ACCURATE

D5.1 Decentralized Data Space Infrastructure: Provide a robust, scalable, and resilient decentralized data space architecture designed for secure data sharing

Actual Submission Date: **10/11/2024**
Produced by: DAO: deltaDAO AG

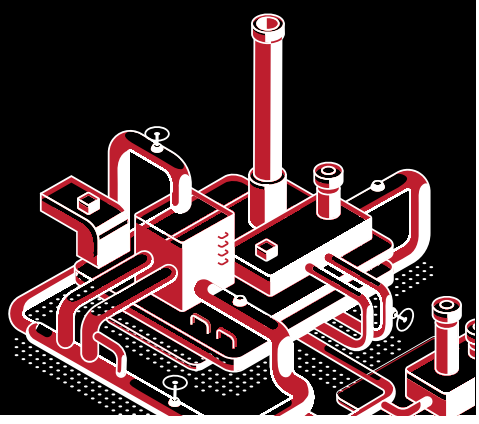
Accurate

https://accurateproject.eu/

HORIZON 1.0– 2023-12-04
ACCURATE — HORIZON-CL4-2023-TWIN-TRANSITION-01
Grant Agreement no.: 101138269
Start date of project: 01122023 - Duration: 36 months

Funded by the European Union

The ACCURATE project is funded by the European Union, under Grant Agreement number 101138269. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.



DELIVERABLE FACTSHEET

Deliverable D5.1	
Nature of the Deliverable:	Demonstrator
Due date of the Deliverable:	M8 – 31/07/2024
Actual Submission Date:	M10 – 11/10-2024
Produced by:	DAO
Contributors:	N/A
Work Package Leader Responsible:	DAO
Reviewed by:	IMT, HWR

Dissemination level	
	PU = Public
PP	PP = Restricted to other programme participants (including the EC)
	RE = Restricted to a group of the consortium (including the EC)
	CO = Confidential, only members of the consortium (including the EC)

Contents

Figures

Terms and abbreviations

ABAC	Attribute Based Access Control
AIA	European Artificial Intelligence Act
AML	Anti Money Laundering
API	Application Programming Interface
B2B	Business to Business
BIP	Bitcoin Improvement Proposal (Standard)
CAD	Compute Aided Design
CES	Gaia-X Credential Event Service
CFT	Combating the Finance of Terrorism
CtD	Compute-to-Data
DA	European Data Act
DDO	Decentralized Data Object
DGA	European Data Governance Act
DID	Decentralized Identifier
DSS	Decision Support System
DSSC	Data Space Support Centre
ECC	Elliptic-Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
EMT	Electronic Money Transfer
ERC	Ethereum Request for Comment (Ethereum Standard)
EVM	Ethereum Virtual Machine
FOSS	Free Open-Source Software
GDPR	General Data Protection Regulation
GXDCH	Gaia-X Digital Clearing House
HTTP	Hypertext Transfer Protocol
IoT	Internet of Things
IPFS	Interplanetary File System
KECCACK	Cryptographic algorithm used for hashing and signatures
MaaS	Manufacturing as a Service
MICAR	Market in Crypto Assets Regulation
NFT	Non-Fungible Token, ERC-721 Standard
npm	Package manager for the JavaScript programming language
OEM	Original Equipment Manufacturer
OIDC4VP	OpenID Connect For Verifiable Presentation
OPA	Open Policy Agent
ORDL	Open Digital Rights Language

PBKDF2	Password-Based Key Derivation Function
PCF	Product Carbon Footprint
PoS	Proof-of-Stake Consensus Mechanism
RSA	Public-Key Cryptosystem, Rivest-Shamir-Adleman
SECP256K1	Specific Elliptic Curve used in Public Key Cryptography
SME	Small and Medium Sized Enterprise
SSI	Self-Sovereign Identity
TEE	Trusted Execution Environment
TSP	Trust Service Provider
VC	Verifiable Credential
VDR	Verifiable Data Registry
VP	Verifiable Presentation
W3C	World Wide Web Consortium
XFSC	Eclipse Cross Federation Service Components

Public Summary

The ACCURATE project [1] is pioneering a decentralized data space infrastructure for the European manufacturing sector, aiming to enhance competitiveness, sustainability, and resilience across complex supply chains. At its core, the project leverages cutting-edge distributed ledger technology and adheres to Gaia-X principles [2] to create a secure, interoperable, sovereign data and digital service sharing ecosystem.

The infrastructure is built on a three-layer architecture:

i) The network and protocol Layer provides a robust foundation using an EVM-compatible distributed ledger, capable of smart contract execution (here based on Pontus-X [3] and Oasis Sapphire [4]), ensuring data integrity, high performance, privacy, scalability, and shared operation of the ecosystem base services used by all participants.
ii) The Middleware Layer, powered by Ocean Enterprise [5], offers essential services for digital service orchestration, data management, contracting, logging, and access controls.
iii) The Application and Services Layer delivers user-centric interfaces and integration capabilities, enabling manufacturers to seamlessly participate in the data space and operate it in a decentralized manner.

Key innovations include the implementation of Compute-to-Data features, allowing sensitive manufacturing data to be processed without republication and exposure of sensitive raw information, and the integration of the EUROe stablecoin [6] for instant and secure financial transactions within the ecosystem, covered by European electronic money regulation [7]. The project also incorporates advanced identity management solutions, with plans to implement a comprehensive Self-Sovereign Identity (SSI) system aligned with European Digital Identity standards [8].

ACCURATE's commitment to the Gaia-X Trust Framework [9] ensures compliance with Gaia-X standards, European data regulations and facilitates trust across the manufacturing ecosystem. By enabling secure data exchange and collaboration among OEMs, SMEs, and research institutions, the project supports innovation in areas such as supply chain management, manufacturing as a service, and human-centric decision support systems.

This decentralized data space infrastructure positions European manufacturers at the forefront of digital transformation, providing the tools needed to harness the power of data while maintaining sovereignty and security. As the project evolves, it promises to drive efficiency, foster innovation, and strengthen the competitiveness of the European manufacturing sector in the global market.

1 Introduction

1.1 About this Deliverable

This deliverable presents the comprehensive architecture and implementation details of the Decentralized Data Space Infrastructure developed for the ACCURATE project. It outlines the key components, technologies, and integration strategies employed to create a secure, interoperable, and sovereign data sharing ecosystem for the European manufacturing sector. The document serves as a technical reference for project partners, stakeholders, and future implementers of similar data space solutions.

1.2 Document Structure

This deliverable is structured as follows:

1. Introduction: Provides context and outlines the document structure.
2. Deliverable Preface: Contextualizes the document within the ACCURATE project and broader data economy.
3. Architecture Overview: Presents the high-level architecture of the data space infrastructure.
4. Network and Protocol Layer: Details the foundational blockchain and distributed ledger technologies.
5. Middleware Layer: Describes data management and access control components.
6. Application and Services Layer: Outlines user-facing interfaces and integration capabilities.
7. Gaia-X Trust Framework and Compliance Integration: Discusses alignment with European standards and regulations.
8. Future Developments: Explores planned enhancements and ongoing research areas.

1.3 Relation with Other Tasks and Deliverables

This deliverable is closely related to several ongoing tasks and upcoming deliverables within the ACCURATE project:

1. Task 5.3 - Enabling Technical Sovereign Data Usage (M14 – M26, Lead: DAO):
    - Focuses on developing a secure Compute-to-Data (CtD) environment.
    - Enables publication of data and algorithms for secure usage without compromising IP.
    - Facilitates federated learning and analytics while maintaining data privacy and sovereignty.
    - Related Deliverable: D5.2 - Compute-to-Data Environment
2. Task 5.4 - System Integration and Decentralization (M14 – M26, Lead: SIMAVI, Participants: ES, DAO):
    - Enables connection of decentralized data sources and supports various data types.
    - Implements logging infrastructure for data access, sharing, and usage events.
    - Contributes to the overall system integration described in this deliverable.
3. Task 6.2 - Establishing Trust with SSI, Secure Data Transaction and Automated Contracting Solutions (M14 – M26, Lead: DAO, Participants: IAO):

- Implements Self-Sovereign Identity (SSI) mechanisms for secure authentication and authorization.
- Develops automated contracting solutions for compliant data sharing.
- Ensures interoperability with other European data space initiatives.
- Related Deliverable: D5.3 - Sovereign Data Sharing

The infrastructure described in this deliverable provides the foundation upon which these tasks build, ensuring a cohesive and comprehensive data space solution for the manufacturing sector.

2 Deliverable Preface

2.1 ACCURATE overview

The ACCURATE project seeks to enhance the competitiveness of European manufacturing companies by improving their sustainability, performance stability, and resilience in the face of unforeseen events. To achieve this goal via Manufacturing as a Service and making data usage and collaboration more efficient, a decentralized data space infrastructure is crucial for enabling secure, efficient, and collaborative data sharing across the manufacturing value chain.

