DOME - A **D**istributed **O**pen **M**arketplace for **E**urope Cloud and Edge Services

DOME Architecture and functionalities

Jesus Ruiz

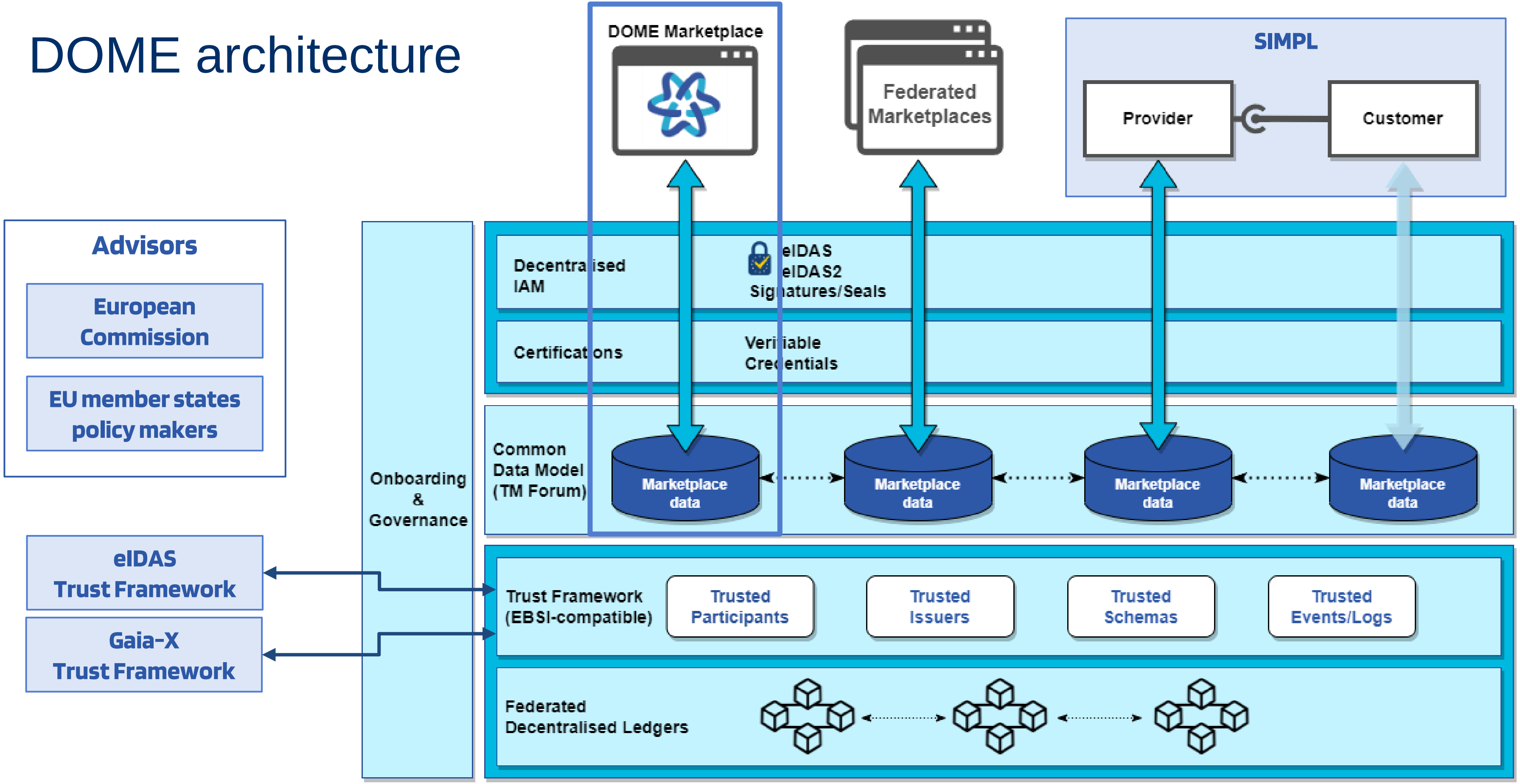
DOME Technical coordinator

June 2024

Co-funded by the
European Union

DOME architecture overview

DOME architecture



DOME Marketplace

Federated Marketplaces

SIMPL

Provider

Customer

Advisors

European Commission

EU member states policy makers

eIDAS Trust Framework

Gaia-X Trust Framework

Onboarding & Governance

Decentralised IAM

eIDAS
eIDAS2
Signatures/Seals

Certifications

Verifiable Credentials

Common Data Model (TM Forum)

Marketplace data

Marketplace data

Marketplace data

Marketplace data

Trust Framework (EBSI-compatible)

Trusted Participants

Trusted Issuers

Trusted Schemas

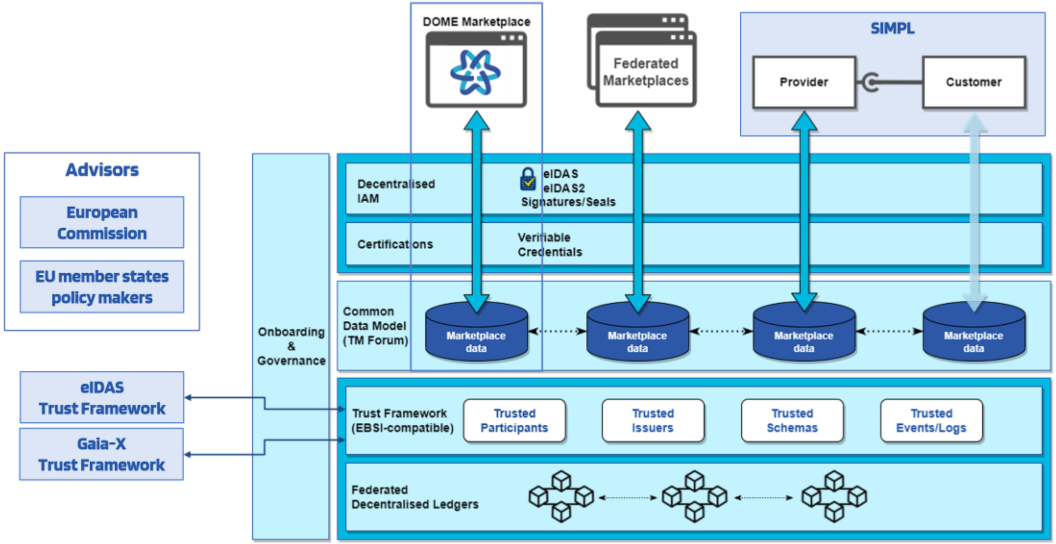
Trusted Events/Logs

Federated Decentralised Ledgers

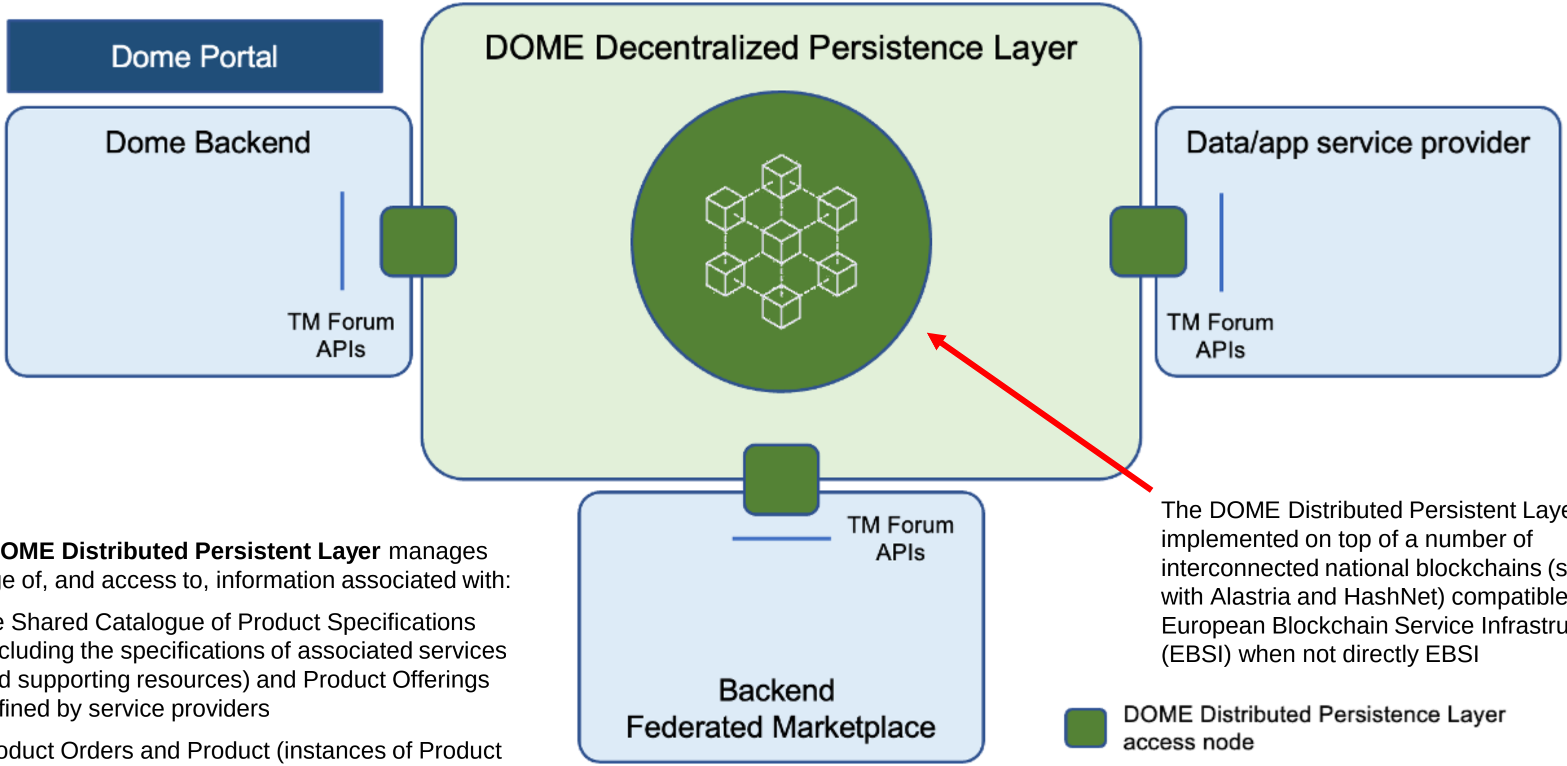
Overview

- DOME will take the form of a **federated marketplace of curated cloud and edge services made available through**:
  - the **global DOME portal**; and
  - **federated marketplaces**

- A federated marketplace can be**:**
  - **Independent Marketplace**, which comprises a catalogue of cloud and edge data/app services not tied to an IaaS or Platform provider
  - **Marketplace connected to an IaaS provider**, which comprises a catalogue of cloud and edge data/app services which customers can pick and then easily deploy on top of the provided infrastructure
  - **Marketplace connected to a Platform provider** which comprises a catalogue of cloud and edge data/app services which customers can pick, easily activate and run integrated with the rest of data/app services already running, integrated with the provided Platform.



Marketplaces federation + Shared Catalogue


Dome Portal
Dome Backend
TM Forum APIs
DOME Decentralized Persistence Layer
Data/app service provider
TM Forum APIs
TM Forum APIs
Backend Federated Marketplace

The DOME Distributed Persistent Layer will be implemented on top of a number of interconnected national blockchains (starting with Alastria and HashNet) compatible with the European Blockchain Service Infrastructure (EBSI) when not directly EBSI

🟩 DOME Distributed Persistence Layer access node

The **DOME Distributed 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

Strategic allignment

The approach is fully aligned with the Digital Europe Program initiative and its Building Blocks.

eDelivery

Exchange electronic data and documents in an interoperable and secure way

eSignature

Create and verify electronic, paperless signatures

eID

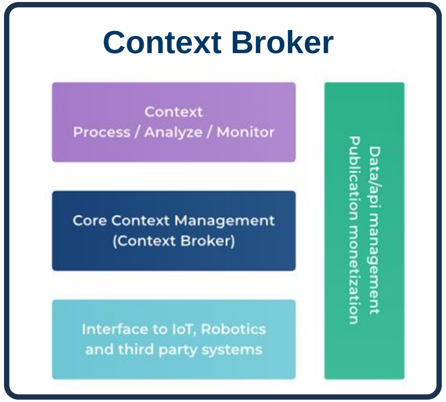
Offer services capable of electronically identifying users from all across Europe

Once-Only Technical System (OOTS)

Reduce administrative burden on citizens and businesses

eInvoicing

Send and receive electronic invoices in line with the European Directive



Context Broker

DOME Distinctive features

- Aligned with Building a European Cloud Marketplace c(Capgemini Invent for the EC).
- Federation and Decentralisation relying on open standards:
  - Description of services in machine-readable verifiable format (Verifiable Credentials)
  - Shared Catalogue and Marketplace functions based on widely adopted TM Forum data model and APIs
  - Decentralized Identity and Access Management aligned with eIDAS2 and the EU Digital Identity Wallet
  - Trust Framework with EBSI-compliant APIs, interoperable with the Gaia-X Trust Framework. Based on a federation of EU clockchain networks.
  - Tamper-evident logs and auditing records for relevant events in the lifecycle of cloud application service offerings.
  - Data services visible through existing Data Publication Platforms supporting DCAT/DCAT-AP
- Vision integrated in first results of Technology Converge discussions under the umbrella of the Data Spaces Business Alliance (DSBA) created by BDVA, FIWARE Foundation, Gaia-X, IDSA

Building a European Cloud Marketplace

– Conceptualisation Study –

August 2021

Capgemini invent

STANDARDS

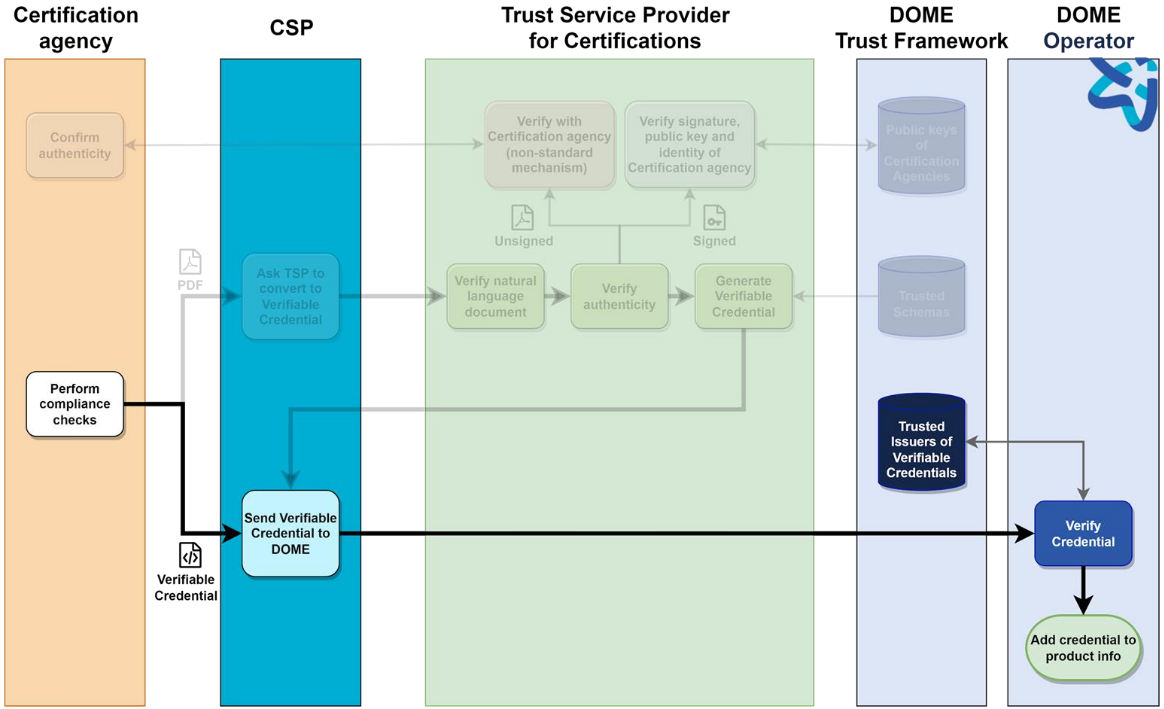
Data Spaces Business Alliance

Unleashing the Data Economy

Certifications and Verifiable Credentials

Implementing Verifiable Certifications for products and services

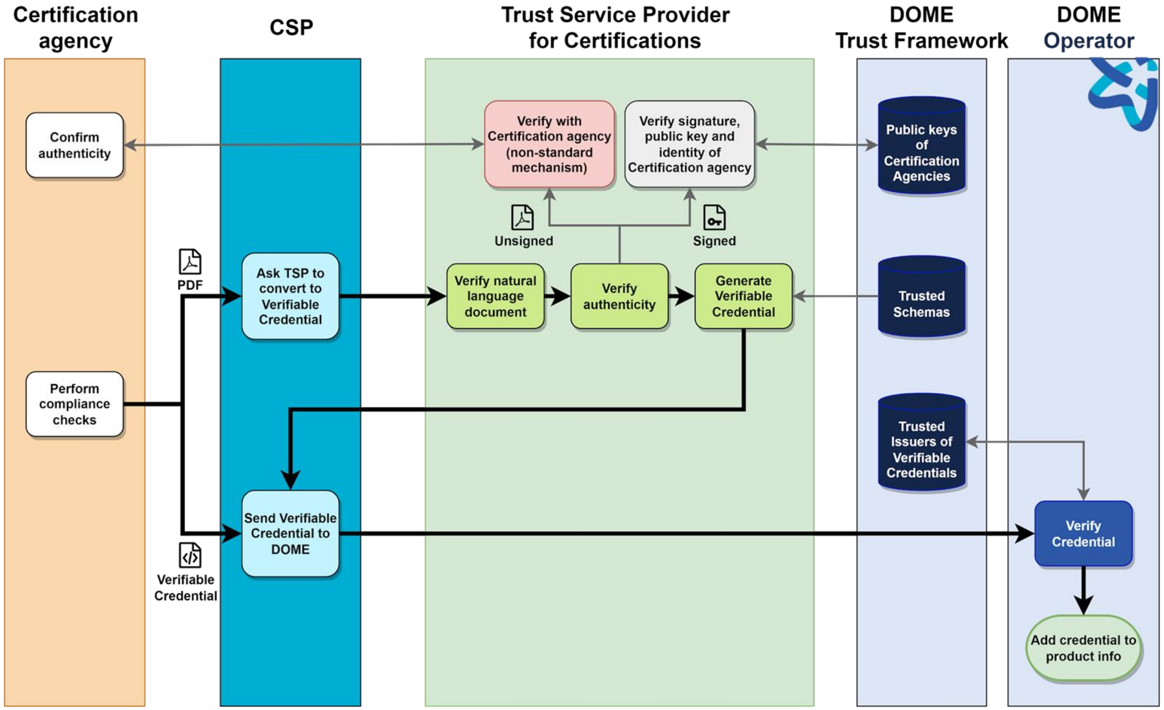
Future: the Certification agency issues a Verifiable Credential


