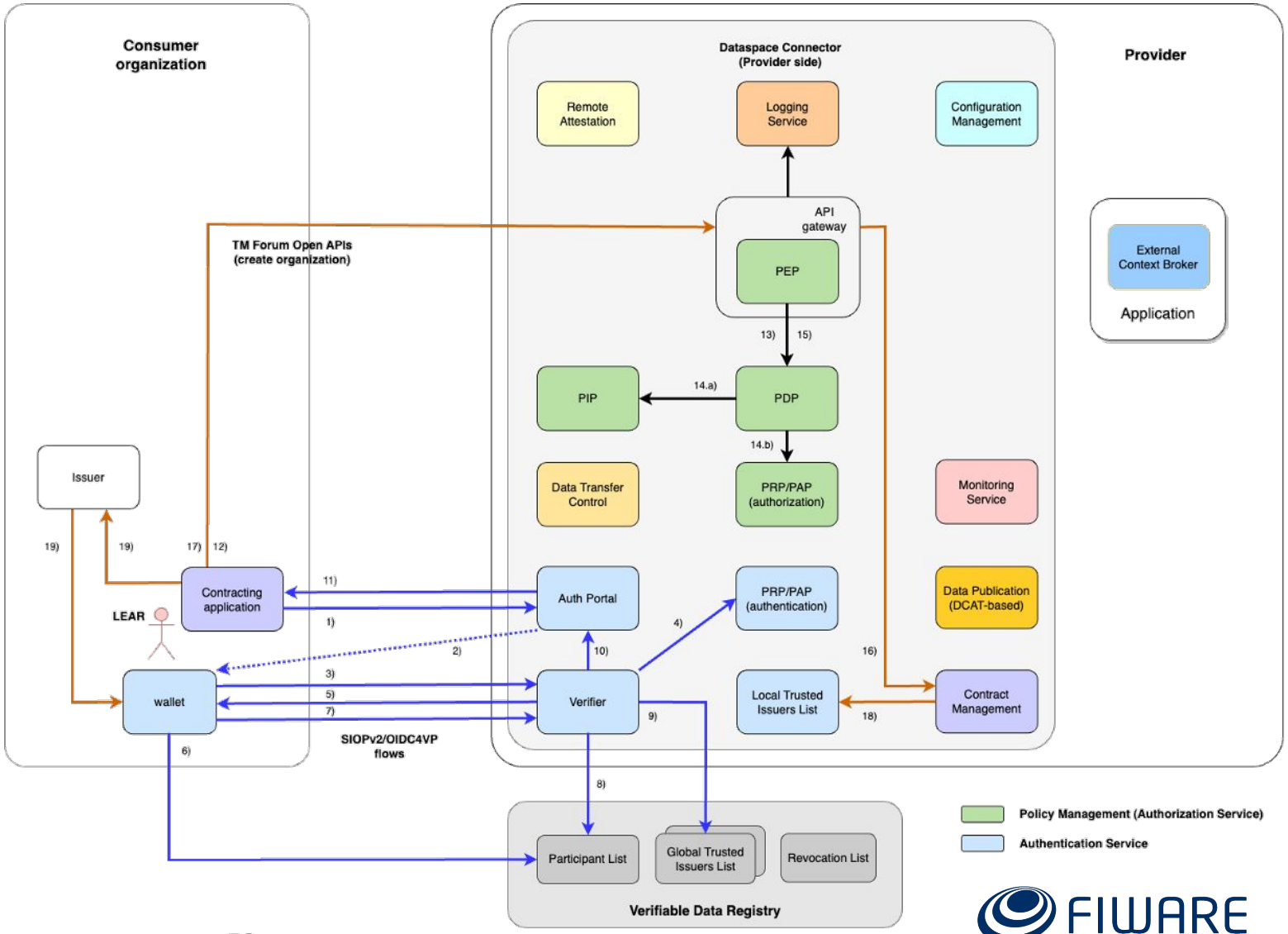
- Organizations that acquire rights to use a product (data service):
  - become trusted issuers of VC including claims relevant for data service access
  - They can issue such VCs for users within the organization
- Organizations willing to access services or resources of a product have to first go through authentication to gain an access token when:
  - it will be verified whether the organization is a trusted participant (Trust service)
  - it will be verified whether the organization is a trusted issuer of the VCs defined around claims that are meaningful for business logic of the product → access rights were properly acquired (e.g., via some marketplace or directly via the connector managing access to the product)
- Authorization based on Attribute Based Access Control (ABAC) will be performed on any request by verifying that users with the VCs traveling in the access token sent with the request can perform the request based on defined policies