2.2 Pontus-X: The Foundation for ACCURATE's Data Space

Pontus-X is a pioneering Pan-European Business to Business (B2B) Digital Service Ecosystem designed for the seamless exchange of data, software, and infrastructure services. It serves as the cornerstone for the ACCURATE project's decentralized data space infrastructure, providing a robust foundation that aligns with European values and regulations.

Initiated by deltaDAO AG [10], EuProGigant, and numerous other ecosystem participants and lighthouse projects, the open-source Pontus-X software stack has evolved over the past three years, continuously demonstrating the viability and concept of data sovereignty and interoperable data spaces. Today, it stands as a widely adopted ecosystem, covering the needs of various domains and industries including manufacturing, industry 4.0, aviation, space, agriculture, cloud services, language models, AI services for SMEs, and energy data spaces.

Key characteristics of Pontus-X include:

1. First of its kind: Pontus-X is the first and largest fully decentralized and publicly available European B2B Digital Service Ecosystem.
2. Ecosystem of ecosystems: It advances the vision of a unified European Data Market, serving as a hub for multiple industry-specific data spaces.
3. Gaia-X compliance: Built on Gaia-X principles, ensuring data sovereignty, interoperability, and transparency and connected to the Gaia-X Digital Clearing Houses (GXDCH) [12], [13].
4. Smart contract integration: Utilizes smart contracts for secure and automated data exchange, logging, settlement, and service orchestration.

Pontus-X comprises several core components that together create a comprehensive data space solution:

1. Decentralized Infrastructure: Leverages distributed ledger technology to ensure data integrity, resilience, shared ecosystem operation, transparency, and security.
2. Data Exchange Services: Facilitates direct and sovereign data exchange between participants.
3. Identity and Trust Layer: Incorporates Self-Sovereign Identity (SSI) and W3C Verifiable Credentials for secure authentication and uses an open identity ecosystem, following the Gaia-X framework.

4. Metadata Catalogues: Smart contract-based catalogues for efficient resource discovery and shared catalogue integrity and availability.
5. Compute-to-Data: Enables privacy- and IP-preserving computations on sensitive data previously unavailable.
6. Monetization Layer: Supports sustainable business models through standardized monetization and settlement mechanisms.
7. Shared operation and economic incentives: Pontus-X base services can be operated by multiple operating institutions without a central point of failure, while incentivizing ecosystem participants to secure the jointly operated data space infrastructure.

The relevance and effectiveness of Pontus-X have been validated through the implementations of several Gaia-X lighthouse projects, including EuProGigant, Gaia-X 4 Future Mobility [14], COOPERANTS [15]. These projects have showcased that cross-data space interoperability and functional sovereign multi-company data exchange in an ecosystem is achievable today. In the manufacturing sector specifically, various use cases have been enabled and implemented with industry leaders such as Airbus, Software AG, and Gühring, demonstrating the effectiveness and economic benefit of data value creation in an open, fair, and transparent environment.

For the ACCURATE project, Pontus-X provides several crucial benefits:

1. Manufacturing-specific adaptations: Pontus-X can be tailored to meet specific needs for data spaces in the manufacturing sector, supporting ACCURATE's focus on Manufacturing as a Service (MaaS) value chains. These include:
    a) The ability to connect to IoT devices and machines used in manufacturing for data transfer and analysis, combined with a
    b) high degree of automation through smart contracting capabilities and automatable workflows which can be triggered by machines and autonomous agents to quickly react to changes in the manufacturing ecosystem
    c) Privacy-preserving computation on sensitive information and company secrets, such as machine or inventory data
    d) Privacy-preserving transactions between participants to protect company secrets
    e) Decentralized operation to avoid a single point of failure or control, which would harm resilience
    f) Support for on-demand and pay-per-use principles that scale well with Manufacturing as a Service needs and provide flexible cost models
    g) Real-time settlement and micropayments reduce third-party risks and increase efficiency, especially in cross-border business transactions.
    h) The ecosystem supports identities of machines and legal persons natively, allowing for direct integration of manufacturing systems.
2. Enhanced supply chain resilience: By enabling secure and efficient data sharing based on decentralized and resilient infrastructure, removing single point of failures, Pontus-X supports ACCURATE's goal of improving supply chain resilience in the face of disruptions. More detailed:
    a) The ecosystem is operated in a decentralized manner by multiple operating companies, which makes it more resilient against attacks and outages

b) The ecosystem provides important incentives for operating base services and keeping them highly available, which improves quality of service and resilience
c) The ecosystem rewards efficient service providers in a collaborative and competitive environment which benefits small and medium enterprises and a diverse ecosystem which is more resilient and distributed than a platform.
d) Individual manufacturing services work together through a peer-to-peer network, without a centralized intermediary
e) Pontus-X natively supports the business model of Manufacturing as a Service, Software as a Service, Data Providers, Software Providers and Compute-Providers
f) Automated data sharing and contracting is not bound to human interaction and allows automatic and coordinated recovery from shocks to the ecosystem
g) Ecosystem data is available to all participants and stored in a tamper-proof and Byzantine-Fault tolerant manner.

3. Interoperability: Facilitates seamless data exchange between different actors in the manufacturing ecosystem, from suppliers to end-users while supporting domain-specific semantic standards on the data plane and application level.
4. Regulatory compliance: Built with European regulations in mind, ensuring compliance with GDPR [16], the Data Act [17], and other relevant legislation.
5. Innovation enablement: Provides a platform for developing and deploying new manufacturing services and applications.

Based on the requirements engineering phase of the ACCURATE project, a production reference implementation is currently being built based on the OASIS network. This implementation leverages the ecosystem's proven track record in enabling data-driven collaboration, functional sovereign data sharing, monetization of services, privacy- and IP-preserving orchestration methods, and sustainable business models for digital service ecosystem operation.

By leveraging the capabilities of Pontus-X, the ACCURATE project is well-positioned to transform the European manufacturing sector, enhancing its resilience, sustainability, efficiency, and competitiveness in the global market via Manufacturing as a Service. The production reference implementation being built for ACCURATE based on Pontus-X will serve as a blueprint for future manufacturing data spaces, showcasing the potential of sovereign, interoperable, and value-creating digital ecosystems.

3 Architecture Overview

The architecture of the ACCURATE project's data space is the result of the requirements engineering phase in Task 5.1 and the experience and feedback loop from the various projects of the Pontus-X ecosystem. This process involved a multifaceted approach to ensure that the final design would not only meet the current needs of the manufacturing industry but also be adaptable to future challenges and regulatory landscapes.

Key aspects of the requirements engineering phase included:

1. Analysis of Gaia-X specifications: Ensuring alignment with European data infrastructure standards and principles.
2. Incorporation of conceptual models from the Data Space Support Centre (DSSC) [18]: Leveraging best practices in data space design and implementation.
3. Integration of requirements from pilot partners: Addressing real-world needs and use cases within the manufacturing sector.
4. Regulatory compliance considerations: Ensuring adherence to key European regulations such as the Data Act (DA), Data Governance Act (DGA) [19], AI Act (AIA) [20], GDPR, and MiCAR [21].
5. Futureproofing: Designing an architecture that can adapt to evolving technological and regulatory landscapes.

As illustrated in Figure 1 (below), the resulting architecture is a three-layer design that holistically addresses the complex needs of the manufacturing industry and its supply chain partners:

1. Network and Protocol Layer: This foundational layer provides the decentralized infrastructure and smart contract capabilities essential for implementing Gaia-X Federation Services. It ensures data sovereignty, resilience, transparency, scalability, inclusion, and security at the most fundamental level of the system.
2. Middleware Layer: Acting as the bridge between the network infrastructure and user-facing applications, this layer offers essential services for data management, access control, and system interoperability. It facilitates seamless data flow and enforces governance policies across the ecosystem. The middleware can be deployed in a cloud agnostic manner and on IoT devices to enable technical data sovereignty on the shop floor.
3. Application and Services Layer: The topmost layer focuses on user interaction and value creation. It encompasses business applications offered by Service Providers and tools for identification, publishing, discovery, and consumption of services. This layer translates the underlying technological capabilities into tangible benefits for end-users in the manufacturing sector.

Integral to the ACCURATE architecture is the integration of the Gaia-X Trust Framework [9] and compliance services, i.e., Gaia-X Registry Service [22], Gaia-X Notarization Service, Gaia-X Compliance Service [24], the Credential Event Service (CES) [25][26] and Trust Service Providers (TSPs) [27]. These services are explainer in chapter 6 of this document. The Gaia-X services validate that participants, services, and resources in the ecosystem adhere to minimum standards, including a uniform identification level with a high identity assurance level, commonly used semantics to

describe services and declare legally required and contractual components of the services provided by service providers. This integration ensures trust, interoperability, and sovereignty across the data space ecosystem. By incorporating key Gaia-X services and the ability to interact with multiple Gaia-X Digital Clearing Houses (GXDCH), the architecture establishes a foundation for standardized data exchange.