Certification agency
CSP
Trust Service Provider for Certifications
DOME Trust Framework
DOME Operator
Confirm authenticity
Verify with Certification agency (non-standard mechanism)
Verify signature, public key and identity of Certification agency
Public keys of Certification Agencies
Unsigned
Signed
PDF
Ask TSP to convert to Verifiable Credential
Verify natural language document
Verify authenticity
Generate Verifiable Credential
Trusted Schemas
Perform compliance checks
Trusted Issuers of Verifiable Credentials
Send Verifiable Credential to DOME
Verify Credential
Verifiable Credential
Add credential to product info

The flow is very simple:

- The CSP receives the certification in its enterprise wallet.
- The CSP sends the certification to DOME onboarding.
- DOME verifies automatically the authenticity of certification and that it is one of the required certifications.
- Identities of certifications agencies are in the Trust Framework

Today: services to “convert” PDF to Verifiable Credential



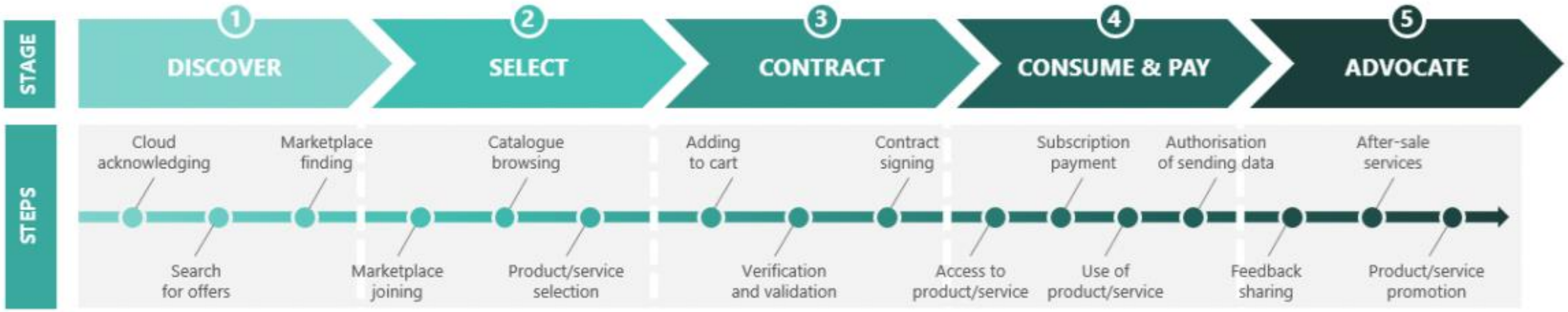
Certification agency
CSP
Trust Service Provider for Certifications
DOME Trust Framework
DOME Operator
Confirm authenticity
Verify with Certification agency (non-standard mechanism)
Verify signature, public key and identity of Certification agency
Public keys of Certification Agencies
Unsigned
Signed
PDF
Ask TSP to convert to Verifiable Credential
Verify natural language document
Verify authenticity
Generate Verifiable Credential
Trusted Schemas
Perform compliance checks
Trusted Issuers of Verifiable Credentials
Send Verifiable Credential to DOME
Verify Credential
Verifiable Credential
Add credential to product info

There is an intermediate trusted service:

- Verifies the content of credential (typically natural language).
- If it is not digitally signed, checks with the certification agency (may be manual or automatic).
- If it is signed, checks signature and that signer is authorised.
- Generates a VC and returns it to CSP.

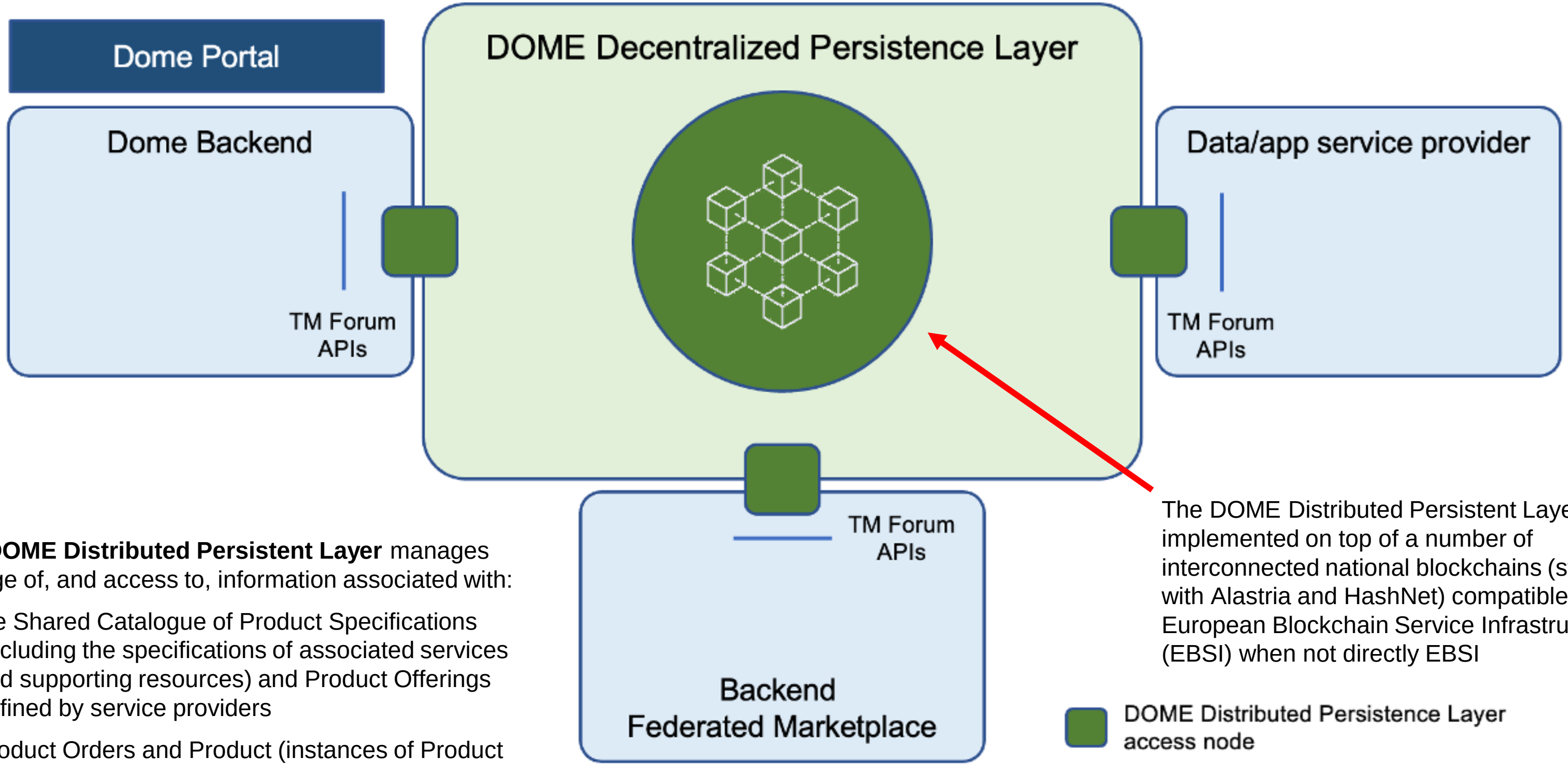
The Trusted Service can be provided by DOME and by other market operators.

Customer journey



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

Marketplaces federation + Shared Catalogue



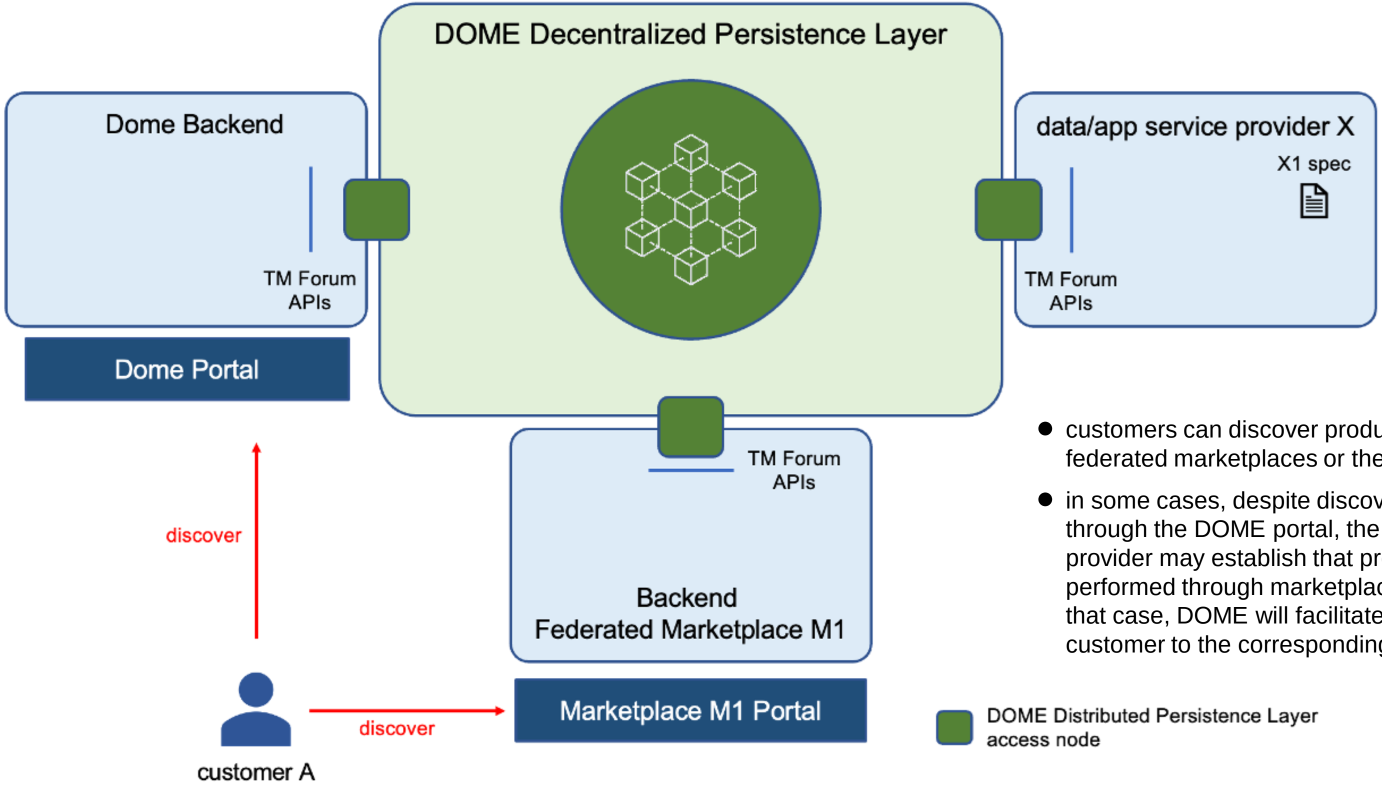
The DOME Distributed Persistent Layer will be implemented on top of a number of interconnected national blockchains (starting with Alastria and HashNet) compatible with the European Blockchain Service Infrastructure (EBSI) when not directly EBSI

🟩 DOME Distributed Persistence Layer access node

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

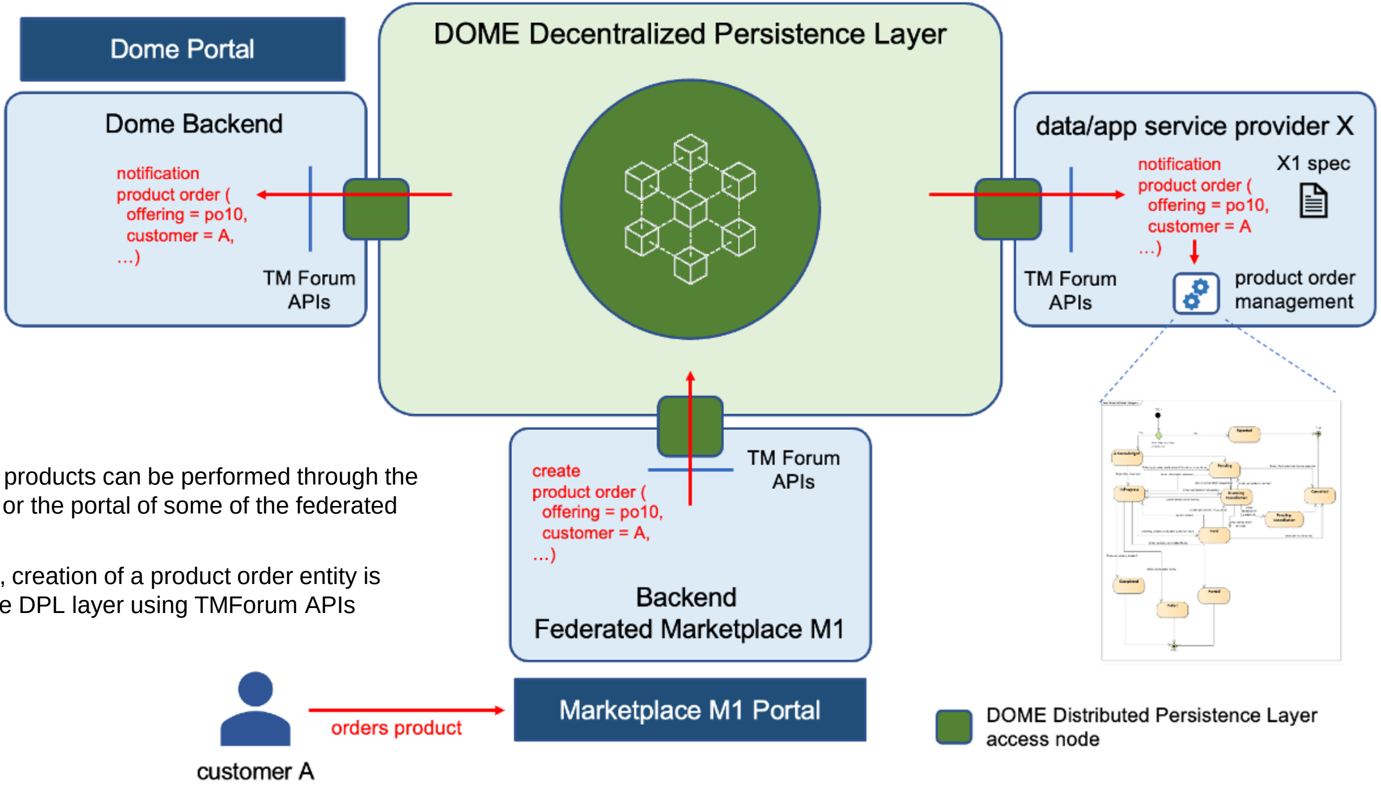
- the Shared Catalogue of Product Specifications (including the specifications of associated services and supporting resources) and Product Offerings defined by service providers
- Product Orders and Product (instances of Product Specifications) along their lifecycle, as well as information about actual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