FIWARE

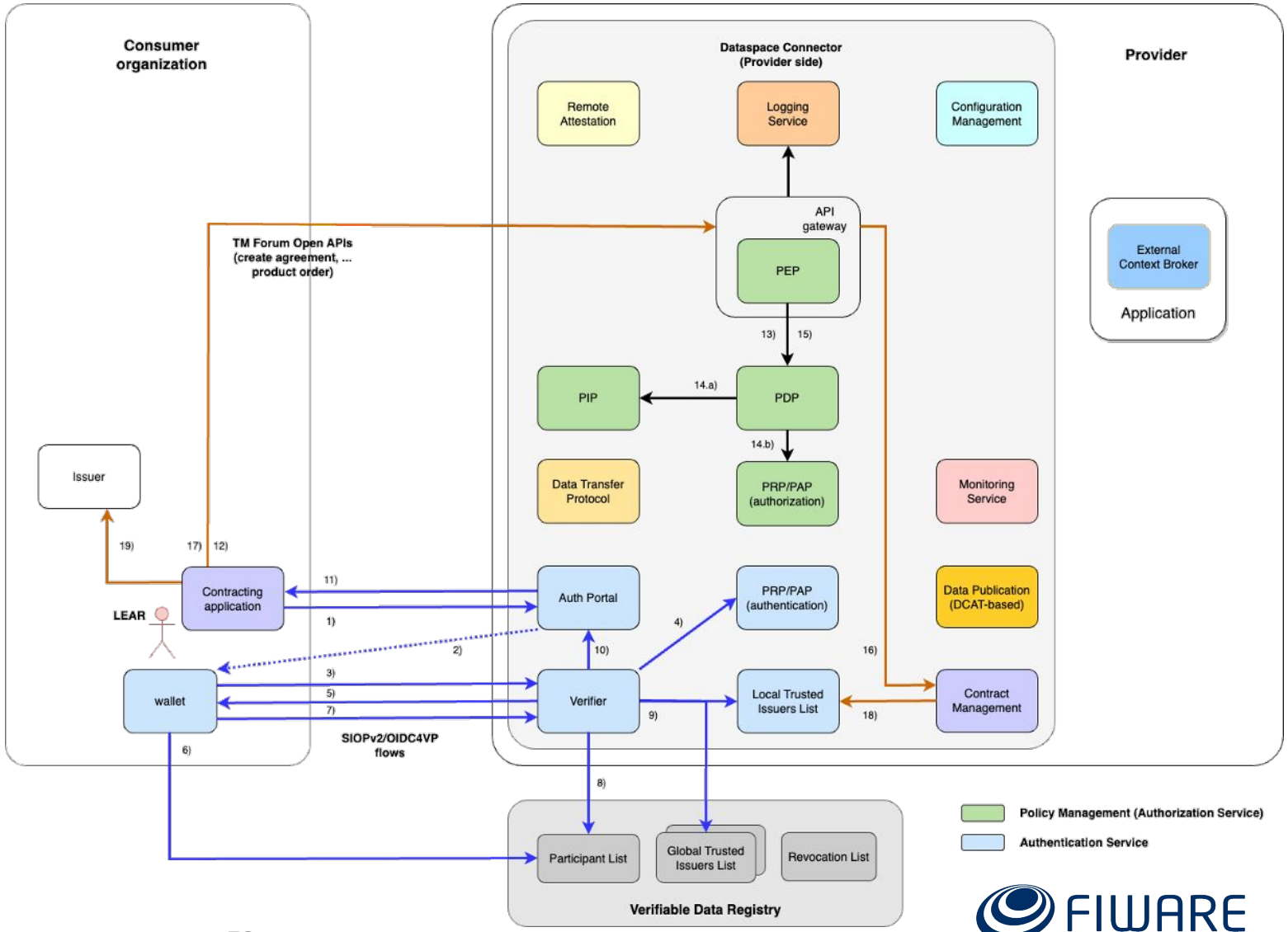
Consumer registration at Connector Level using TM Forum APIs