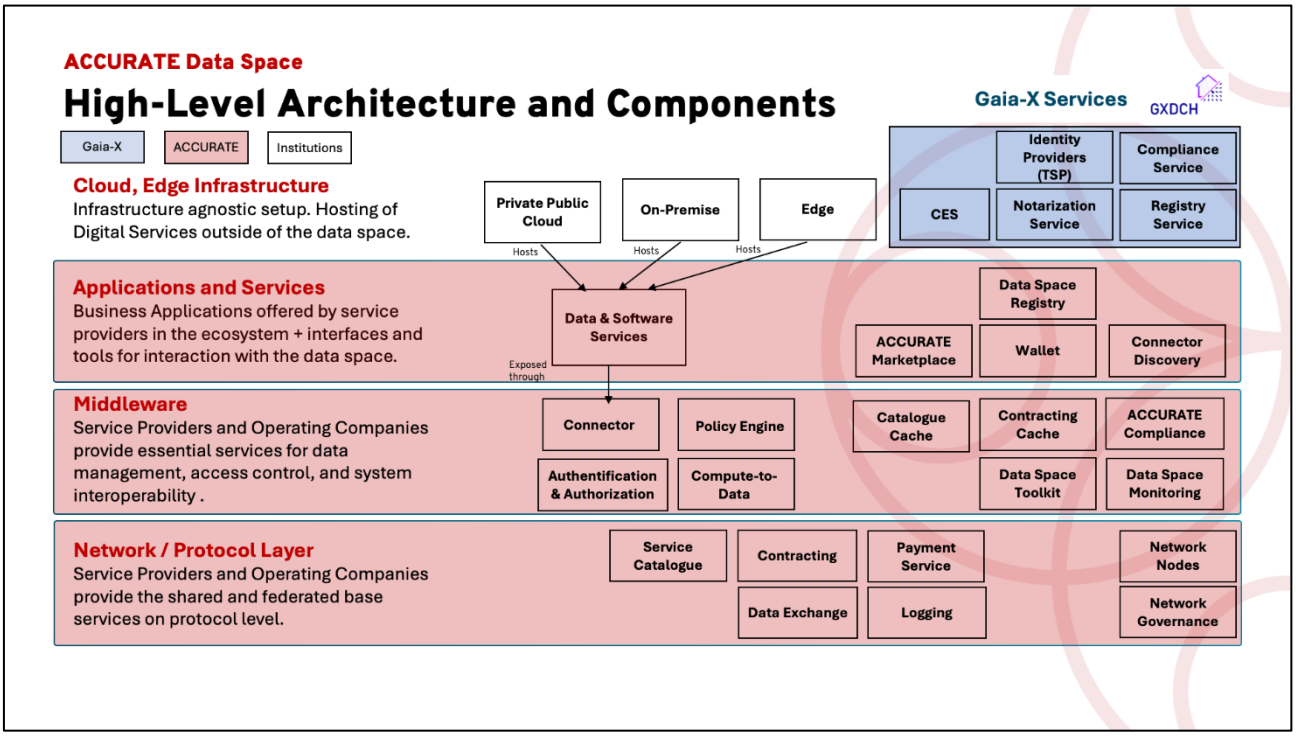


Figure 1: ACCURATE High-Level Architecture and Components (Source: deltaDAO)

This three-layer approach, including the Gaia-X Services integration, synergistically combines several key strengths:

- Decentralization: Leveraging distributed ledger technology to ensure data integrity, transparency, and resilience against single points of failure.
- Data Sovereignty: Empowering data owners with full control over their data, including how it's shared, used, and processed within the ecosystem. The data is always hosted outside of the data space, and exchanged, peer-to-peer.
- User-Centricity: Focusing on intuitive and value-adding applications that address real-world manufacturing challenges.
- Interoperability: Ensuring smooth communication and data exchange between different systems, crucial for complex manufacturing supply chains.
- Scalability: Designing each layer to handle growing data volumes and increasing numbers of participants.
- Security: Implementing robust security measures at every level to protect sensitive manufacturing data.

By adopting this architecture, the ACCURATE project aims to create a resilient, secure, scalable, and interoperable data space ecosystem. This ecosystem will empower manufacturers to harness the full potential of their data, foster innovation, enhance supply chain resilience, offer, and utilize Manufacturing as a Service, and ultimately increase the competitiveness of the European manufacturing sector in the global market. A more detailed breakdown of the technical architecture and the relations of the basic components is given in Figure 2.

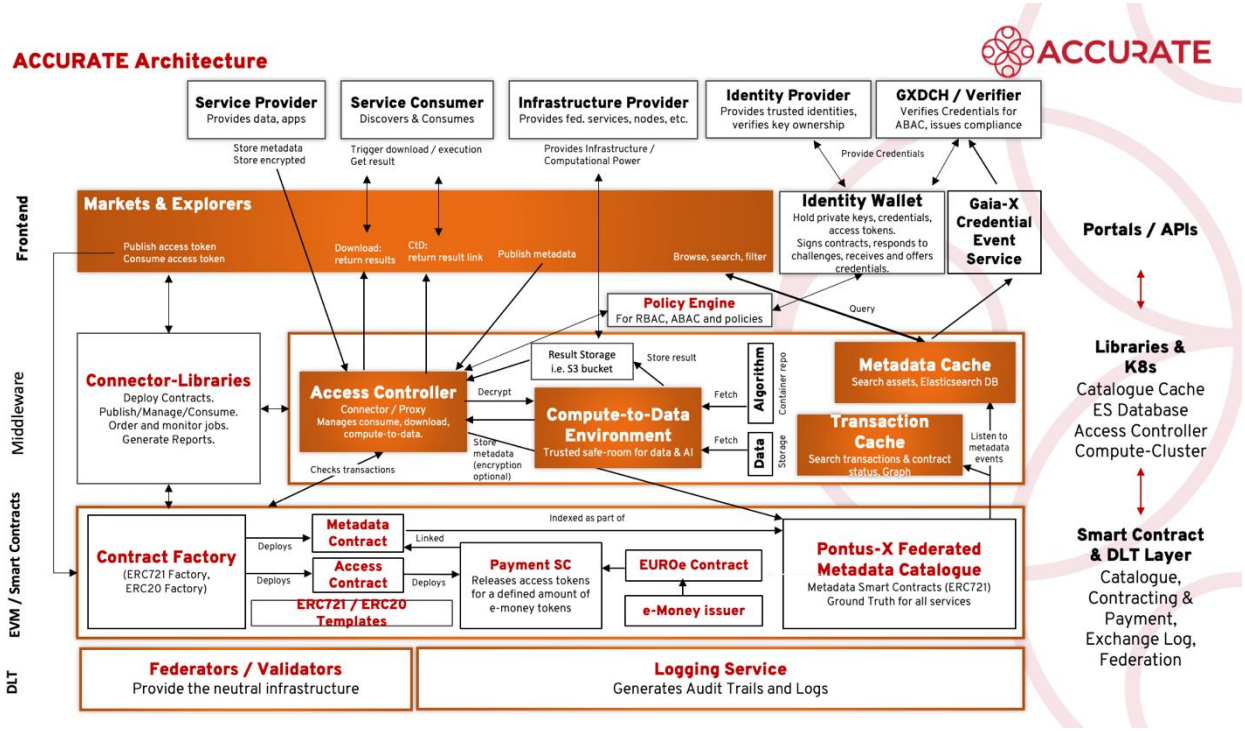


Figure 2: ACCURATE Technical Architecture (Source: deltaDAO)

The following chapters will describe into the specifics of each layer, exploring the technologies, protocols, and services that bring this architecture to life and drive the vision of the ACCURATE project.

4 Network and Protocol Layer

The Network and Protocol Layer forms the foundation of the digital solution for ACCURATE, providing a federated and secure infrastructure for data exchange and collaboration. This layer enables Service Providers and Operating Companies to offer shared and federated base services at the protocol level, ensuring a decentralized, transparent, and trustworthy ecosystem.

Key components of this layer include:

1. Distributed Ledger: An EVM-compatible distributed ledger serves as the backbone of our solution, offering a scalable and transparent infrastructure operable by multiple entities. This component in the reference implementation is based on the Oasis Protocol but can be easily customized and implemented on other networks to avoid lock-in effects.
2. Network Nodes and Governance: A decentralized network of nodes ensures system resilience, data integrity in a distributed system and consensus. The federated setup allows multiple data space participants to operate nodes, preventing single points of control and fostering a collaborative trusted environment.
3. Logging Service [28]: This service logs data exchange and contracting events on the distributed ledger, providing a comprehensive audit trail and enhancing transparency within the data space.
4. Smart Contracts: These play a pivotal role in enabling Gaia-X federation services and ensuring the integrity and functionality of the data space. The smart contract implementation is based on Ocean Enterprise / Ocean Protocol as well as EUROe to enable settlement with European regulated electronic money.

The Network and Protocol Layer is designed to avoid dependency on a single point of control or failure, achieving highly available core services and maximum metadata integrity. It supports the core principles of data sovereignty, allowing participants to maintain control over their data and decide how it's shared and used within the ecosystem.

The following subchapters will provide detailed insights into the distributed ledger implementation based on the Oasis Protocol [29], and the smart contract framework leveraging Ocean Enterprise / Ocean Protocol [5].