Product offering discovery



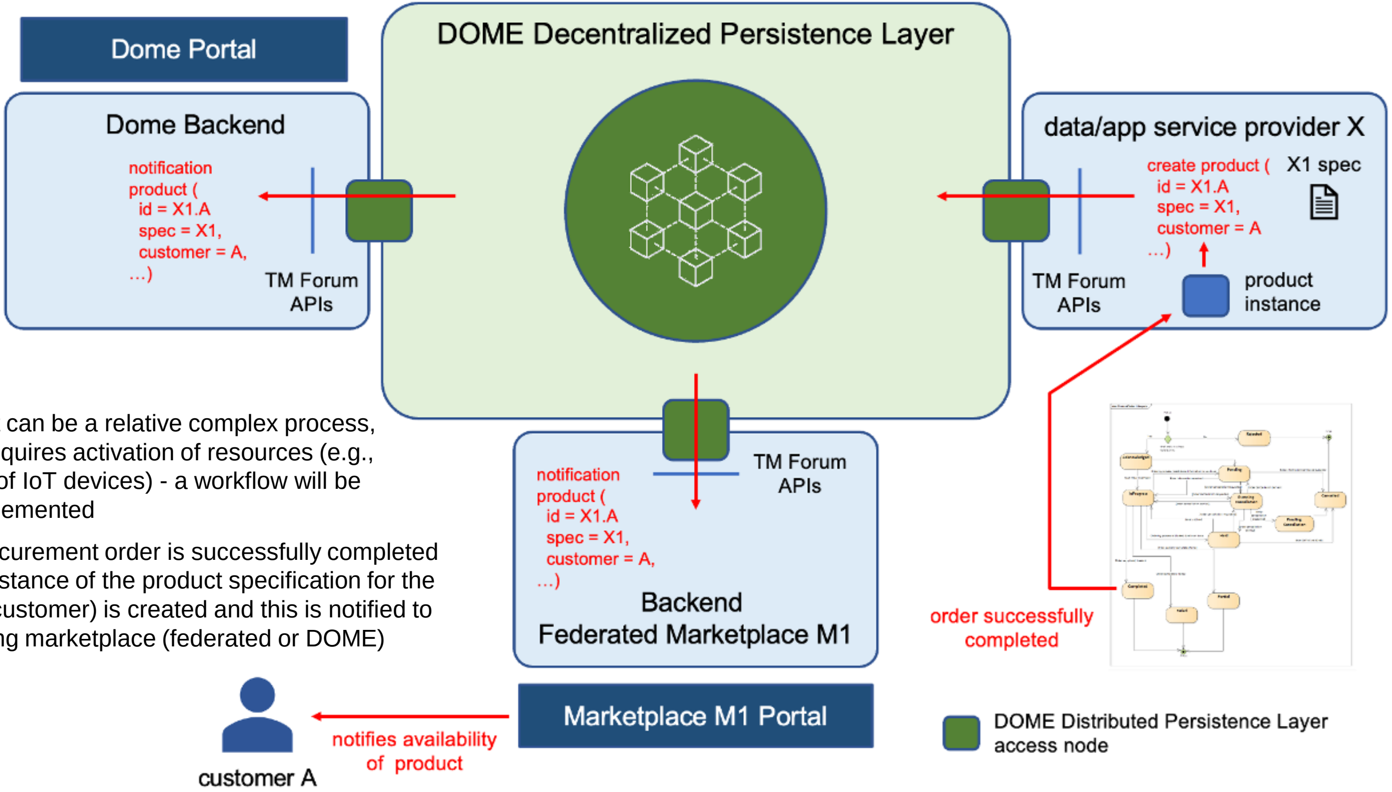
- customers can discover product offerings through a federated marketplaces or the DOME portal
- in some cases, despite discovery can take place through the DOME portal, the data/app service provider may establish that procurement has to be performed through marketplaces of its choice - in that case,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

Product acquisition (through federated marketplace)



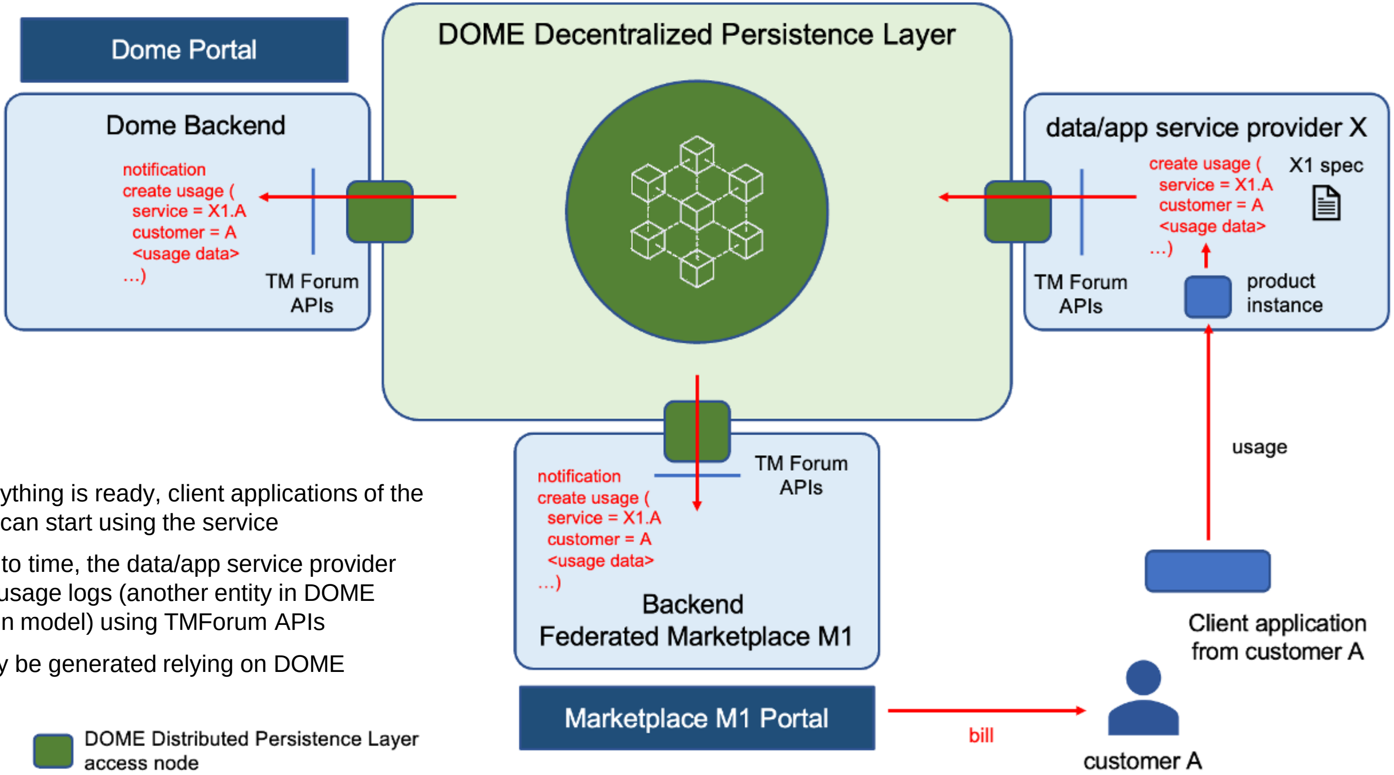
- acquisition of products can be performed through the DOME portal or the portal of some of the federated marketplaces
- in both cases, creation of a product order entity is issued into the DPL layer using TMForum APIs

Product activation (product becomes available for use)


Dome Portal
Dome Backend
notification product (id = X1.A spec = X1, customer = A, …)
TM Forum APIs
DOME Decentralized Persistence Layer
data/app service provider X
create product (id = X1.A spec = X1, customer = A …)
X1 spec
TM Forum APIs
product instance
notification product (id = X1.A spec = X1, customer = A, …)
TM Forum APIs
Backend Federated Marketplace M1
Marketplace M1 Portal
order successfully completed
customer A
notifies availability of product
🟩 DOME Distributed Persistence Layer access node

- 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



Dome Portal

Dome Backend

notification
create usage (
service = X1.A
customer = A
<usage data>
...)

TM Forum APIs

DOME Decentralized Persistence Layer

data/app service provider X

create usage (
service = X1.A
customer = A
<usage data>
...)

X1 spec

TM Forum APIs

product instance

usage

Client application from customer A

notification
create usage (
service = X1.A
customer = A
<usage data>
...)

TM Forum APIs

Backend
Federated Marketplace M1

Marketplace M1 Portal

bill

customer A

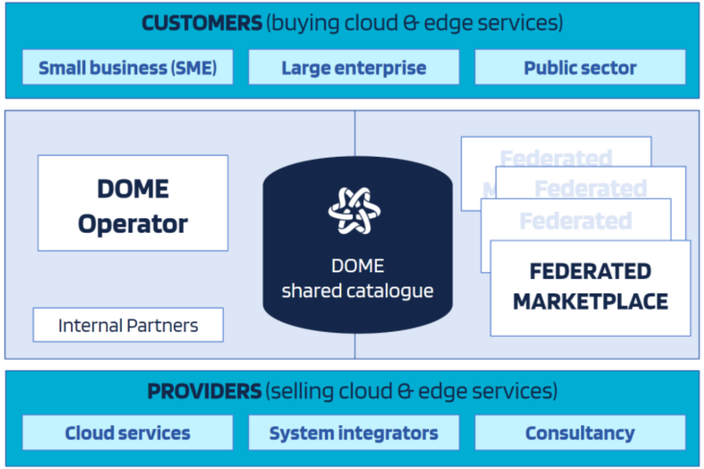
- once everything is ready, client applications of the customer can start using the service
- from time to time, the data/app service provider generate usage logs (another entity in DOME information model) using TMForum APIs
- billing may be generated relying on DOME

🟩 DOME Distributed Persistence Layer access node

Decentralized Trust Framework and IAM (Identity and Access Management)

Introduction: some requirements

- A legal person wants to onboard the DOME ecosystem.
- Relationships in DOME are among legal persons, but legal persons do not have capacity to act.
- Onboarding and many other tasks are performed by employees acting on-behalf-of the legal entity.
- Once agreements are in place, some interactions are among machines acting on-behalf-of the legal entities, under the conditions of the agreements between legal entities.



Problem statement 1: Onboarding in the ecosystem

- We want to enable an employee of a given department of an organisation to perform onboarding in the DOME ecosystem and later some specific operations in it.
- The employee should not be required to be a legal representative (registered in the business registry of the country), or to be able to use a certificate issued to the organisation.
- The organisation (via a legal representative) should be able to nominate (or appoint) an employee and assign limited powers to the employee for the specific functions that she will perform in the ecosystem (this is a mandate).

Typical approach to Onboarding

1. A legal representative of the organisation signs a PDF (handwritten or with eIDAS certificate), identifying an employee and specifying the restricted powers that the employee has with regards to the ecosystem. We call this employee the LEAR (Legal Entity Appointed Representative).
2. An employee of a centralized entity managing onboarding in the ecosystem verifies manually the PDF and signature, and registers the legal entity and employee in the IAM system of the DOME.
3. The LEAR uploads all required documentation, typically in PDF format, which should be verified by people in the back-office of the central entity.
4. The LEAR can then register in the IAM of the centralised entity all other employees of its company that will perform different operations in the ecosystem.

DOME uses a fully digital approach using structured documents and eIDAS signatures to minimize manual work and associated errors as much as possible.

Problem statement 2: Agreements among participants

- We want to enable an employee of a Customer organisation to contract services from a Provider, and other employees of the Customer to manage that service.
- We want to enable an employee of the Customer to designate machines to interact unattended with the services contracted with the Provider.
- The Provider requires an efficient, trusted and decentralised method to verify that the employees and machines accessing its services have been formally empowered by the organisation which contracted the services.
- The Provider wants the highest level of legal certainty and assurance which is practical in the specific environment, and in case of litigation in the courts (EU).

Typical approaches to problem 2

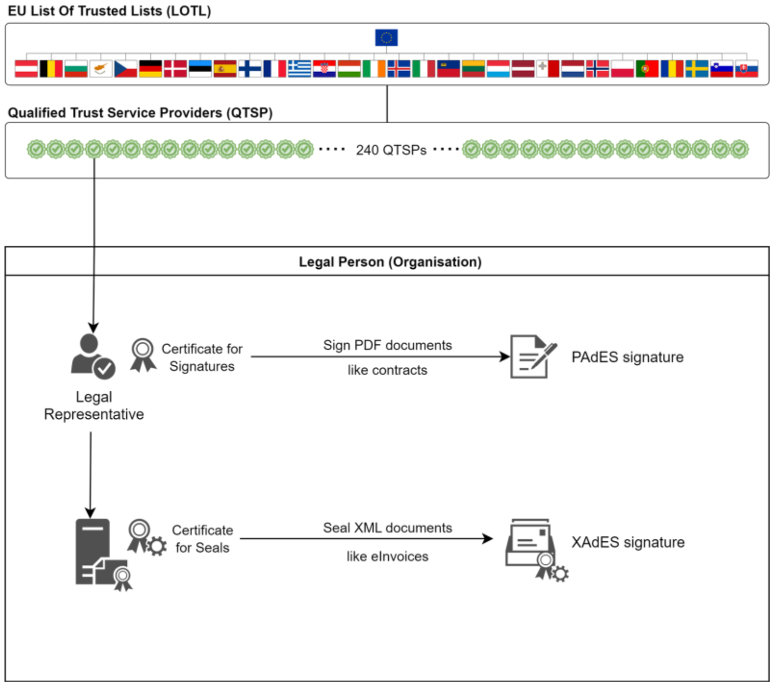
1. One approach is that all Participants (Providers and Customers) trust in the central entity, hoping that its onboarding process is correct, and that its IAM system is never compromised.
2. Another is that each Provider requires a LEAR of the Customer and that all involved employees of the Customer are registered in the IAM system of the each Provider, with the proper rights assigned to each of them.

DOME does not use those approaches because it is a burden on Providers and Customers, and it also generates a lot of disputes (e.g., the Provider having to prove that one employee had the power to perform an operation, and the Customer claiming that the employee did not have the power and it was a problem of the IAM system of the Provider).

Verifiable Credentials with eIDAS certificates

A modern approach

eIDAS Trust Framework and digital signatures


EU List Of Trusted Lists (LOTL)
Qualified Trust Service Providers (QTSP)
240 QTSPs
Legal Person (Organisation)
Legal Representative
Certificate for Signatures
Sign PDF documents like contracts
PAdES signature
Certificate for Seals
Seal XML documents like eInvoices
XAdES signature

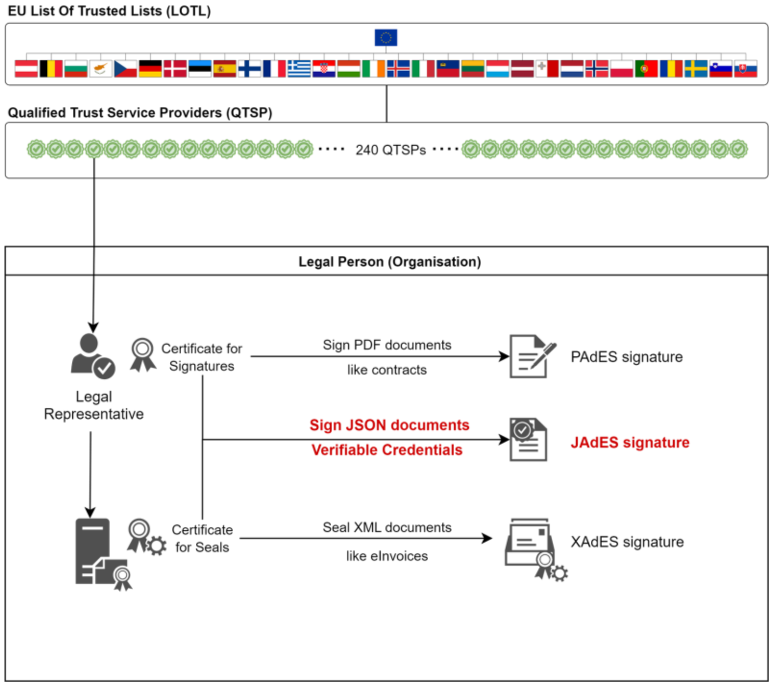
Certificates for signatures and for seals are provided by QTSPs under the eIDAS legal framework. There are some 240 QTSPs, providing different Trust Services.