- Using a contracting app (or a web portal), a LEAR of the consumer organization will request authentication into the connector of the service provider (steps 1-3 involving scanning of QR code using the wallet)
- The Verifier will request from the user's wallet a VC that acredits him/her as LEAR of the organization, eventually other VCs (steps 4-5). The wallet will check whether the verifier belongs to a participant in the data space (step 6) and return the requested VCs (step 7)
- The Verifier checks whether the LEAR's VC was issued by a trusted participant of the data space (step 8), and also checks whether other VCs required were issued by trusted issuers (step 9)
- If verifications were ok, it issues a token (step 10) that is transmitted to the user (step 11)
- Using the returned token, the user invokes TM Forum API to register the consumer organization at the Connector (steps 12-17) establishing the necessary access control (steps 12-14)
- Once the organization is registered and fulfills all the necessary information (which may take some time), the organization is registered in the local trusted issuers list as trusted issuer of VCs which include claims as buyer of products in the connector (step 18)



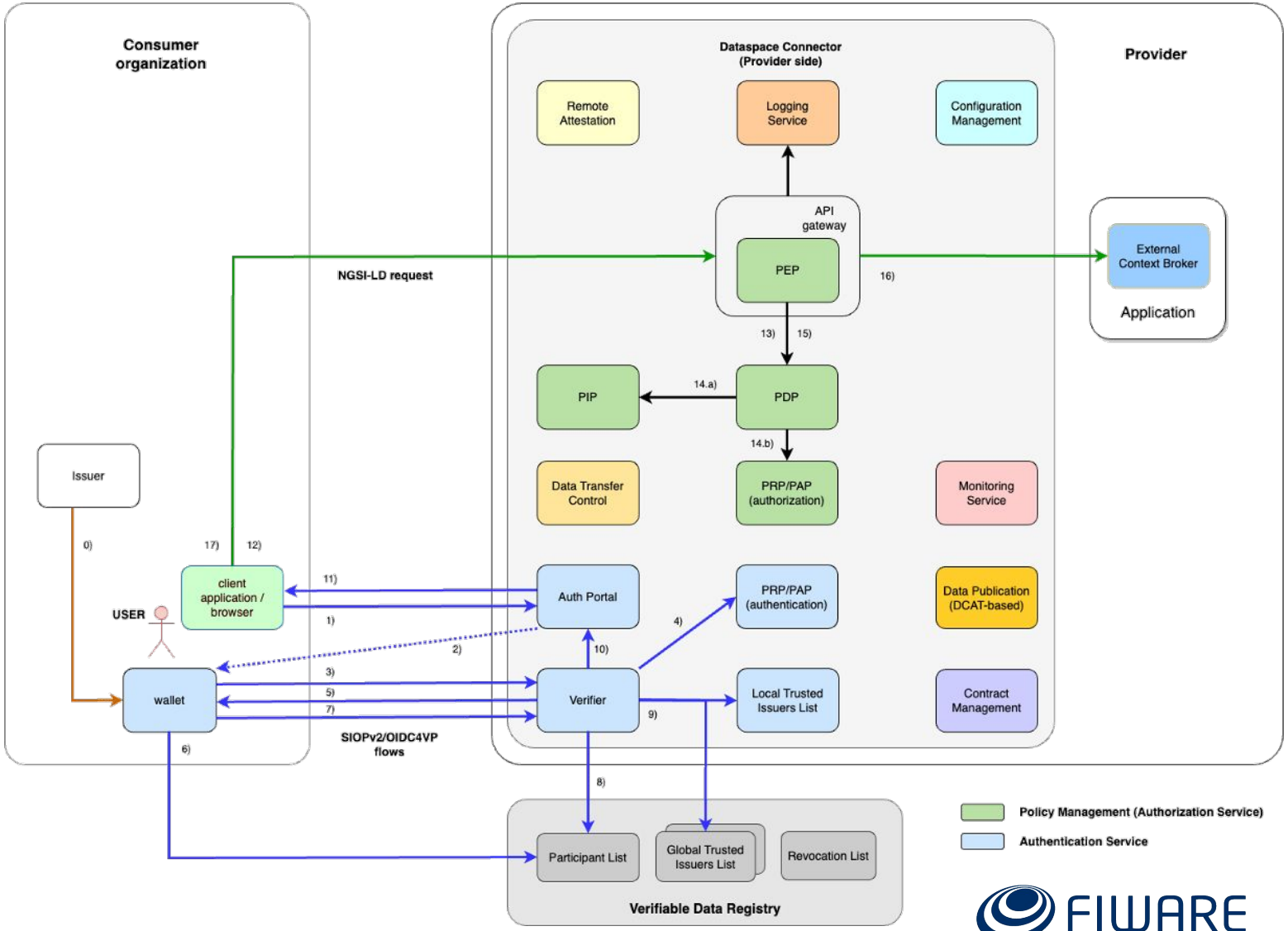
Contract Management at Connector Level using TM Forum APIs