4.1 Distributed Ledger

The distributed ledger serves as the decentralized backbone of the ACCURATE data space. Following a comprehensive requirement engineering phase, a thorough evaluation of various distributed ledger technologies was conducted to identify the most suitable solution for the project's needs. This evaluation process led to the decision to transition from a previous Polygon-based network to a more advanced distributed ledger based on the Oasis Network.

4.1.1 Evaluation Process

The selection of the new distributed ledger technology involved a rigorous assessment of multiple blockchain networks, including but not limited to Oasis Network [5][29], Polygon [30], Polkadot

[31], Avalanche [32], Hyperledger [33], and Arbitrum [34]. The evaluation was based on several key criteria essential for meeting the diverse needs of the ACCURATE ecosystem:

1. Selective Privacy [35] and Custom Fee Token: The ability to provide granular privacy controls and support custom tokens for transaction fees was crucial for supporting diverse use cases within the manufacturing sector.
2. Development Tools and Ecosystem Maturity: A mature ecosystem with robust development tools, libraries, and documentation was essential for efficient development and integration.
3. Network Scalability: High throughput capabilities and support for off-chain computation were necessary to handle the large volumes of data expected in a manufacturing data space.
4. EVM Compatibility: Compatibility with the Ethereum Virtual Machine was important for ensuring easy integration with existing Ethereum-based applications and tools.
5. Governance Model: A decentralized, on-chain governance model was sought to ensure transparency, security, and community participation in network decisions.
6. Shared Vision of an Open Data Economy: Alignment with the principles of openness, decentralization, and data sovereignty was considered crucial for long-term collaboration and growth.

After careful consideration of these criteria, the Oasis Network open-source software components emerged as the best fit for the ACCURATE project. Its unique combination of scalability, privacy-first design, versatility, and alignment with the vision of an open data economy made it the ideal choice for building a secure and efficient manufacturing data space.

4.1.2 Oasis Network Overview

The Oasis Network is a Layer 1 decentralized blockchain network designed to prioritize scalability, privacy, and versatility. It features a unique two-layer architecture comprising the consensus layer and the ParaTime layer [36], which sets it apart from other blockchain networks and makes it particularly suitable for the ACCURATE project's needs in the manufacturing sector.

Key features of the Oasis Network include:

1. Two-Layer Architecture:
    - Consensus Layer: A high-throughput, secure, proof-of-stake (PoS) consensus mechanism run by a decentralized set of validator nodes.
    - ParaTime Layer: Hosts multiple parallel runtimes (ParaTimes), each representing a replicated compute environment with a shared state.
2. Scalability:
    - High Throughput: The architecture allows for high transaction speeds and throughput, supporting large-scale applications without performance degradation.
    - Parallel Processing: Multiple ParaTimes can process transactions simultaneously, ensuring that complex workloads on one ParaTime do not slow down simpler transactions on another.
3. Privacy-First Design:

    - Confidential Compute: ParaTimes support confidential smart contracts using Trusted Execution Environments (TEEs), ensuring that processed data remains confidential, even from node operators.
    - Selective Disclosure: Allows for granular control over data privacy, enabling secure sharing of sensitive manufacturing data.
4. Versatility:
    - EVM Compatibility: Fully compatible with the Ethereum Virtual Machine, enabling seamless integration with existing Ethereum-based applications and tools.
    - Flexible Development: Developers can create ParaTimes tailored to specific application needs, whether they require high security, different runtime environments, or specific governance models.
5. Governance:
    - On-Chain Governance: Implements a decentralized on-chain governance model, promoting transparency and community participation in network decisions.
6. Custom Fee Tokens:
    - Supports the use of custom tokens for transaction fees, allowing for the integration of EUROe as the fee token within the ACCURATE ecosystem.

4.2 Benefits for ACCURATE

The adoption of the Oasis Network as the distributed ledger for ACCURATE brings several key advantages:

1. Enhanced Data Privacy: The confidential compute feature aligns perfectly with the need for secure handling of sensitive manufacturing data, allowing for collaborative analysis without compromising data privacy.
2. Scalability for Industrial IoT: The high throughput and parallel processing capabilities can support the large volumes of data generated by industrial IoT devices in manufacturing environments.
3. Customizable ParaTimes: Allows for the creation of manufacturing specific ParaTimes, tailored to the unique needs of different segments of the manufacturing supply chain.
4. Interoperability: EVM compatibility ensures easy integration with existing tools and applications used in the manufacturing sector, reducing barriers to adoption.
5. Futureproofing: The flexible architecture of the Oasis Network allows for ongoing adaptation to evolving needs in the manufacturing data space, ensuring long-term viability of the ACCURATE solution.
6. Sustainable Operation: The proof-of-stake consensus mechanism aligns with sustainability goals in the manufacturing sector, offering an energy-efficient alternative to traditional blockchain networks.

By leveraging the advanced features of the Oasis Network, the ACCURATE project establishes a distributed ledger infrastructure capable of meeting the complex demands of a secure, scalable, and privacy-preserving manufacturing data space. This foundation enables the development of innovative applications and use cases that can drive efficiency, collaboration, and innovation across the European manufacturing ecosystem.

4.2.1 Network Nodes and Governance

The network nodes and governance structure of the ACCURATE project build upon the principles established in earlier network generations while incorporating enhancements offered by the Oasis Network to meet the project's evolving needs. This subchapter details the transition of validators, the current governance structure, and plans for future expansion.

4.2.2 Validator Migration and Expansion

Following the transition to the Oasis Network components, previously existing operating institutions and their validators have successfully migrated to the new infrastructure. This migration ensures continuity in network operation and maintains the trust and experience built within the ecosystem. The current validator set includes a diverse group of organizations from across Europe, including companies such as Arsys, deltaDAO, Exaion/Energy de France, EuProGigant, A1 Exoscale, IONOS, State Library of Berlin, AIRBUS Defense and Space GmbH, Software AG, University de Lleida, COOPERANTS, and WOBCOM GmbH.

As the ACCURATE project progresses, there are plans to expand the validator set by incorporating new validators from the ACCURATE consortium. This gradual expansion will enhance the network's decentralization, increase its geographical distribution, and bring in sector-specific expertise from the manufacturing industry. The inclusion of ACCURATE consortium members as validators will strengthen the alignment between the network's governance and the specific needs of the manufacturing data space.

4.2.3 Decentralized Network Structure

The ACCURATE network maintains a decentralized structure where multiple data space participants operate nodes. This approach prevents single points of control and fosters a truly collaborative environment. Key aspects of this structure include:

- Distributed Responsibility: Validators are spread across different organizations and geographical locations, enhancing network resilience, and reducing the risk of centralized control.
- Collaborative Decision-Making: The diverse set of validators contributes to a more robust and representative decision-making process.
- Sector-Specific Expertise: As validators from the ACCURATE consortium join, they will bring valuable insights from the manufacturing sector, ensuring the network's development aligns closely with industry needs.

4.2.4 Governance Model

The governance model for the ACCURATE network builds on the strengths of both the Pontus-X [37] and Oasis Network approaches:

1. On-Chain Voting: The network utilizes on-chain voting mechanisms for critical decisions, such as adding or removing validators, protocol upgrades, and parameter changes. This ensures transparent and auditable governance processes.

2. Proposal System: Any validator can submit proposals for network improvements or changes. These proposals are then voted on by the validator set.
3. Stake-Weighted Voting: Voting power can be proportional to the number of tokens staked by each validator, ensuring that those with the most at stake, financial involvement, contributing to the security of the network, have a proportional say in network decisions.
4. Delegation: Token holders can delegate their tokens to validators, allowing for broader participation in network governance without the need to run a validator node.
5. Transparent Decision Records: All governance decisions are recorded on-chain, providing a transparent and immutable record of the network's evolution.

4.2.5 Validator Responsibilities

Validators in the ACCURATE network play a crucial role in maintaining the network's integrity and performance. Their responsibilities include:

- Block Production and Validation: Participating in the consensus process to produce and validate new blocks.
- Network Security: Ensuring the security of their nodes to protect the network from potential attacks.
- Governance Participation: Actively participating in governance decisions through proposal submission and voting.
- Community Engagement: Engaging with the broader ACCURATE community to gather feedback and represent diverse perspectives in governance decisions.
- Storage of a jointly secured database: Catalogue and logging information is distributed to all nodes in the network and secured against corruption and manipulation.

4.3 Future Developments

As the ACCURATE project evolves, several developments are planned for the network nodes and governance structure:

1. Gradual Incorporation of ACCURATE Consortium Validators: Over time, members of the ACCURATE consortium will be onboarded as validators, bringing their manufacturing expertise to the network governance.
2. Refinement of Governance Processes: The governance model will be continuously evaluated and refined based on the specific needs of the manufacturing data space and feedback from participants.
3. Enhanced Tooling for Validator Operations: Development of specialized tools to support validators in their operations and decision-making processes. One key initiative will be the implementation of a decentralized voting application on the Oasis Sapphire platform. This tool will enable gasless voting with flexible access control, customizable voting parameters, and support for both identified and anonymous voting, aligning with the diverse governance needs of different stakeholder groups within the ACCURATE ecosystem. The application will facilitate proposal discussions, notifications, and customizable decision thresholds, enhancing the efficiency and inclusivity of governance activities.