The certificates are provided via a legal representative of the organisation. Typical usages are:

- Sign PDF documents (eg. contracts) by the legal representative.
- Seal XML documents (eg. eInvoices) automatically by a machine that has installed a certificate for seals.

Qualified signatures are equivalent to handwritten signatures across the EU.

eIDAS Trust Framework and digital signatures



In DOME we use eIDAS certificates to sign/seal Verifiable Credentials, which are JSON documents.

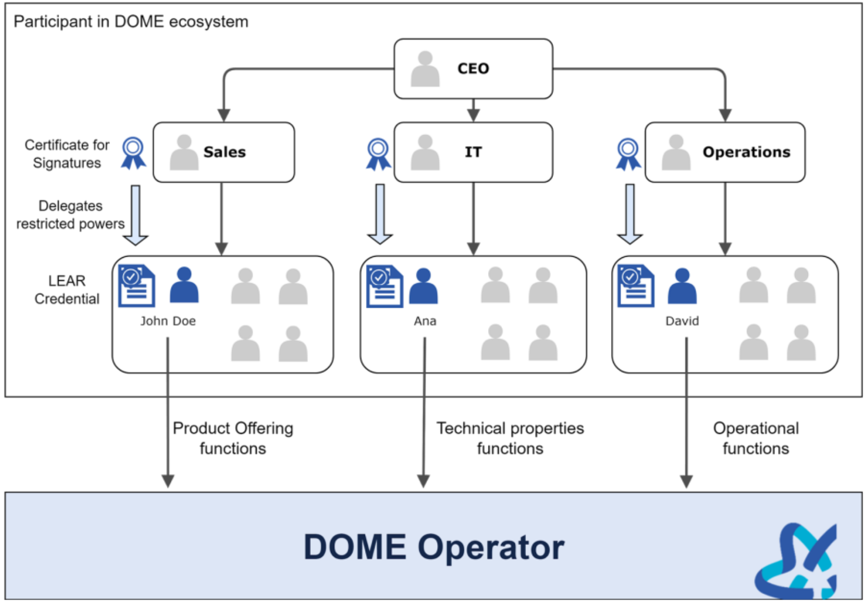
Verifiable Credentials represent several types of documents in structured format and be machine readable and machine verifiable.

Advanced/qualified signatures provide the same legal validity as “traditional” PDF or XML documents.

Legal Entity Appointed Representative credential (LEAR Credential)

A legal representative nominates (or appoints) an employee to act as LEAR by issuing a Verifiable Credential (LEAR Credential) containing:

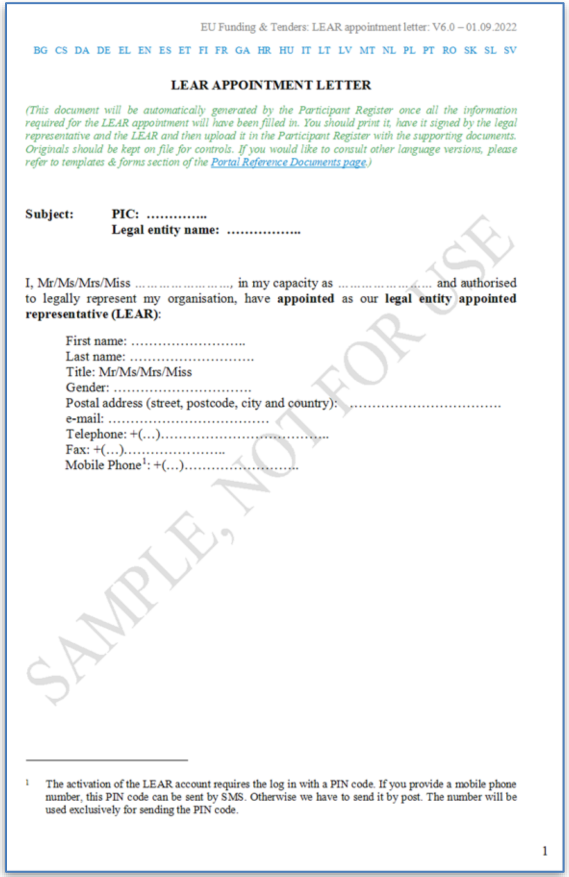
- Claims identifying the employee
- Claims identifying the legal representative attesting and delegating some restricted powers to the employee
- DID of the issuing legal entity
- The specific roles and duties of the LEAR
- Advanced/Qualified signature/seal of the credential


Participant in DOME ecosystem
CEO
Certificate for Signatures
Sales
IT
Operations
Delegates restricted powers
LEAR Credential
John Doe
Ana
David
Product Offering functions
Technical properties functions
Operational functions
DOME Operator

The LEAR Credential

An essential Verifiable Credential for onboarding

Using the EU Funding & Tenders system as an example



EU Funding & Tenders: LEAR appointment letter: V6.0 – 01.09.2022

BG CS DA DE EL EN ES ET FI FR GA HR HU IT LT LV MT NL PL PT RO SK SL SV

LEAR APPOINTMENT LETTER

(This document will be automatically generated by the Participant Register once all the information required for the LEAR appointment will have been filled in. You should print it, have it signed by the legal representative and the LEAR and then upload it in the Participant Register with the supporting documents. Originals should be kept on file for controls. If you would like to consult other language versions, please refer to templates & forms section of the Portal Reference Documents page.)

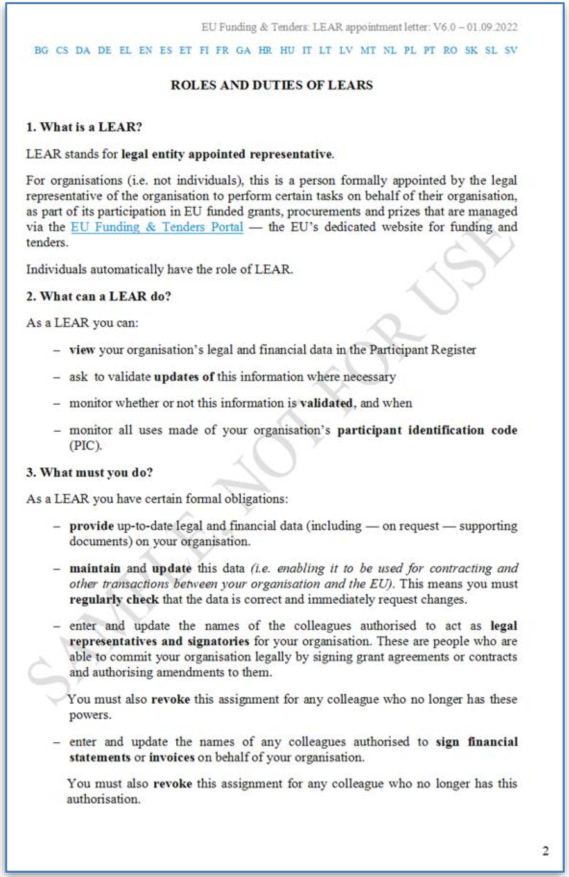
Subject: PIC: …………..
Legal entity name: ……………..

I, Mr/Ms/Mrs/Miss ……………………, in my capacity as …………………… and authorised to legally represent my organisation, have **appointed** as our **legal entity appointed representative (LEAR)**:

First name: ……………………..
Last name: ……………………….
Title: Mr/Ms/Mrs/Miss
Gender: ………………………….
Postal address (street, postcode, city and country): …………………………….
e-mail: ……………………………….
Telephone: +(…)………………………………..
Fax: +(…)…………………..
Mobile Phone[1]: +(…)……………………..

[1] The activation of the LEAR account requires the log in with a PIN code. If you provide a mobile phone number, this PIN code can be sent by SMS. Otherwise we have to send it by post. The number will be used exclusively for sending the PIN code.

1



EU Funding & Tenders: LEAR appointment letter: V6.0 – 01.09.2022

BG CS DA DE EL EN ES ET FI FR GA HR HU IT LT LV MT NL PL PT RO SK SL SV

ROLES AND DUTIES OF LEARS

1. What is a LEAR?

LEAR stands for **legal entity appointed representative**.

For organisations (i.e. not individuals), this is a person formally appointed by the legal representative of the organisation to perform certain tasks on behalf of their organisation, as part of its participation in EU funded grants, procurements and prizes that are managed via the EU Funding & Tenders Portal — the EU's dedicated website for funding and tenders.

Individuals automatically have the role of LEAR.

2. What can a LEAR do?

As a LEAR you can:

- **view** your organisation's legal and financial data in the Participant Register
- ask to validate **updates of** this information where necessary
- monitor whether or not this information is **validated**, and when
- monitor all uses made of your organisation's **participant identification code** (PIC).

3. What must you do?

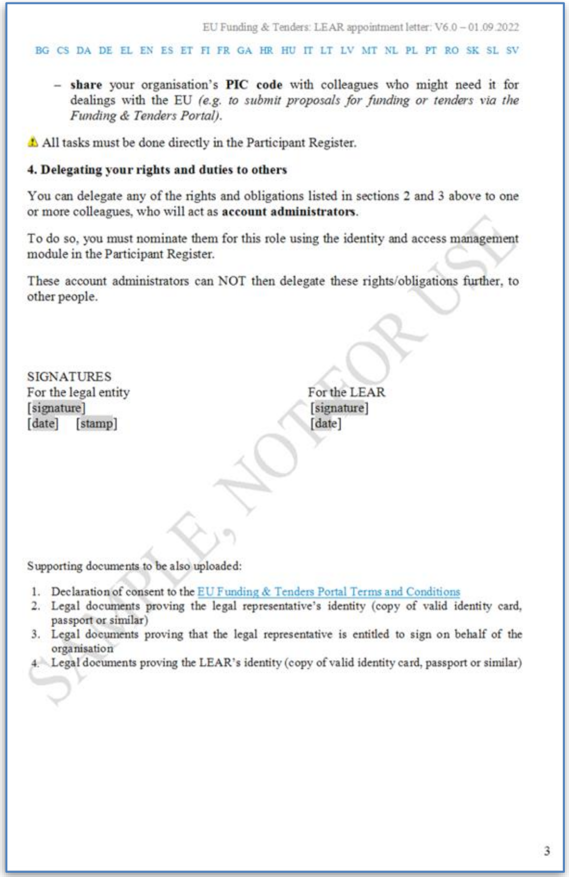
As a LEAR you have certain formal obligations:

- **provide** up-to-date legal and financial data (including — on request — supporting documents) on your organisation.
- **maintain** and **update** this data *(i.e. enabling it to be used for contracting and other transactions between your organisation and the EU)*. This means you must **regularly check** that the data is correct and immediately request changes.
- enter and update the names of the colleagues authorised to act as **legal representatives and signatories** for your organisation. These are people who are able to commit your organisation legally by signing grant agreements or contracts and authorising amendments to them.

  You must also **revoke** this assignment for any colleague who no longer has these powers.
- enter and update the names of any colleagues authorised to **sign financial statements** or **invoices** on behalf of your organisation.

  You must also **revoke** this assignment for any colleague who no longer has this authorisation.

2



EU Funding & Tenders: LEAR appointment letter: V6.0 – 01.09.2022

BG CS DA DE EL EN ES ET FI FR GA HR HU IT LT LV MT NL PL PT RO SK SL SV

- **share** your organisation's **PIC code** with colleagues who might need it for dealings with the EU *(e.g. to submit proposals for funding or tenders via the Funding & Tenders Portal)*.

⚠ All tasks must be done directly in the Participant Register.

4. Delegating your rights and duties to others

You can delegate any of the rights and obligations listed in sections 2 and 3 above to one or more colleagues, who will act as **account administrators**.

To do so, you must nominate them for this role using the identity and access management module in the Participant Register.

These account administrators can NOT then delegate these rights/obligations further, to other people.

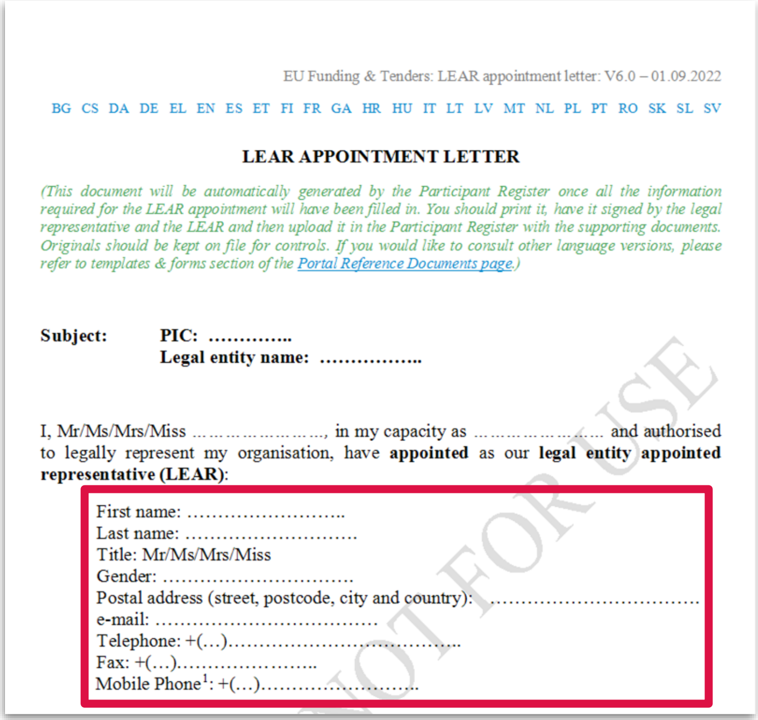
SIGNATURES	
For the legal entity	For the LEAR
[signature]	[signature]
[date] [stamp]	[date]

Supporting documents to be also uploaded:

1. Declaration of consent to the EU Funding & Tenders Portal Terms and Conditions
2. Legal documents proving the legal representative's identity (copy of valid identity card, passport or similar)
3. Legal documents proving that the legal representative is entitled to sign on behalf of the organisation
4. Legal documents proving the LEAR's identity (copy of valid identity card, passport or similar)

3

Claims about employee who will act as LEAR



EU Funding & Tenders: LEAR appointment letter: V6.0 – 01.09.2022

BG CS DA DE EL EN ES ET FI FR GA HR HU IT LT LV MT NL PL PT RO SK SL SV

LEAR APPOINTMENT LETTER

(This document will be automatically generated by the Participant Register once all the information required for the LEAR appointment will have been filled in. You should print it, have it signed by the legal representative and the LEAR and then upload it in the Participant Register with the supporting documents. Originals should be kept on file for controls. If you would like to consult other language versions, please refer to templates & forms section of the Portal Reference Documents page.)

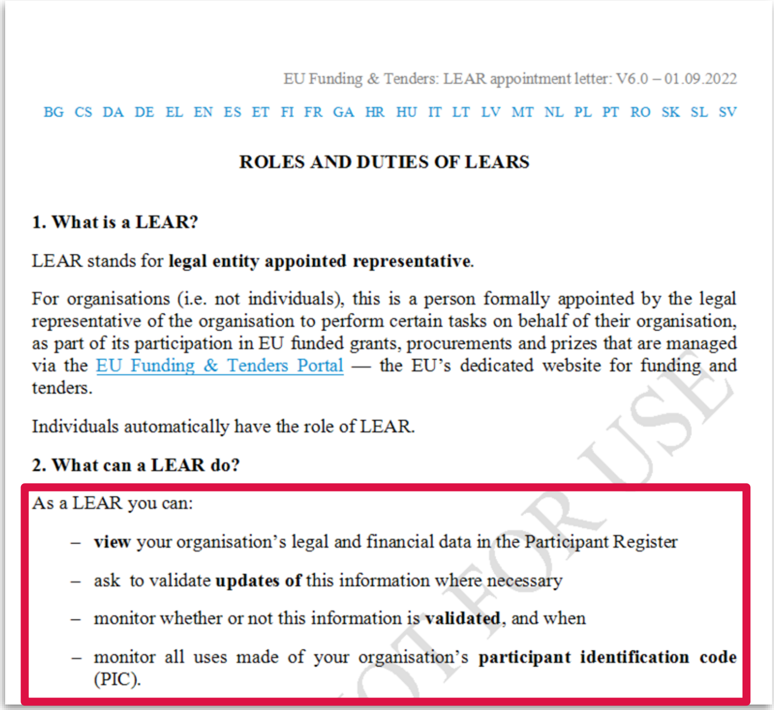
Subject: **PIC: ………….**
Legal entity name: ……………..