- A LEAR of the consumer organization will start authentication into the contract negotiation module of the connector of a service provider (steps 1-3 involving scanning of QR code using the wallet)
- The Verifier will request to the user (via his/her wallet) for VCs that acredit a) the user is a LEAR of the organization, b) (s)he owns credentials connected to roles meaningful for contract negotiation that the organization issued to the user and c) some other VCs (steps 4-5). The wallet will check that the verifier belongs to a participant in the data space (step 6) and return the requested VCs (step 7)
- The Verifier checks whether the LEAR's VC was issued by a trusted participant of the data space (step 8), and rest of VCs required were issued by trusted issuers (step 9). Note that the VC for accessing contract negotiation functions requires that the organization were previously registered in the contract negotiation module, otherwise it will not be found in local trusted issuers registry
- If verifications were ok, it issues a token (step 10) that is transmitted to the user (step 11)
- Using the returned token, the user invokes TM Forum API to perform operations on the contract negotiation module (steps 12-17) establishing the necessary access control (steps 12-14)
- Once the organization is registered and fulfills all the necessary information (which may take some time), the organization is registered as trusted issuer of VCs which include claims as valid user of products accessible via the connector (step 18)



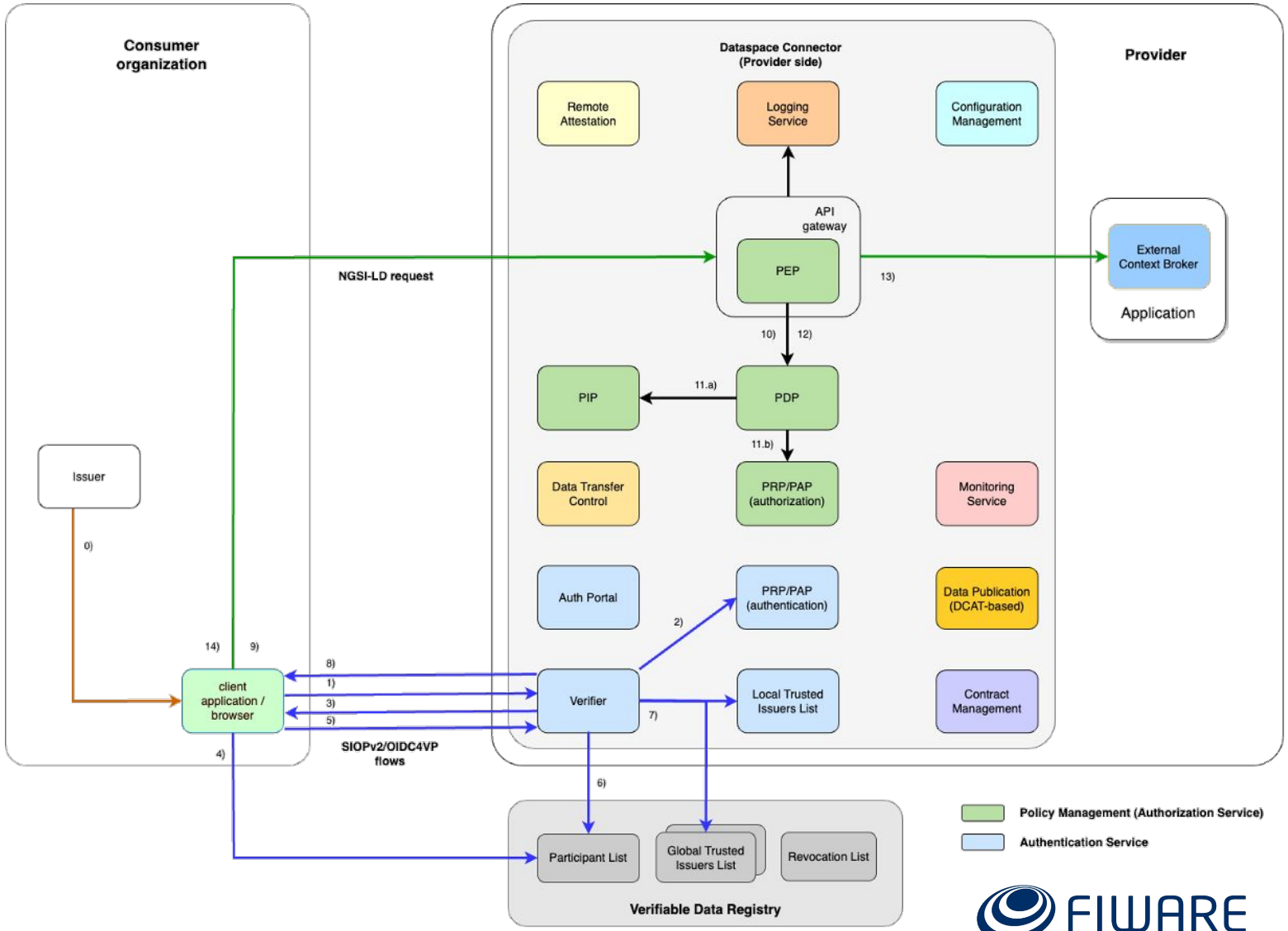
Interaction once procurement has been completed (user involved)

- A user of the product (employee or customer of the consumer oganization that was issued a VC in step 0 that acredits him/her as user playing a role relevant to the business logic of the product) request authentication in the connector (steps 1-3 involving scanning of QR code using the wallet)
- The Verifier will request to the user (via his/her wallet) for VCs that acredit a) the user owns credentials connected to roles meaningful for the given product/application and b) some other VCs (steps 4-5). The wallet will check that the verifier belongs to a participant in the data space (step 6) and return the requested VCs (step 7)
- Verifier verifies whether the VC was issued by an organization that a) is a trusted participant of the data space (step 8) and b) is a trusted issuer of the VCs meaningful for the application (that is, VCs only organizations that ordered the product can issue), also checks whether other VCs required were issued by trusted issuers (steps 9)
- If verifications were ok, it issues a token (step 10) that is transmitted to the user (step 11)
- Using the returned token, the user invokes services of the product (step 12)
- The PEP proxy will verify whether a user with the claims (attributes) included in the VCs extracted from the token is authorized to perform the given request (steps 13-15)
- If authorization is ok, the request is forwarded (step 16) and a response returned to the user (step 17)