By maintaining a robust, decentralized, and continuously evolving governance structure, the ACCURATE network ensures that it remains responsive to the needs of the manufacturing data space while upholding the principles of transparency, security, and collaborative decision-making.

4.3.1 Data Contract Logging Service

The Data Contract Logging Service is a critical component of the Network and Protocol Layer, ensuring transparency and auditability within the ACCURATE ecosystem.

Key features include:

- Comprehensive Logging: All contracting events are logged by the distributed ledger, documenting the contract opt-in of consumers in specified service contracts with service providers.
- Public Visibility: Event logging is public by default and can be observed by all participants of the data space, enhancing transparency.
- Private Execution Logs: While contract events are public, the execution of data exchange is logged privately on the consumer and service provider side at the component level.
- Audit Trail: The logging service provides a comprehensive audit trail, useful for provenance, compliance audits, and dispute resolution.
- Logging Explorer: To enhance the accessibility and usability of the logged data, the ACCURATE project implements a Logging Explorer that leverages the Oasis Nexus API. This integration provides a user-friendly interface for accessing, querying, and analyzing the logged data from the Pontus-X test network.

This logging service plays a crucial role in maintaining trust and accountability within the ACCURATE ecosystem, supporting the project's commitment to transparent and secure data sharing in the manufacturing sector.

4.4 Smart Contracts

Smart contracts play a pivotal role in enabling Gaia-X federation services and ensuring the integrity and functionality of the ACCURATE data space. The project leverages Ocean Protocol v4 for its core smart contract infrastructure, complemented by the EUROe stablecoin for monetization and settlement. This combination provides a robust foundation for secure, transparent, and efficient data exchange in the manufacturing sector.

4.4.1 Ocean Enterprise / Ocean Protocol Framework overview

Ocean Protocol [38] is an open-source software framework that provides a scalable, decentralized data infrastructure, federated learning and analytics orchestration layer and a set of tools that enable developers to build data marketplaces, AI applications, and other data-driven solutions and data-driven value chains and pipelines. Its primary purpose is to serve as a reusable foundation for various applications, rather than addressing a specific need as a standalone project, thus fitting the definition of an open-source software framework.

Ocean Protocol comprises several key components (see Figure 3) that collectively form its open-source software framework, allowing developers to create decentralized data, software and infrastructure marketplaces and applications (see Ocean Protocol Architecture Overview) [39].

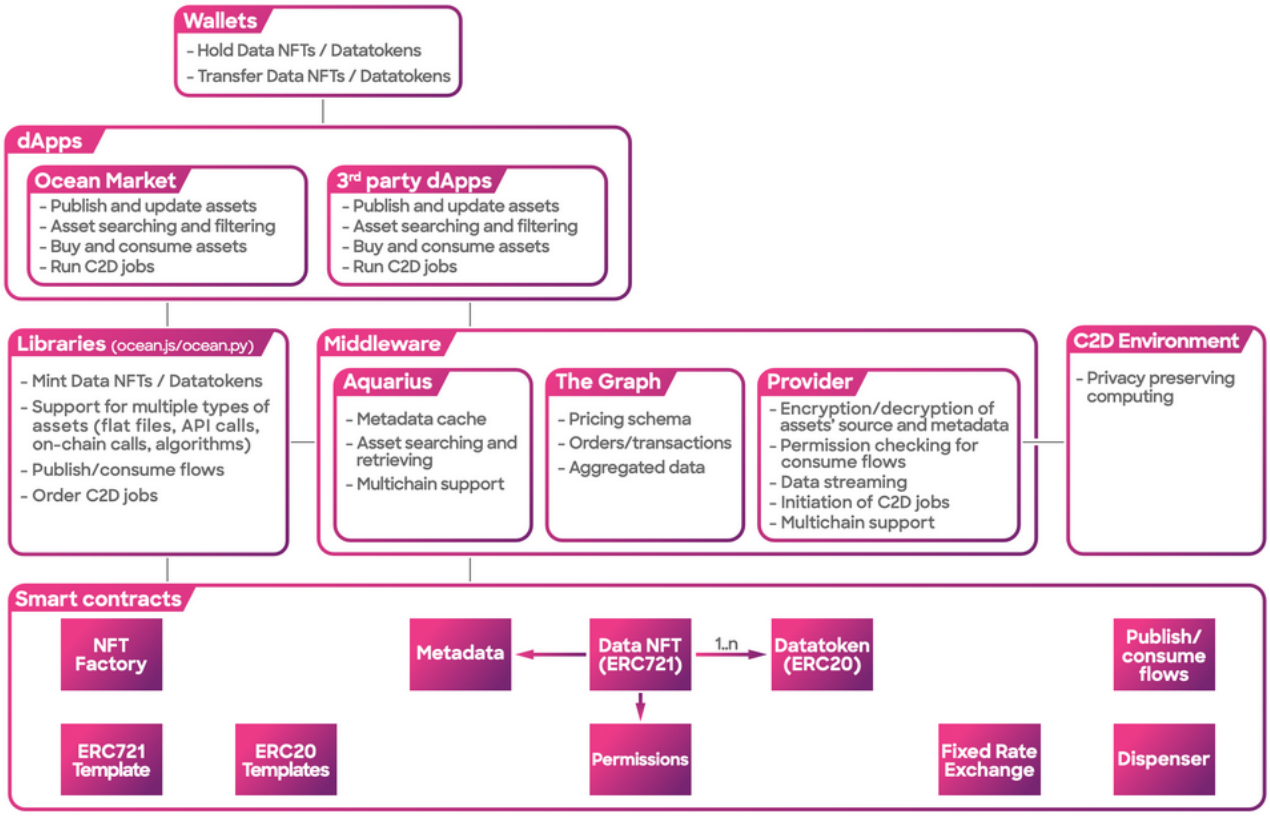


Figure 3: Ocean Protocol Architecture (Source: Ocean Protocol)

Ocean Protocol utilizes Solidity-based smart contracts (see Figure 4) in any EVM-compatible environment to automate and manage interactions between service providers, consumers, and other ecosystem participants. These contracts ensure resilient, secure, transparent, and trustless interactions and transactions. Smart contracts allow the storage and management of metadata and the settlement of commercial/non-commercial agreements for the use of data, software, and infrastructure offerings.

Key features of Ocean Protocol v4 smart contracts include:

1. Service Catalogue:
    - Stores self-descriptions of all resources available in the data space, based on Decentralized Identifiers (DIDs), a well-established standard by W3C [40].
    - Provides a decentralized, tamper-resistant "single source of truth" for asset information.
    - Facilitates efficient resource discovery and utilization across the ACCURATE ecosystem and beyond.
2. Sovereign Data Exchange:
    - Utilizes standardized Data Contract templates for negotiating and stipulating data exchange agreements.

- Ensures data sovereignty by allowing participants to control data sharing terms and conditions.
- Integrates with connectors to enforce access rights based on smart contract events.

3. Connector Discovery:
   - Integrated with the service catalogue to enable discovery of active connectors and service endpoints.
   - Facilitates smooth interactions between participants in the ACCURATE ecosystem.
4. Data Contracting:
   - Enables decentralized creation, negotiation, and enforcement of data exchange agreements.
   - Utilizes contract templates and a contract factory for standardized yet flexible agreement creation.
5. Authentication and Authorization:
   - Implements attribute-based access controls (ABAC) using cryptographically signed messages and credential exchanges.
   - Ensures high security and flexibility in access management.
6. Access Tokens:
   - Implements ERC-20 tokens [41] representing access rights to specific services.
   - Enables provenance tracking, audit trails, and interoperability through the ERC-20 standard.
7. Pricing and Settlement:
   - Enables automated fee collection and distribution to service providers, infrastructure providers, and ecosystem participants.
   - Allows for customization of fee collectors to support sustainable business models for all actors.
   - Supports on-chain and off-chain settlement options, including integration with electronic money like EUROe.