I, Mr/Ms/Mrs/Miss ……………………, in my capacity as ………………… and authorised to legally represent my organisation, have **appointed** as our **legal entity appointed representative (LEAR)**:

First name: ……………………..
Last name: ………………………
Title: Mr/Ms/Mrs/Miss
Gender: ………………………….
Postal address (street, postcode, city and country): ……………………………
e-mail: ………………………………
Telephone: +(…)………………………………..
Fax: +(…)…………………..
Mobile Phone[1]: +(…)……………………..

```
{
   "first_name": "John",
   "last_name": "Doe",
   "title": "Mr.",
   "gender": "M",
   "postal_address": "",
   "email": "johndoe@goodair.com",
   "telephone": "",
   "fax": "",
   "mobile_phone": "+34787426623",
   "id": "did:key:z6MkhaXgBZ…LGpbnnEGta2doK"
}
```

Roles and duties of the employee



EU Funding & Tenders: LEAR appointment letter: V6.0 – 01.09.2022

BG CS DA DE EL EN ES ET FI FR GA HR HU IT LT LV MT NL PL PT RO SK SL SV

ROLES AND DUTIES OF LEARS

1. What is a LEAR?

LEAR stands for **legal entity appointed representative**.

For organisations (i.e. not individuals), this is a person formally appointed by the legal representative of the organisation to perform certain tasks on behalf of their organisation, as part of its participation in EU funded grants, procurements and prizes that are managed via the EU Funding & Tenders Portal — the EU's dedicated website for funding and tenders.

Individuals automatically have the role of LEAR.

2. What can a LEAR do?

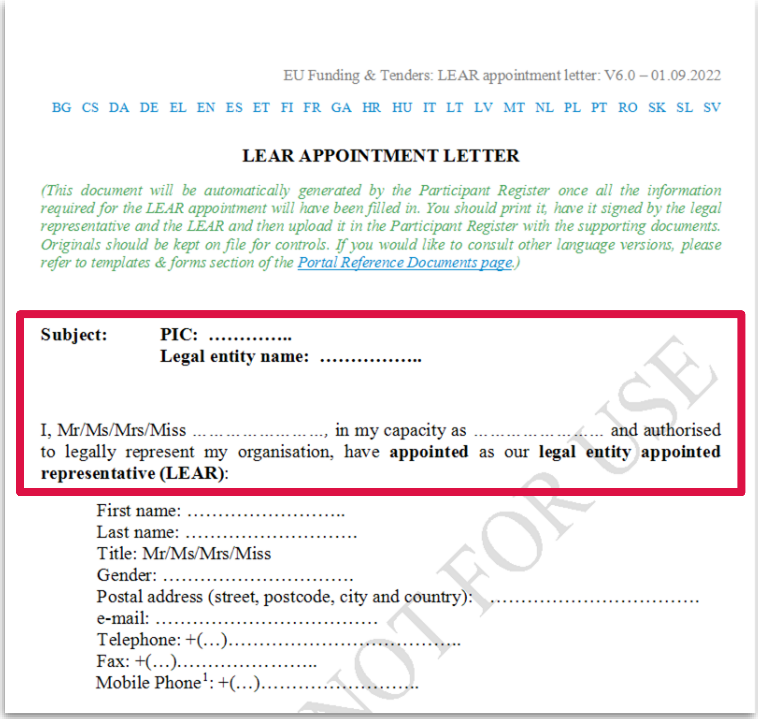
As a LEAR you can:

- **view** your organisation's legal and financial data in the Participant Register
- ask to validate **updates of** this information where necessary
- monitor whether or not this information is **validated**, and when
- monitor all uses made of your organisation's **participant identification code** (PIC).

```
[
   {
      "id": "https://dome-marketplace.eu/lear/v1/6484994n4r9e990494",
      "target":"https://bae.dome-marketplace.eu/",
      "roleNames": ["onboarder","contracter","reporter"]
   }
]
```

We will talk later about the roles in DOME, specifically to access the TM Forum APIs.

Identification of the legal representative



EU Funding & Tenders: LEAR appointment letter: V6.0 – 01.09.2022

BG CS DA DE EL EN ES ET FI FR GA HR HU IT LT LV MT NL PL PT RO SK SL SV

LEAR APPOINTMENT LETTER

(This document will be automatically generated by the Participant Register once all the information required for the LEAR appointment will have been filled in. You should print it, have it signed by the legal representative and the LEAR and then upload it in the Participant Register with the supporting documents. Originals should be kept on file for controls. If you would like to consult other language versions, please refer to templates & forms section of the Portal Reference Documents page.)

Subject: **PIC: ………….**
Legal entity name: ……………..

I, Mr/Ms/Mrs/Miss ………………….., in my capacity as ………………… and authorised to legally represent my organisation, have **appointed** as our **legal entity appointed representative (LEAR)**:

First name: ……………………..
Last name: ………………………
Title: Mr/Ms/Mrs/Miss
Gender: …………………………
Postal address (street, postcode, city and country): ……………………………
e-mail: ………………………………
Telephone: +(…)………………………………..
Fax: +(…)…………………..
Mobile Phone[1]: +(…)……………………..

```
cn = 56565656V Jesus Ruiz
serialNumber = 56565656V
givenName = Jesus
sn = Ruiz
organizationIdentifier = VATES-12345678
o = GoodAir
c = ES
```

This information extracted from the eIDAS certificate used to sign the Verifiable Credential.

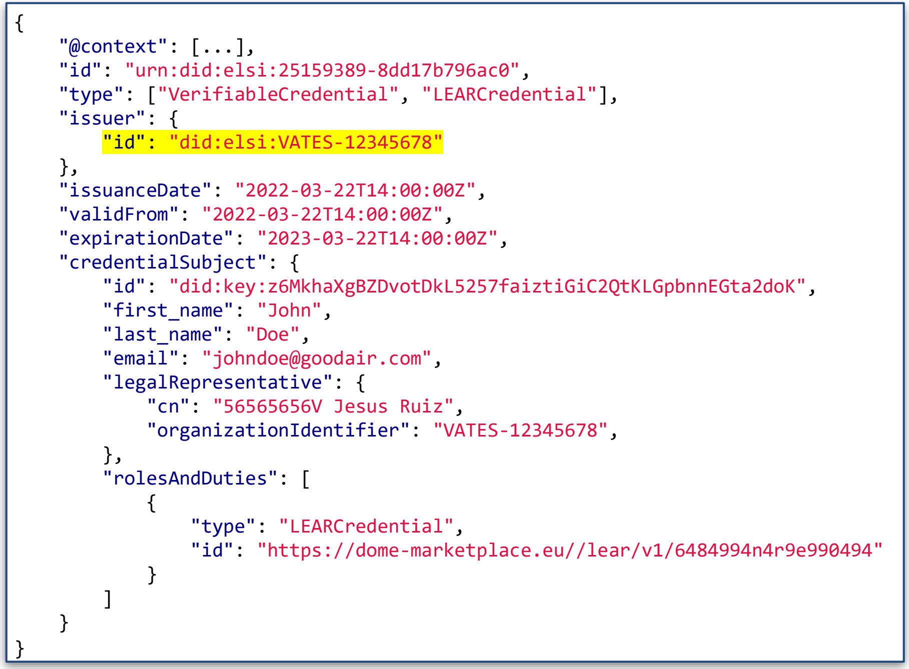
This way, the identification information in the document (Verifiable Credential) and in the signature match, and automatic verification is enabled.

Putting the pieces together

We use the did:elsi (**E**TSI **L**egal person **S**emantic **I**dentifier) method to identify the issuer of the Verifiable Credential.

```
did-format := did:elsi:<organizationIdentifier>
```

Where organizationIdentifier is equal to attribute *organizationIdentifier* of the Subject Distinguished Name field of the eIDAS certificate (aka eIDAS LegalPersonIdentifier), as specified in ETSI 119 412-1.



```
{
    "@context": [...],
    "id": "urn:did:elsi:25159389-8dd17b796ac0",
    "type": ["VerifiableCredential", "LEARCredential"],
    "issuer": {
        "id": "did:elsi:VATES-12345678"
    },
    "issuanceDate": "2022-03-22T14:00:00Z",
    "validFrom": "2022-03-22T14:00:00Z",
    "expirationDate": "2023-03-22T14:00:00Z",
    "credentialSubject": {
        "id": "did:key:z6MkhaXgBZDvotDkL5257faiztiGiC2QtKLGpbnnEGta2doK",
        "first_name": "John",
        "last_name": "Doe",
        "email": "johndoe@goodair.com",
        "legalRepresentative": {
            "cn": "56565656V Jesus Ruiz",
            "organizationIdentifier": "VATES-12345678",
        },
        "rolesAndDuties": [
            {
                "type": "LEARCredential",
                "id": "https://dome-marketplace.eu//lear/v1/6484994n4r9e990494"
            }
        ]
    }
}
```

Signature with the eIDAS certificate of a legal representative

The Issuer is a QTSP in the eIDAs Trust Framework.

The Subject field contains both:

- Identification of the organisation
- Identification of the legal representative (natural person) owning the certificate

When using the certificate (signature, authentication, email) the natural person is acting as a legal representative of the organisation identified in the certificate.

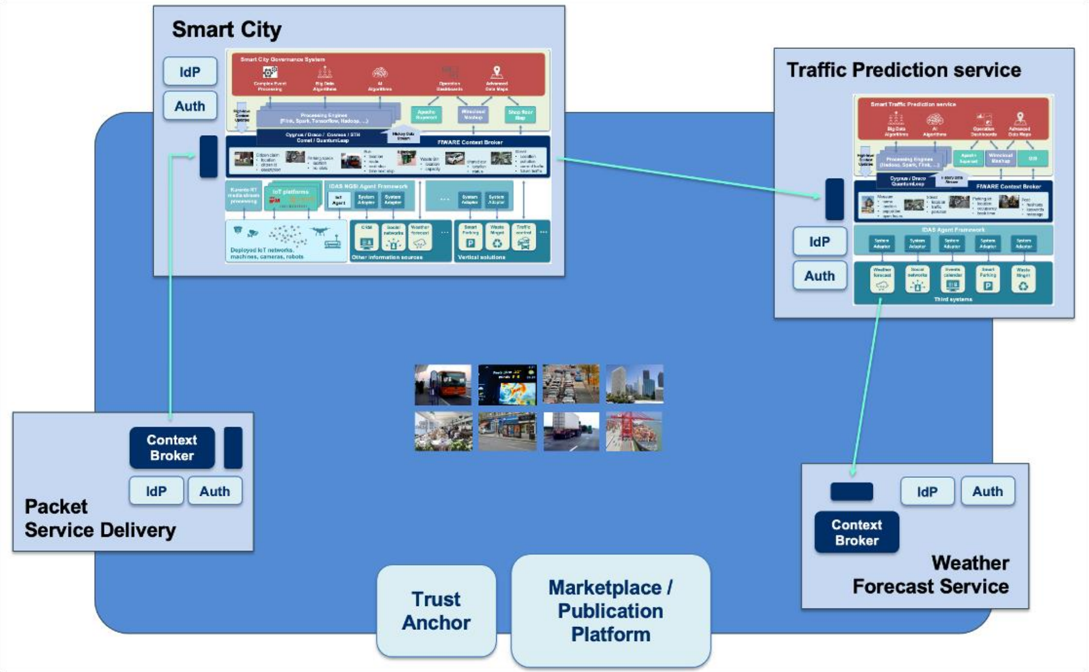
```
Version: 3 (0x2)
Issuer:
   C = ES,
   O = CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA,
   OU = Serveis Públics de Certificació, CN = EC-SectorPublic Validity
   Not Before: Mar  8 16:35:43 2021 GMT
   Not After : Mar  8 16:35:42 2025 GMT

Subject:
   organizationIdentifier = VATES-Q5856338H,
   C = ES,
   O = Centre de Telecomunicacions i Tecnologies de la Informació
       de la Generalitat de Catalunya,
   OU = Treballador públic de nivell mig, title = Director Gerent (e. f.),
   serialNumber = IDCES-12345678B,
   SN = MILA VIDAL - DNI 12345678B,
   GN = XAVIER,
   CN = XAVIER MILA VIDAL - DNI 77286397A (TCAT)

X509v3 extensions:
   X509v3 Extended Key Usage:
      TLS Web Client Authentication, E-mail Protection
   X509v3 Key Usage: critical
      Digital Signature, Non Repudiation, Key Encipherment
```

Examples

Gaia-X	did:elsi:VATBE-0762747721
Instituto de Fisica de Cantabria	did:elsi:VATES-Q3918001C
Alastria	did:elsi:VATES-G87936159
IN2	did:elsi:VATES-B60645900
Digitel TS	did:elsi:VATES-B47447560
FIWARE Foundation	did:elsi:VATDE-309937516
TNO	did:elsi:LEIXG-724500AZSGBRY55MNS59

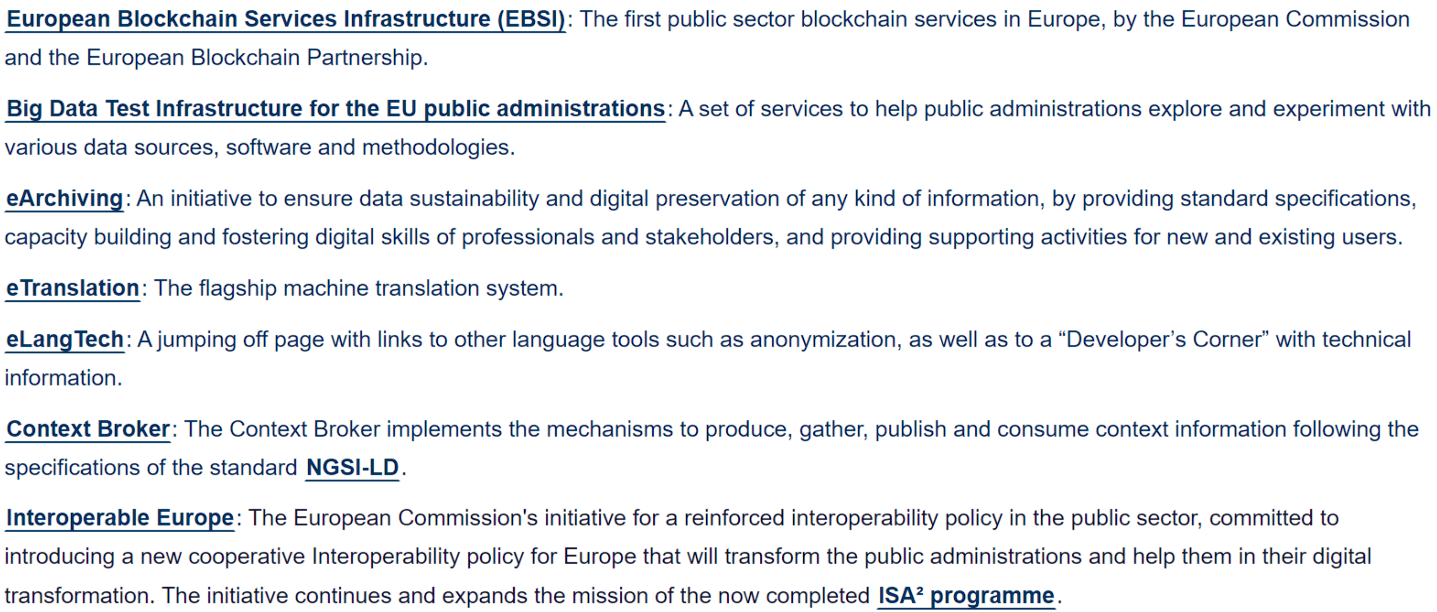
Some key concepts: Verifiable Credentials

- VCs will be used to describe participants in the DOME ecosystem
- 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)
- VCs will be used to support Attribute Based Access Control (ABAC) in DOME:
  - claims linked to VCs will map to attributes (roles) assigned to users
  - policies will map to rules over those claims and other environment attributes
- VC-based ABAC can be also implemented by product providers, the DOME Trust and IAM framework will be available for them



Some considerations

The approach is fully aligned with the Digital Europe Program initiative and its Building Blocks.



European Blockchain Services Infrastructure (EBSI): The first public sector blockchain services in Europe, by the European Commission and the European Blockchain Partnership.

Big Data Test Infrastructure for the EU public administrations: A set of services to help public administrations explore and experiment with various data sources, software and methodologies.

eArchiving: An initiative to ensure data sustainability and digital preservation of any kind of information, by providing standard specifications, capacity building and fostering digital skills of professionals and stakeholders, and providing supporting activities for new and existing users.

eTranslation: The flagship machine translation system.

eLangTech: A jumping off page with links to other language tools such as anonymization, as well as to a “Developer’s Corner” with technical information.

Context Broker: The Context Broker implements the mechanisms to produce, gather, publish and consume context information following the specifications of the standard **NGSI-LD**.