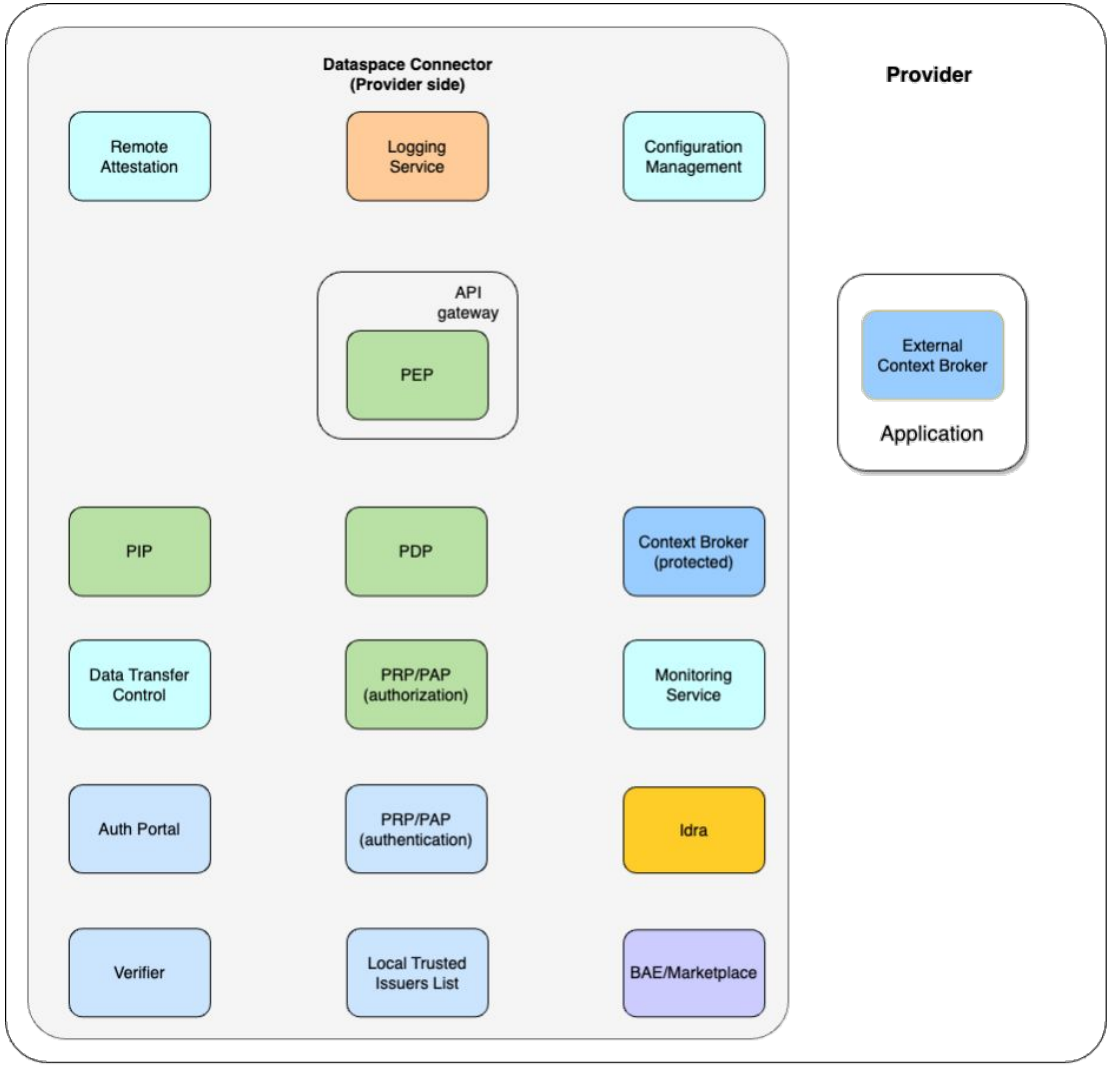


Interaction once procurement has been completed (M2M)

- An application from the consumer organization that acquired rights to use a product requests its authentication in the connector (steps 1)
- The Verifier will request to the application for VCs that acredit a) the application owns credentials connected to roles meaningful for the given product/application and b) some other VCs (steps 2-3). The wallet will check that the verifier belongs to a participant in the data space (step 4) and returns the requested VCs (step 5)
- Verifier verifies whether the VC was issued by an organization that is a trusted participant of the data space (step 6) and is a trusted issuer of the VCs meaningful for the application (that is, VCs that only organizations that ordered the product can issue), also checks whether other VCs required were issued by trusted issuers (steps 7)
- If verifications were ok, it issues a token that is transmitted to the application (steps 8)
- Using the returned token, the application invokes services of the product (step 9)
- The PEP proxy will verify whether the application with the claims (attributes) included in the VCs extracted from the token is authorized to perform the given request (steps 10-12)
- If authorization is ok, the request is forwarded (step 13) and a response returned to the app (step 14)



DSBA-compliant FIWARE Data Space Connector



FIWARE