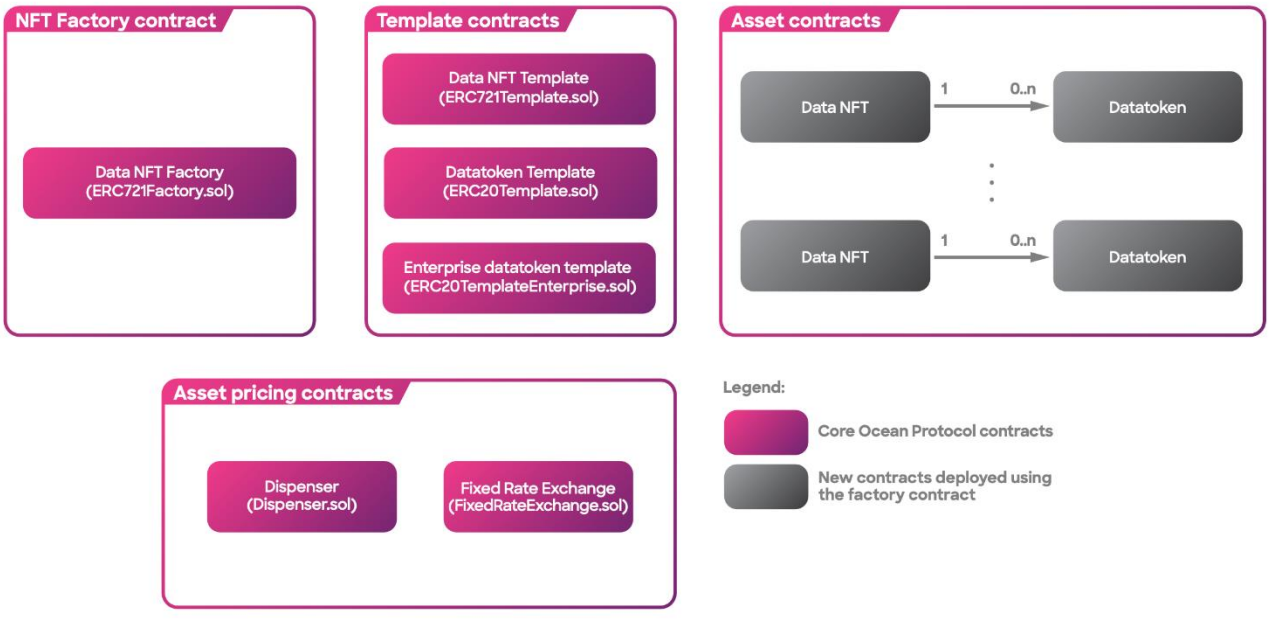


Figure 4: Ocean Protocol Smart Contracts and Access Tokens (source: Ocean Protocol)

4.5 EUROe Stablecoin

To support monetization, settlement and gas fee provision within the ACCURATE data space, the project integrates the EUROe stablecoin. EUROe is an EU-regulated e-money token issued by Finish Fintech Company Membrane Finance that provides a stable, compliant medium of exchange for data transactions.

Key aspects of EUROe stablecoin integration include:

1. Regulatory Compliance:
    - Regulated as Electronic Money Transfer (EMT) by the Finnish Financial Supervisory Authority [42].
    - EU-passported for issuance and redemption by licensed financial institutions in Europe.
    - Fully compliant with upcoming MiCA regulations, ensuring future proofing of the ACCURATE ecosystem.
2. Stability and Security:
    - Always redeemable 1:1 with Euros.
    - Fully backed by reserves held in European banks, with quarterly audited reports.
    - Implements precautionary measures to honor claims even in case of blockchain failure.
3. Versatility:
    - Blockchain-agnostic, supporting multiple networks including Ethereum, Polygon, Avalanche, and Arbitrum.
    - Can be integrated with private blockchains or proprietary systems.
    - Supports programmatic access through APIs for minting and burning.
4. Smart Contract Integration:
    - Implements the ERC-20 standard, ensuring compatibility with existing smart contract systems.
    - Enables programmable money features within the ACCURATE ecosystem.
5. Cross-chain Functionality:
    - Provides near-instant, no-slippage cross-chain bridging of EUROe.
    - Enhances interoperability within the ACCURATE ecosystem and beyond.
6. AML and CFT Compliance:
    - Adheres to strict AML (Anti-Money Laundering) and CFT (Countering the Financing of Terrorism) regulations.
    - Performs due diligence on customers and screens wallets/addresses for compliance.

Integration of EUROe in the ACCURATE project offers several benefits:

1. Stable Value: Provides a stable medium of exchange, crucial for predictable pricing of data services.
2. Regulatory Alignment: Ensures compliance with EU financial regulations, building trust in the ecosystem.
3. Seamless Transactions: Enables efficient, programmable transactions within the data space.
4. Cross-chain Capabilities: Supports potential future expansion to other blockchain networks.

5 Middleware Layer

The Middleware Layer of the ACCURATE data space solution serves as a bridge between the foundational Network and Protocol Layer and the user-facing Application and Services Layer. This layer houses the components that enable data management, access controls, and system interoperability. Building upon the smart contracts discussed in the previous chapter, the Middleware Layer leverages the Ocean Protocol open-source software framework to provide additional powerful tools for developers, enabling integration and interaction with the protocol, and components.

The following sections detail the key components of the Middleware Layer, based on the Ocean Enterprise / Ocean Protocol framework, and adapted for the ACCURATE project's needs.

5.1 Metadata Cache (Aquarius)

The Metadata Cache, implemented through Aquarius in the ACCURATE project, is a crucial component for managing and discovering data assets within the ecosystem. Aquarius serves as a highly performant local catalogue cache, based on Elastic Search (see Figure 5), that tracks and caches metadata from the Pontus-X Testnet, where the Ocean Protocol smart contracts are deployed. It avoids unnecessary traffic while adding to the scalability of the ecosystem.

Key features and functions of Aquarius include:

1. Metadata Caching:
    - Stores metadata from multiple blockchains off-chain in an Elasticsearch database.
    - Provides a scalable solution for efficient metadata retrieval and querying.
2. Event Monitoring:
    - Continuously monitors for updated Metadata and newly created Metadata events on the blockchain, corresponding with updates in the federated catalogue.
    - Processes these events and updates the database in real-time, ensuring up-to-date metadata.
3. Easy Query Access:
    - Offers a REST API for convenient access to metadata without the need to scan the blockchain directly.
    - Enables efficient search functionality within decentralized applications (dApps) in the ACCURATE ecosystem.
4. Events Monitor:
    - Runs continually to retrieve and index chain metadata.
    - Saves results into the Elasticsearch database for quick access.
5. Configurable Components:
    - Allows customization of various features including used smart contracts used for Metadata storage, Decryptor class, allowed publishers, lifecycle management settings, and start blocks indicating the begin of relevant events to be tracked and cached.

Aquarius leverages the following technologies:

- Python: The main programming language used in Aquarius development.
- Flask: A Python framework used to construct the Aquarius API.
- Elasticsearch: A search and analytics engine used for efficient data indexing and retrieval.
- REST API: Provides interoperability between computer systems on the internet.

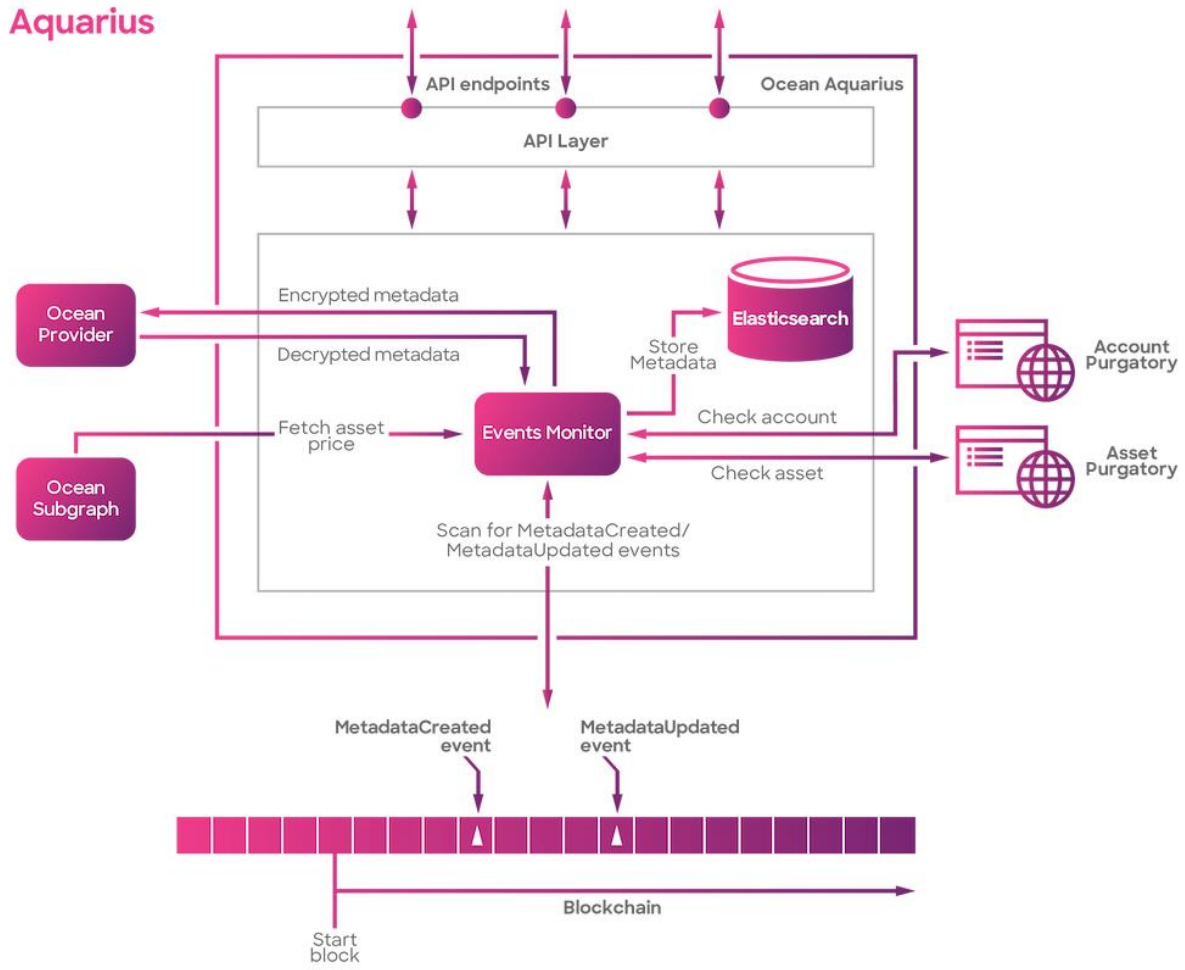


Figure 5: Aquarius Catalogue Cache Architecture

By implementing Aquarius as the Metadata Cache (see Figure 5) [42], the ACCURATE project ensures efficient metadata management and discovery across its decentralized data infrastructure. This component plays a crucial role in enabling seamless data asset discovery and management within the manufacturing data space.