Interoperable Europe: The European Commission's initiative for a reinforced interoperability policy in the public sector, committed to introducing a new cooperative Interoperability policy for Europe that will transform the public administrations and help them in their digital transformation. The initiative continues and expands the mission of the now completed **ISA² programme**.

Some considerations

The approach is fully aligned with the Digital Europe Program initiative and its Building Blocks.

eDelivery

Exchange electronic data and documents in an interoperable and secure way

eSignature

Create and verify electronic, paperless signatures

eID

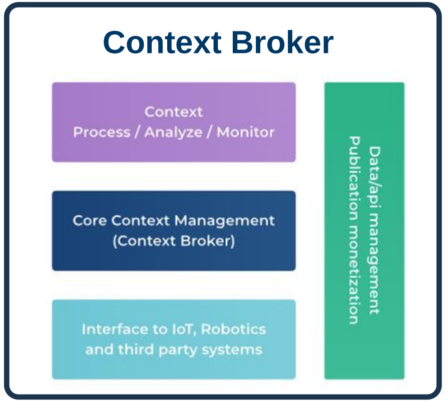
Offer services capable of electronically identifying users from all across Europe

Once-Only Technical System (OOTS)

Reduce administrative burden on citizens and businesses

eInvoicing

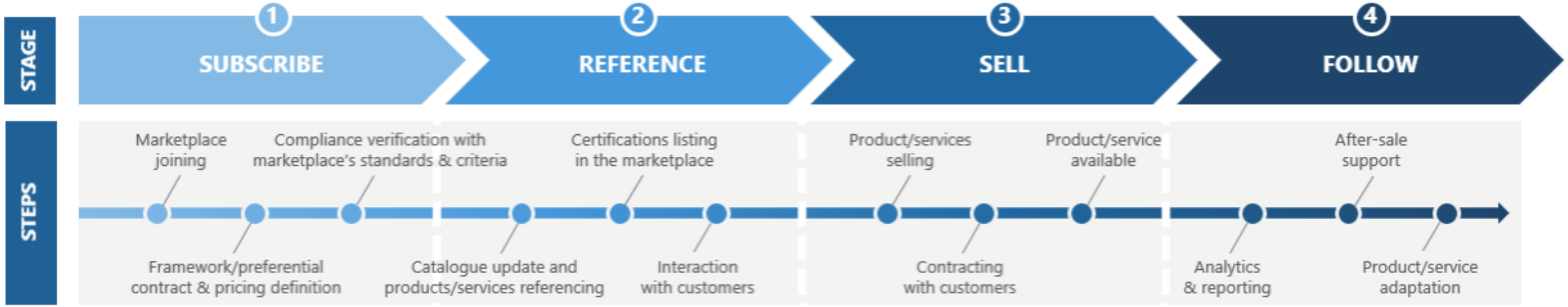
Send and receive electronic invoices in line with the European Directive


Context Broker

Some considerations (2)

- Usage of eIDAS certificates for citizens is very low, but it is much higher for organisations.
- Any organisation which can sign (advanced or qualified) PDF documents or eInvoices has already the certificate required for the LEAR Credential.
- This is also aligned with the mandatory B2B requirements for eInvoicing being implemented across the EU (complementing to the B2G requirements).
- For the actors involved in DOME (especially CSPs), the requirement to be able to sign a JSON document should not a problem. eIDAS certificates are a fundamental building block for the cross-border digitalisation of the EU.
- Any legally incorporated organisation in the EU can request an eIDAS certificate from any of the QTSPs providing service in its country of incorporation.

Cloud and Edge Service Provider journey


STAGE

1 SUBSCRIBE

2 REFERENCE

3 SELL

4 FOLLOW

STEPS

Marketplace joining

Framework/preferential contract & pricing definition

Compliance verification with marketplace's standards & criteria

Catalogue update and products/services referencing

Certifications listing in the marketplace

Interaction with customers

Product/services selling

Contracting with customers

Product/service available

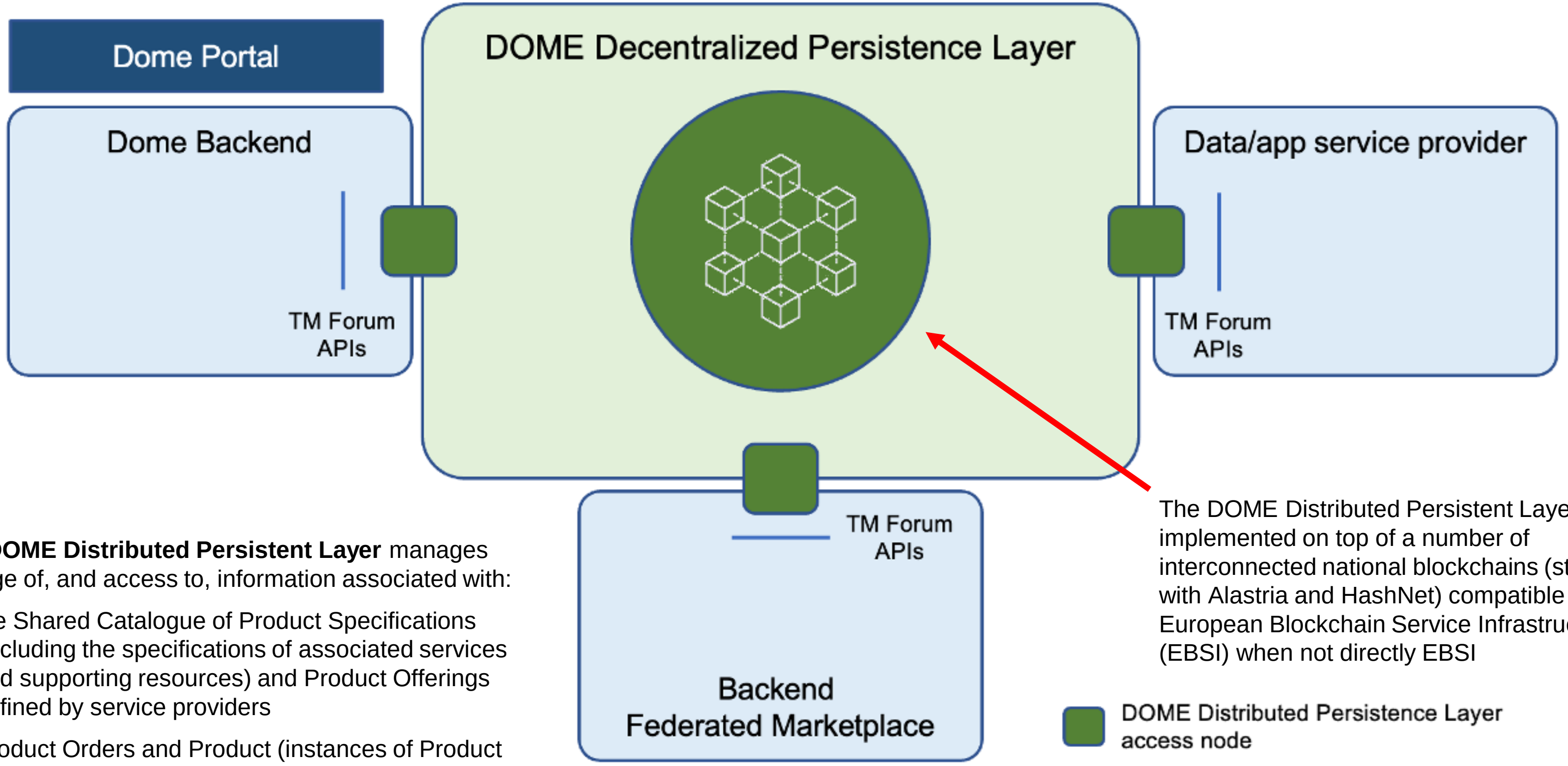
Analytics & reporting

After-sale support

Product/service adaptation

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

Marketplaces federation + Shared Catalogue



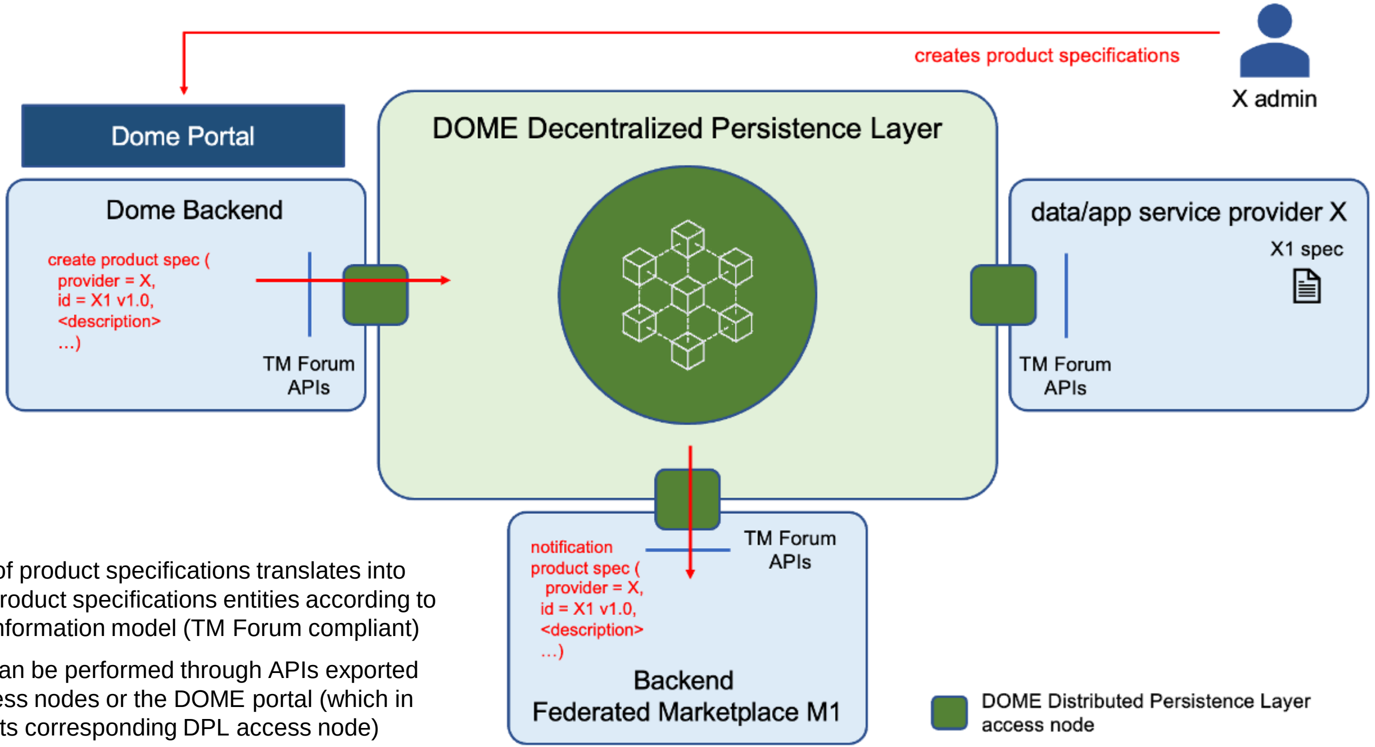
The DOME Distributed Persistent Layer will be implemented on top of a number of interconnected national blockchains (starting with Alastria and HashNet) compatible with the European Blockchain Service Infrastructure (EBSI) when not directly EBSI

🟩 DOME Distributed Persistence Layer access node

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

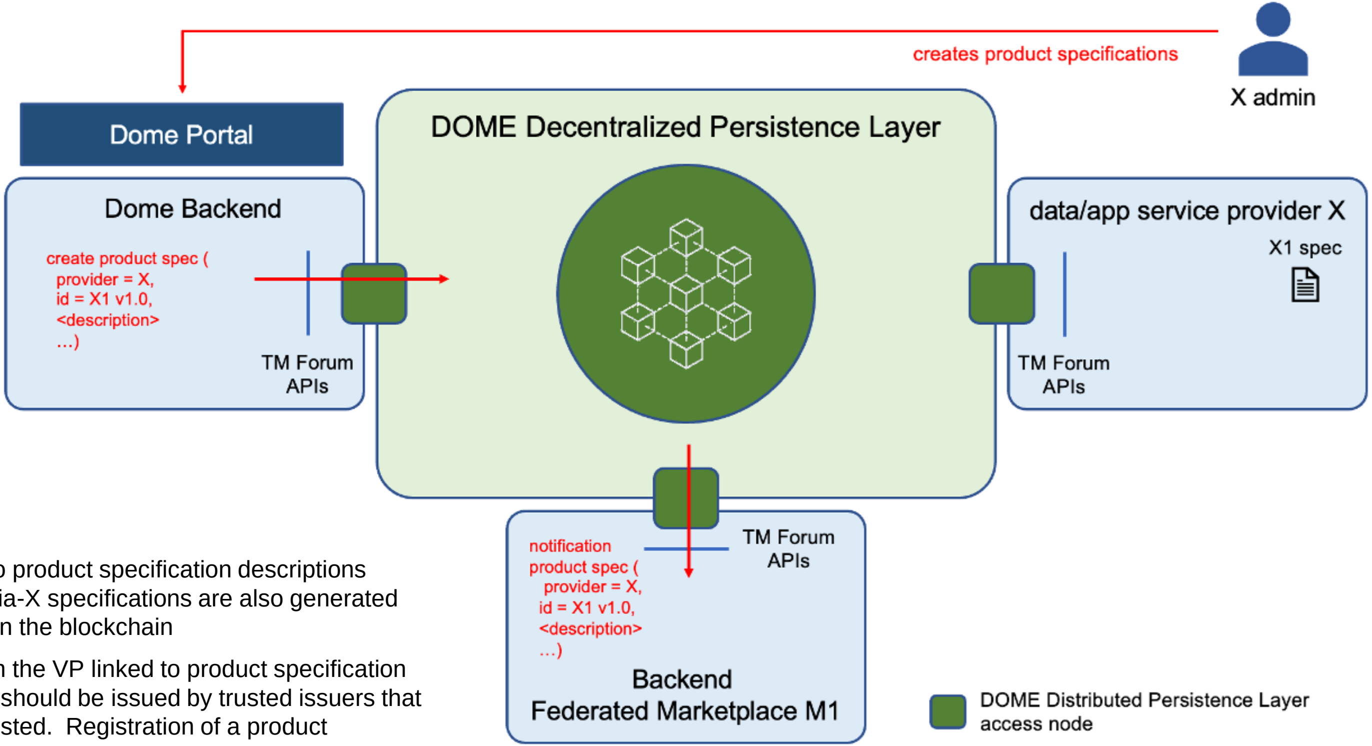
- the Shared Catalogue of Product Specifications (including the specifications of associated services and supporting resources) and Product Offerings defined by service providers
- Product Orders and Product (instances of Product Specifications) along their lifecycle, as well as information about actual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

Registration of product specification



- 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 or the DOME portal (which in turn rely on its corresponding DPL access node)

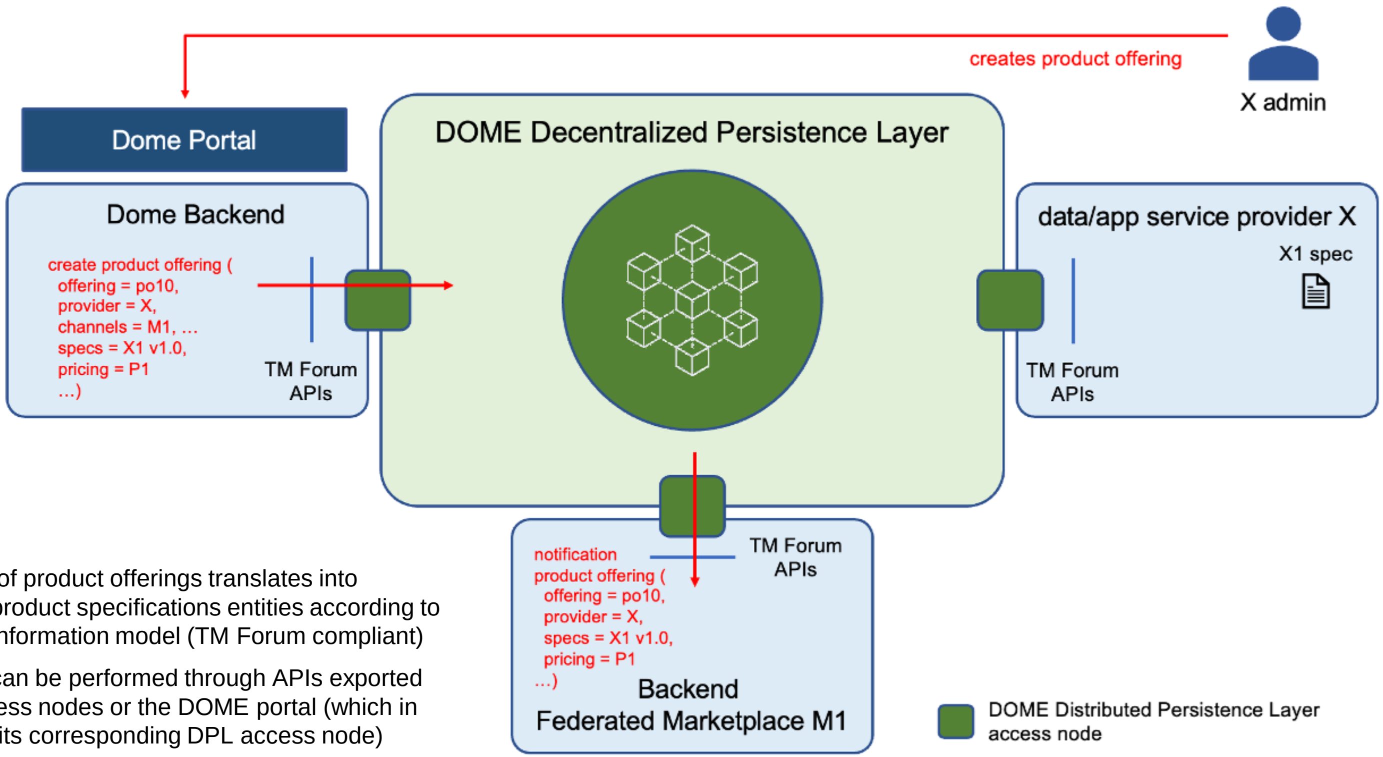
Registration of product specification (cont.)



🟩 DOME Distributed Persistence Layer access node

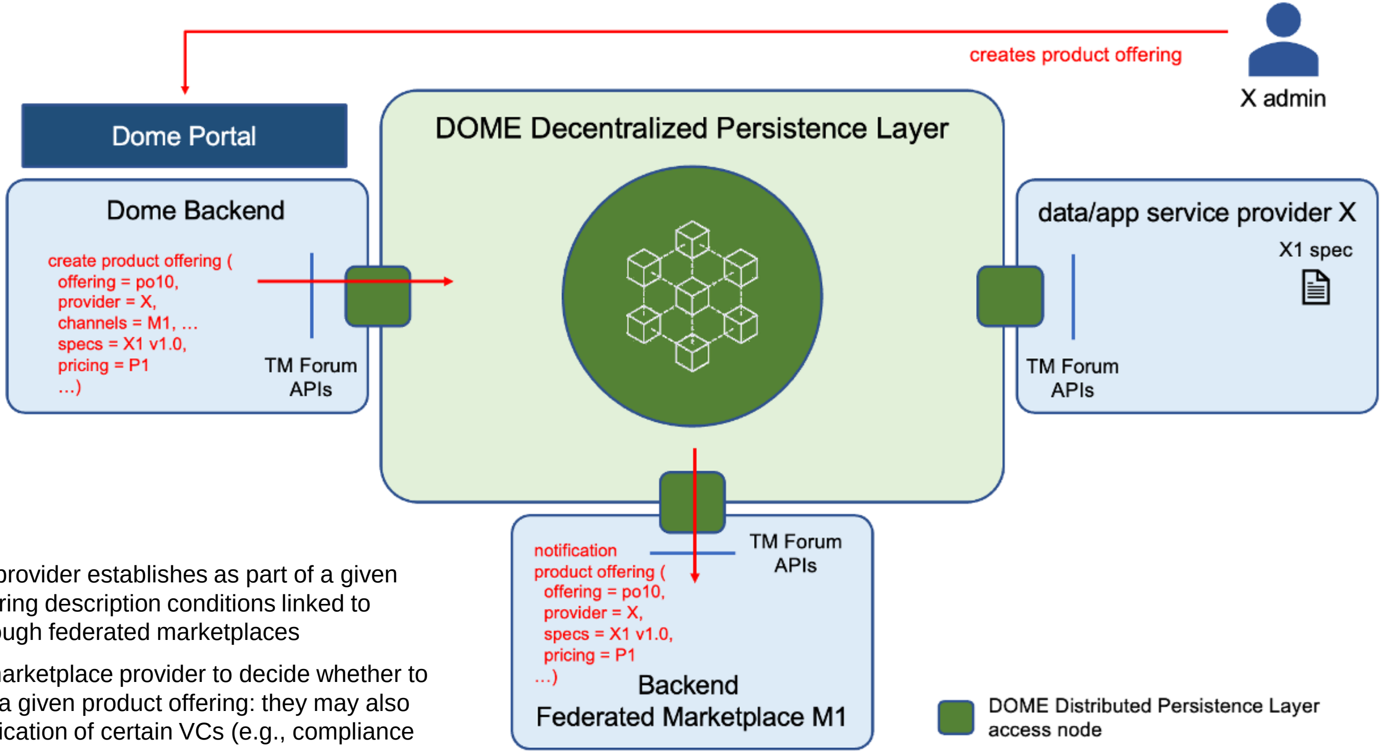
- VPs linked to product specification descriptions following Gaia-X specifications are also generated and stored on the blockchain
- Some VCs in the VP linked to product specification descriptions should be issued by trusted issuers that DOME has listed. Registration of a product specification may be rejected if a certain VC is not present or cannot be verified

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

Creation of Product Offering (cont.)



create product offering (
offering = po10,
provider = X,
channels = M1, …
specs = X1 v1.0,
pricing = P1
…)

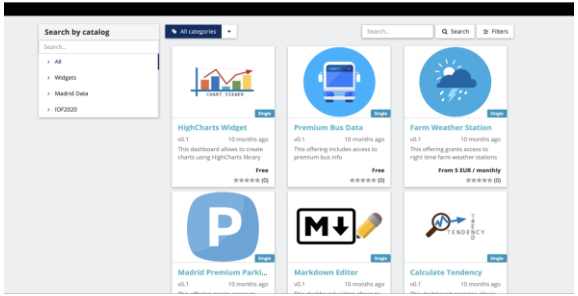
notification
product offering (
offering = po10,
provider = X,
specs = X1 v1.0,
pricing = P1
…)

- 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

Marketplace data model and APIs

Alignment with TM Forum Open APIs and Gaia-X

- DOME relies on a subset of TM Forum Open API recommendations with regards to the definition of its underlying information model as well as APIs supporting:
  - storage of information about products (= services and supporting resources instantiated for a particular customer), product specifications and product offerings
  - storage of logs along 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



HighCharts Widget
v0.1 10 months ago
This dashboard allows to create charts using HighCharts library
Free
(0)

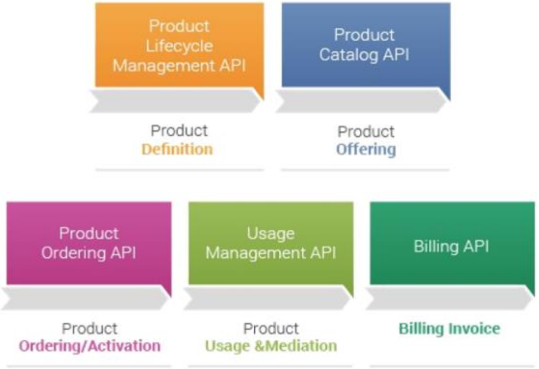
Premium Bus Data
v0.1 10 months ago
This offering includes access to premium bus info
Free
(0)

Farm Weather Station
v0.1 10 months ago
This offering grants access to right time farm weather stations
From 5 EUR / monthly
(0)

Madrid Premium Parki...
v0.1 10 months ago

Markdown Editor
v0.1 10 months ago

Calculate Tendency
v0.1 10 months ago



Product Lifecycle Management API

Product Definition

Product Catalog API

Product Offering

Product Ordering API

Product Ordering/Activation

Usage Management API

Product Usage &Mediation

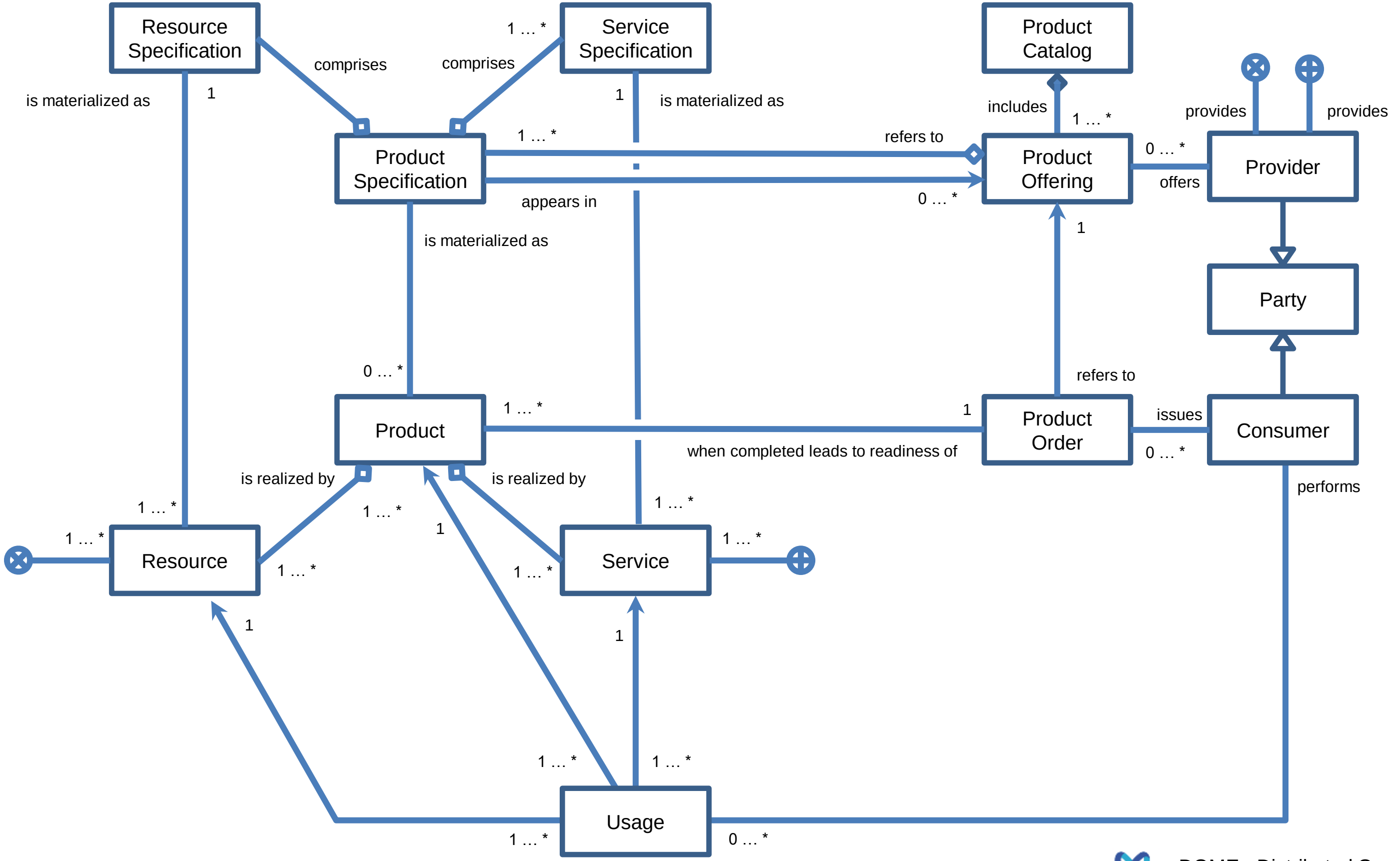
Billing API

Billing Invoice

Some key concepts: Products, Services, Resources

- A Data/Application Provider is considered, using TM Forum terminology, a Product Provider
- A Product is realized as a combination of Services and/or Resources:
  - Services provide access to data or perform processing of data
  - Resources typically required for the execution of the Services
- Products (and corresponding services and resources) are provisioned and activated for a particular Customer:
  - Provision and activation may take days: not all automatically!
  - Not everything runs on the Cloud: cloud-to-edge products
- Example: Air Quality Monitoring Product
  - Comprises a number of Services (e.g., web portal, REST services endpoints, etc) some of which bring access to data (air quality measures) or perform processing of data (air quality predictions)
  - It requires that IoT devices are deployed in the field and some computing capacity provisioned on the cloud (resources)

TM Forum APIs for Marketplaces - Model (Simplification)



Main entities/concepts

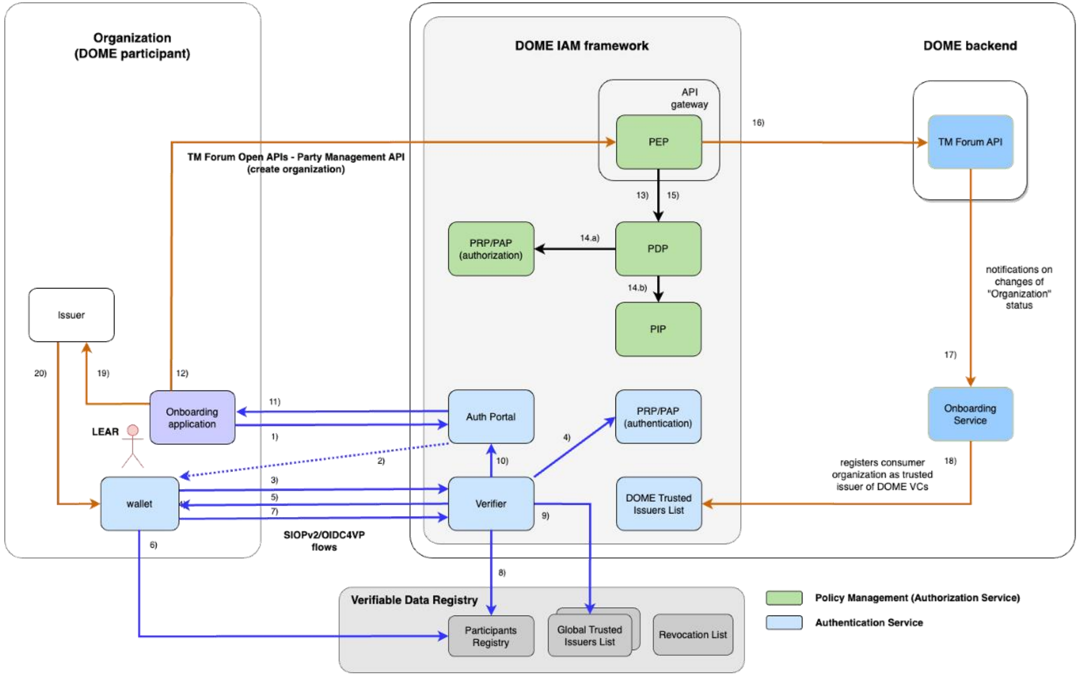
- A **Product Catalog** is a collection of Product Offerings intended for a set of specific Distribution Channels and Market Segments.
- A **Product** is created in the **Product Inventory** when a **Product Offering** is procured by a **Party** (customer or other interested party). This means that a **Product Order** has been issued and successfully completed.
- A Product is realized as a combination of **Services** and/or **Resources** which get instantiated in a **Service Inventory** and a **Resource Inventory**, respectively. **Resource Orders** and **Service Orders** are derived from a Product Order for that purpose.
- A Product Offering comprises:
  - the **Product Specification**, including characteristics of the derived products
  - the **Agreement** that governs usage of derived products,
  - the associated **Product Offering Price**,
  - etc
- Note that a Product is what is generated when a Product Offering is procured for a specific customer, that is, a Product is the instantiation of a Product Specification but in connection to a specific agreement, price, etc for the customer

Main entities/concepts

- A **Product Specification** includes references to a series of **Service Specification**s and/or **Resource Specification**s required to realize the Products linked to the Product Specification:
  - each **Service Specification** is made available through a **Service Candidate** in the **Service Catalog**
  - each **Resource Specification** is made available through a **Resource Candidate** in a **Resource Catalog**
- Note that here may be one or more Product Offerings around the same Product Specification (e.g., associated with different prices or targeted to different market segments).
- Each time a Product, Resource or Service is used, a **Usage** entity is created, which typically is used to calculate how much can be charged to consumers and paid to providers.