Full Documentation here [42].

5.2 Access Controller (Connector)

In the ACCURATE project, the Access Controller, implemented through the Ocean Provider component, serves as a crucial element in managing and securing access to data services. The Provider is a REST API specifically designed for the provision of data services, acting as a proxy that

encrypts and decrypts metadata and access information for data assets. The flows for publication and consumption are shown in Figure 6.

Key features and functions of the Provider include:

1. Data Access Control:
    - Acts as the sole component in the Ocean Protocol stack with direct access to the data.
    - Performs on-chain checks to verify buyer permissions and payments before granting access.
2. Security and Encryption:
    - Encrypts URLs and metadata during the publishing process, ensuring data security during initial upload.
    - Decrypts URLs when datasets are downloaded, or compute jobs are initiated.
    - Streams data directly to buyers without revealing asset URLs, providing an additional layer of security.
3. Compute Services:
    - Establishes connections to the Compute-to-Data (CtD) environment, enabling data computation and manipulation within the Ocean Protocol stack.
4. Publishing and Consumption Flows:
    - In the publishing process, encrypts the Decentralized Data Object (DDO) [43][44]using its private key and stores it on the blockchain.
    - During consumption, decrypts the DDO and fetches data from the source used by the data publisher after a consumer purchases a data token.
5. Fine-grained Access Controls:
    - Supports explicit access control options with the use of data tokens and SSI verifier solutions.
    - Integrates with Keycloak for enhanced identity management.
6. Diverse Data Source Support:
    - Allows provisioning of data from various sources, including static files, decentralized storage (IPFS, Arweave), databases, and APIs.

The Provider utilizes the following technologies:

- Python: The main programming language used in Provider development.
- Flask: A Python framework used to construct the Provider API.
- HTTP Server: Responds to HTTP requests from clients, facilitating data and information exchange over the internet.

By implementing the Provider as the Access Controller, the ACCURATE project ensures secure, controlled, and efficient access to data services within its ecosystem. This component plays a vital role in maintaining data sovereignty, enforcing access policies, and enabling secure data exchange in the manufacturing data space.

Fully documentation [45]: Here

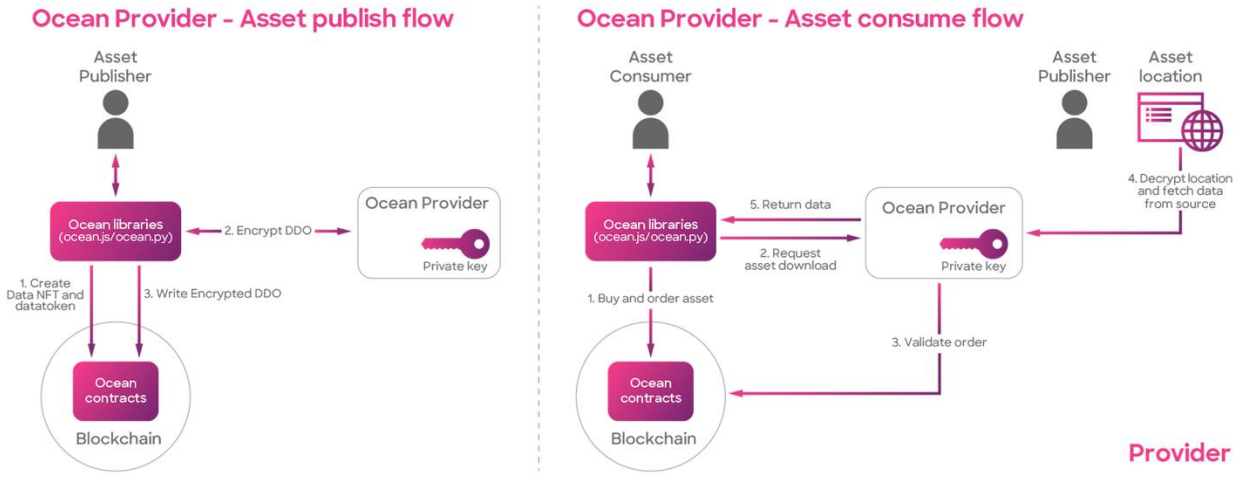


Figure 6: Ocean Provider Access Controller Flows (Source: Ocean Protocol)

5.3 Policy Engine

The Policy Engine is a component that will be included in the Connector to verify data usage and access policies as part of the Verifiable Credentials. It ensures that all data exchanges within the ACCURATE ecosystem adhere to pre-defined rules, including the processing of REGO and ODRL policies, thereby maintaining compliance and trust between participants.

The Policy Engine will be developed as part of the SSI integration in Task 6.2 and will consider software stacks from Eclipse Cross Federation Service Components (XFSC) [46], walt.id [47], Sphereon and others for this integration. Policies can be expressed as ODRL (Open Digital Rights Language) [48] or REGO through an Open Policy Agent (OPA) [49].

5.4 Compute-to-Data

Compute-to-Data (CtD) is a privacy-preserving feature built on Kubernetes and designed to be highly infrastructure agnostic (see Figures 7 and 8). It allows data to remain secure on the data provider's premises while still enabling consumers to use the data for computations and analysis (see Figure 8). This innovative approach is particularly valuable for the ACCURATE project, where sensitive manufacturing data often needs to be processed without compromising data sovereignty or intellectual property.

Key features and benefits of Compute-to-Data include:

1. Secure Data Processing:
    - Enables data processing without moving sensitive raw data from its original location.
    - Preserves data privacy and reduces data transmission costs.
    - Allows data owners to grant compute access while maintaining full control over their data assets.
2. Data Sovereignty:

- Upholds the principle of data sovereignty by ensuring data remains under the control of the data provider.
- Supports compliance with data protection regulations, crucial for the manufacturing sector.

3. Collaborative Innovation:
   - Facilitates collaborative scenarios, such as training machine learning models across multiple datasets from different data providers.
   - Enables analytics on data containing intellectual property without compromising confidentiality.
   - Fosters innovation and cooperation in the manufacturing ecosystem while protecting sensitive information.
4. Flexibility and Scalability:
   - Built on Kubernetes, ensuring adaptability to various infrastructure environments.
   - Supports edge and IoT devices, extending computational capabilities to diverse manufacturing settings.
5. Integrated Audit Trail:
   - Leverages smart contracts for creating data NFTs and data tokens.
   - Records all activities related to data services (e.g., publishing, creating licenses, usage) on the blockchain, providing immutable and tamper-proof audit trails.
6. Manufacturing-Specific Applications:
   - Enables secure analysis of proprietary manufacturing processes across the supply chain.
   - Supports collaborative research and development initiatives without exposing sensitive industrial data.
   - Facilitates benchmarking and optimization studies while protecting competitive advantages.