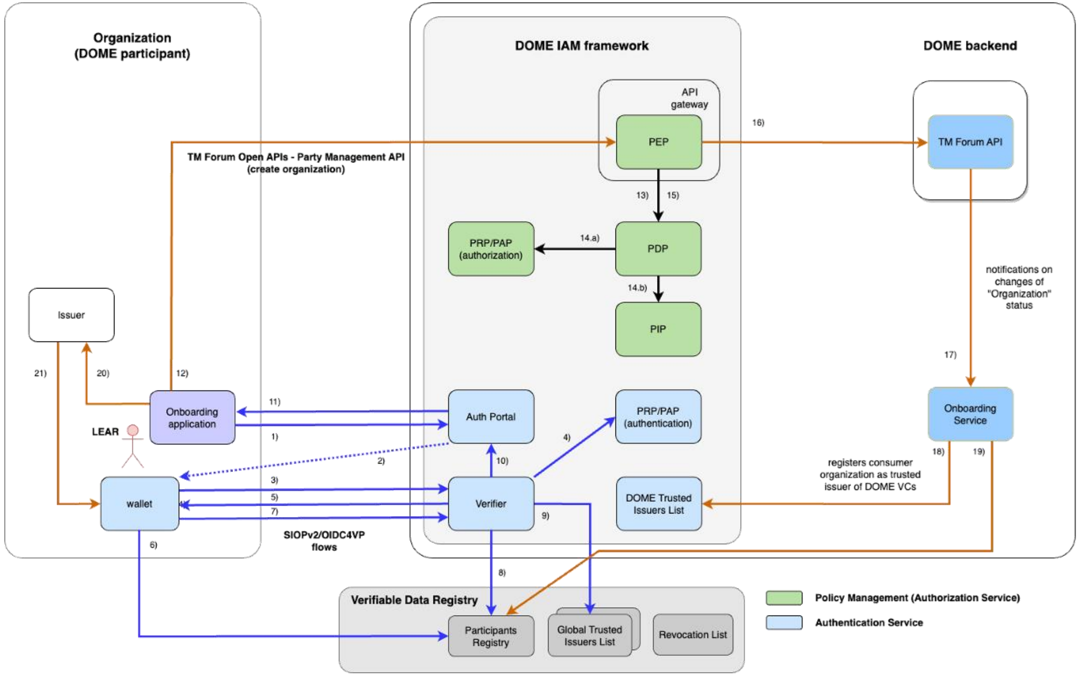
Organization onboarding through the DOME portal (take 1)

- Using an onboarding app (or a web portal), a LEAR of the organization to onboard in DOME will request authentication into the DOME service (steps 1-3 involving scanning of QR code using the wallet)
- The Verifier will request from the user's wallet a VC that accredits him/her as LEAR of the organization, eventually other VCs (steps 4-5).
- Still to be determined, we define the concept of "DOME ecosystem" in which participants have to comply with certain rules. If so, the wallet will check whether the verifier belongs to a participant in the ecosystem (step 6) and return the requested VCs (step 7). Since DOME will be part of that ecosystem, it will return that is the case.
- The Verifier checks whether the LEAR's VC was issued by a trusted participant of the DOME ecosystem (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 completes all the necessary information (which may take even days), it is registered in the DOME trusted issuers list as trusted issuer of VCs that may include claims as buyer, seller or marketplace of products in the connector (step 18)
- Once onboarding is completed, the system for issuance of VCs at the organization can issue DOME VCs (steps 19-20)



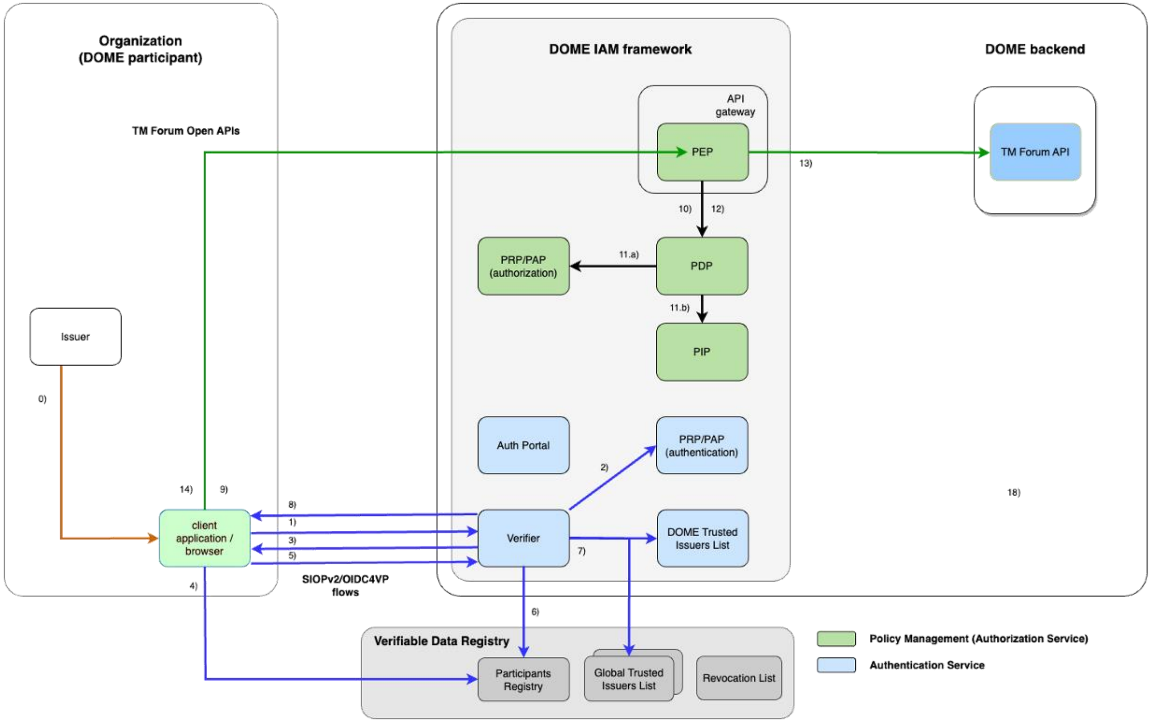
Organization onboarding through the DOME portal (take 2)

- Using an onboarding app (or a web portal), a LEAR of the organization to onboard in DOME will request authentication into the DOME service (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).
- Still to be determined, we define the concept of "DOME ecosystem" in which participants have to comply with certain rules. If so, the wallet will check whether the verifier belongs to a participant in the data space (step 6) and return the requested VCs (step 7). Since DOME is itself part of the ecosystem, it will return that is the case.
- The Verifier checks whether the LEAR's VC was issued by a trusted participant of the DOME ecosystem (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 completes all the necessary information (which may take even days), it is registered in the DOME trusted issuers list as trusted issuer of VCs that may include claims as buyer, seller or marketplace of products in the connector (step 18) and it will be also registered in the Participants Registry (step 19)
- Once onboarding is completed, the system for issuance of VCs at the organization can issue DOME VCs (steps 20-21)



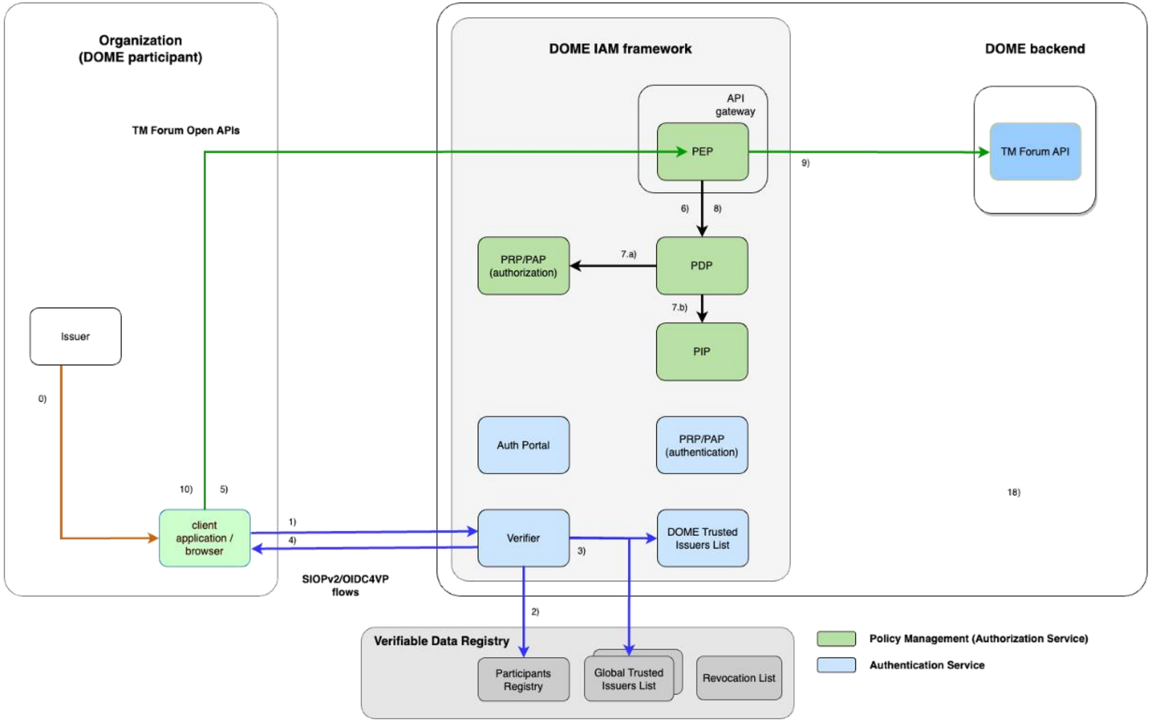
Invocation of TM Forum operations (M2M)

- An application from a DOME user organization (data/app provider or federated marketplace provider) already onboarded in DOME requests its authentication in DOME (step 1)
- The Verifier will check in the PRP/PAP what VCs to request: a) the VCs linked to roles meaningful for DOME the organization willing to authenticate should be a trusted issuer of if it actually had onboarded and b) some other VCs (steps 2-3). The application will check that the verifier belongs to a participant in the DOME ecosystem (step 4) and returns the requested VCs (step 5)
- The DOME Verifier verifies whether the VC was issued by an organization that is a trusted participant of the DOME ecosystem (step 6) and is a trusted issuer of the VCs meaningful for DOME (that is, VCs that only organizations that got on board of DOME can issue), also checks whether other VCs required were issued by trusted issuers (steps 7)
- If verifications is ok, it issues a token that is transmitted to the application (steps 8)
- Using the returned access token, the application invokes an DOME TM Forum API operation (step 9)
- The PEP proxy will verify whether the application with the claims (attributes) included in the VCs extracted from the access token is authorized to perform the given operation request (steps 10-12)
- If authorization is ok, the request is forwarded (step 13) and a response returned to the app (step 14)



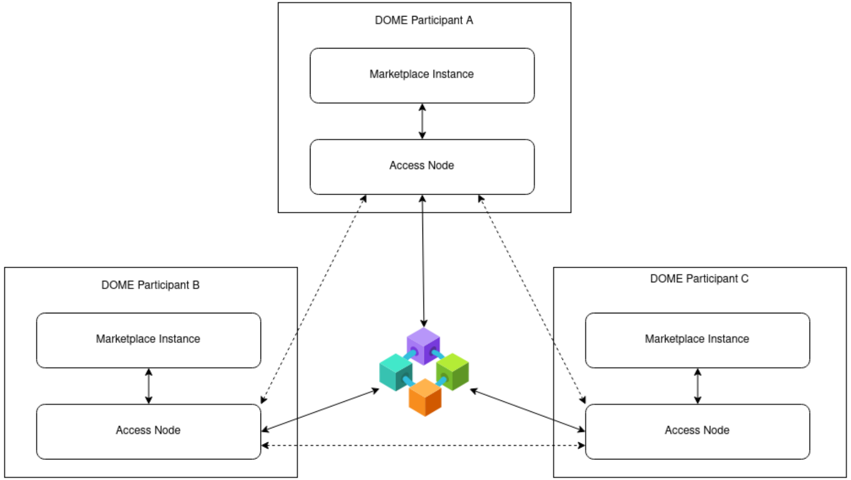
Invocation of TM Forum operations (simplified M2M)

- Step for the authentication can be simplified so that the application willing to access TM Forum operations exported by DOME sends via POST an authentication response with vp_token that contains the VCs it is well known that DOME will ask for
- The DOME Verifier verifies whether the VC was issued by an organization that is a trusted participant of the DOME ecosystem (step 2) and is a trusted issuer of the VCs meaningful for DOME (that is, VCs that only organizations that got on board of DOME can issue), also checks whether other VCs required were issued by trusted issuers (steps 3)
- If verifications is ok, it issues a token that is transmitted to the application (steps 4)
- Using the returned access token, the application invokes an DOME TM Forum API operation (step 5)
- The PEP proxy will verify whether the application with the claims (attributes) included in the VCs extracted from the access token is authorized to perform the given operation request (steps 6-8)
- If authorization is ok, the request is forwarded (step 9) and a response returned to the app (step 10)



The federation and replication layer

Persistence Layer Architecture

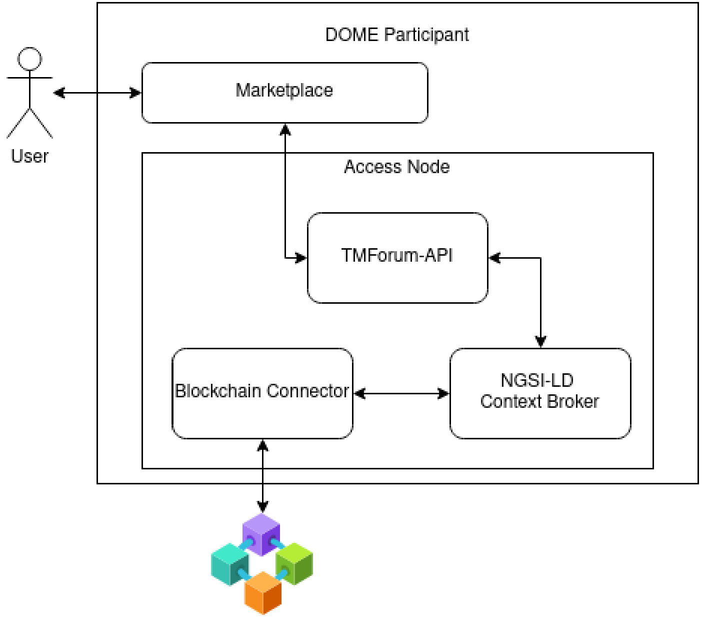


The Decentralized Persistence Layer operates through interconnected Access Node instances on a Blockchain.

Each participant deploys their unique Access Node instance and links it to the Blockchain using an individual address.

The Marketplace instances from different operators integrate via the APIs exposed by the Access node.

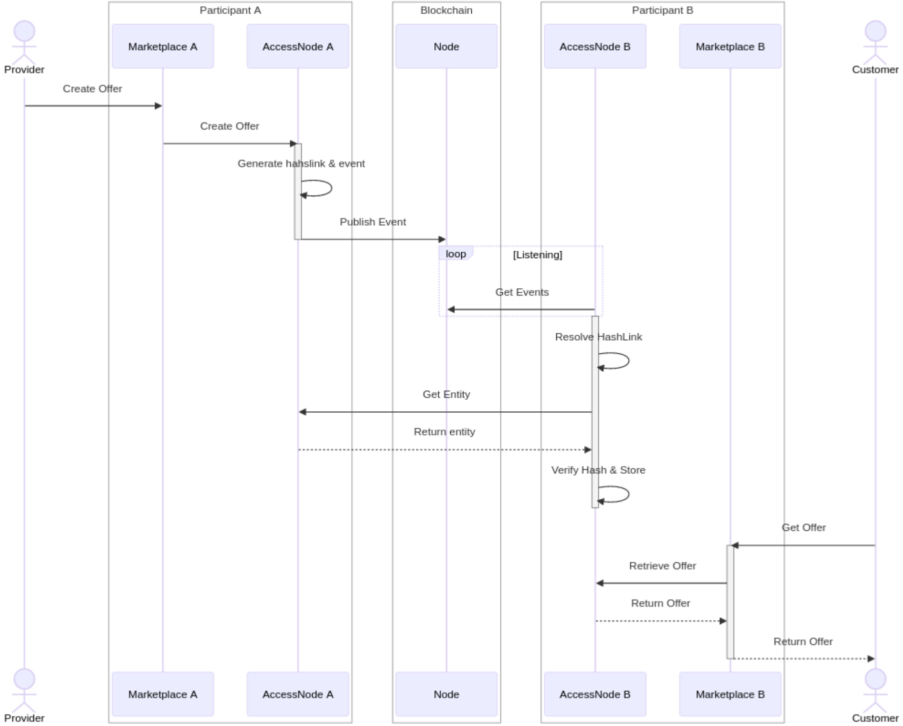
Access Node Architecture



The Access Node provides the following:

- Providing TMForum APIs to Marketplaces
- Local Persistence of Entities Managed via TMForum APIs
- Broadcasting Entity Events on the Blockchain
- Monitoring Entity Events from Other Instances
- Resolving Entity Events and Local Storage
- Offering NGSI-LD API to Other Access Nodes: Providing an interface that allows other Access Nodes to resolve events.

Interactions among components



Thank you!

DOME - Distributed Open Marketplace for
Cloud and Edge Services in Europe