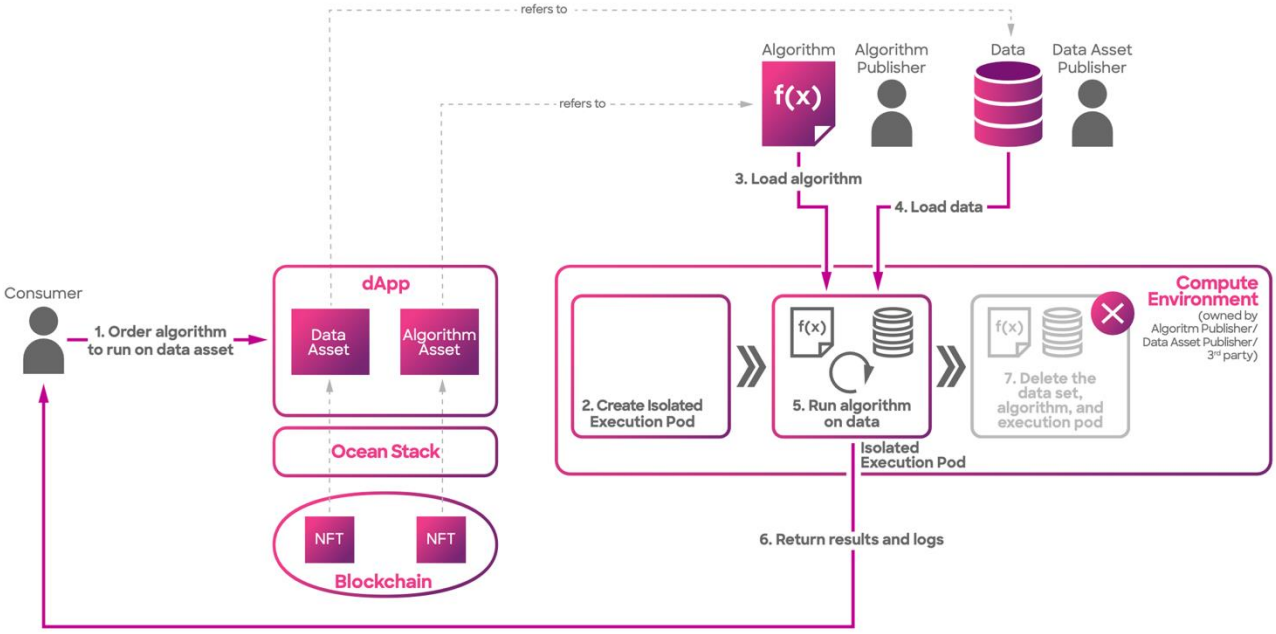


Figure 7: Compute Architecture Overview (Source: Ocean Protocol Docs)

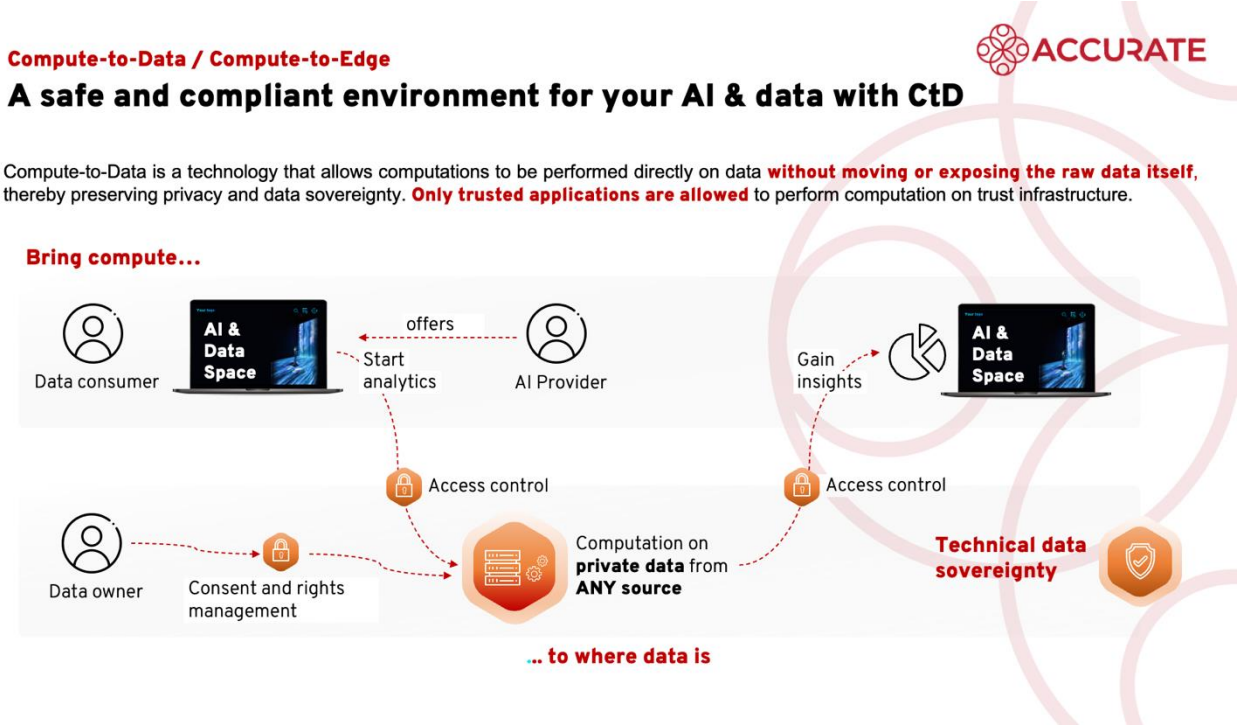


Figure 8: Compute-to-Data Overview (Source: deltaDAO)

The implementation of Compute-to-Data in the ACCURATE project addresses critical concerns in the manufacturing sector regarding data privacy, intellectual property protection, and collaborative innovation. By allowing computations on sensitive data without exposing the raw data itself, CtD opens new possibilities for data-driven insights and cross-organizational collaboration in manufacturing.

Note: The Compute-to-Data component will be validated and added later and extended as part of Task 5.3 in the ACCURATE project. This phased approach ensures that the CtD implementation is tailored to the specific needs and challenges of the European manufacturing data space.

5.5 Contracting Cache (Subgraph)

The Contracting Cache, also called Subgraph, is a component that indexes blockchain data to facilitate easy querying and access. It is particularly useful for front-end interfaces like marketplaces to display blockchain-based transactions and activities in a user-friendly manner.

Key features of the Contracting Cache include:

- Indexing and structuring data from the underlying distributed ledger,
- Offering GraphQL querying capabilities,
- Enhancing cross-ledger interoperability,
- Simplifying the integration of data services metadata into the ACCURATE ecosystem.

Full Documentation [50]: Here

5.6 Data Space Registry

The Registry Service manages the registration of ACCURATE participants. It binds the native identity attribute of the Pontus-X framework (a public address derived from a SECP256K1 key) to a Gaia-X Participant credential [51] for reference and re-identification. The data space registry is an integral part of assigning governance rights and document governance decisions.

Key aspects of the Data Space Registry include:

- Verification of participant credentials through Gaia-X Digital Clearing Houses (GXDCH),
- Documentation of governance decisions,
- Implementation details to be documented in a GitHub repository in the first iteration.

5.7 Identity & Authorization Management

Identity and Access Management in the ACCURATE project is performed at the individual infrastructure and component level to prevent unauthorized access and ensure secure and efficient management of access rights.

Key points about Identity & Authorization Management:

- No centralized identity and authorization management across all data management services,
- Management lies with the DevOps team configuring and maintaining the data space,
- Implemented at the component level for granular control and security,
- Identities shall be based on a reusable open identity ecosystem, not bound to a propriety identity provider to prevent lock-in mechanisms.

5.8 Data Economy Toolkit (Nautilus): A User-Friendly Wrapper for the Ocean Protocol Stack

Nautilus is a TypeScript-based wrapper library for Ocean.js that streamlines the integration of Ocean Protocol's offerings into diverse applications and products. It simplifies tasks such as publishing and consuming services, thereby increasing the usability and accessibility of the Ocean Protocol stack. Nautilus acts as a programmatic participant agent (in DSSC terms) allowing the publication, management, and consumption of services in the ecosystem.

The noteworthy features of Nautilus include:

- Effortless Installation: Nautilus can be installed quickly and easily via npm, empowering users to initiate their projects in minutes.
- Easy Publishing: Nautilus facilitates the uncomplicated publishing of datasets and algorithms for access and computation.
- Compute Job Support: It provides tools for initiating compute jobs and obtaining results.

- Asset Consumption: Nautilus supports the consumption of access-type assets, which include datasets and algorithms.
- Parameter Support: The wrapper extends support for custom user parameters to be utilized when accessing data and custom runtime parameters for the application to allow flexible usage and parametrization on demand before execution.

Nautilus [52] is a significant advancement in promoting the broader adoption of the Ocean Protocol stack, owing to its ability to enhance usability and ease the integration process. It can be accessed via the GitHub repository [53] at https://github.com/deltaDAO/nautilus and the npm package site [54] at https://www.npmjs.com/package/@deltadao/nautilus.

By leveraging these components in the Middleware Layer, the ACCURATE project creates a robust, secure, and flexible infrastructure for managing data, controlling access, and enabling interoperability within the manufacturing data space. This layer forms the crucial link between the underlying blockchain infrastructure and the user-facing applications, enabling the development of innovative data-driven solutions for the European manufacturing sector.

6 Application and Services Layer

The Application and Services Layer of the ACCURATE solution comprises data and software integration services offered by providers within the ecosystem, along with user-centric interfaces that empower participants to publish, consume, and discover applications and institutions. This layer also includes tools to participate in and leverage the full potential of the manufacturing data space ecosystem. Identity and trust features, such as the Organizational Credential Manager, enable secure and trustworthy interactions within the data space. The Application and Services Layer is designed to meet the complex requirements of the manufacturing industry, enabling multi-tier visibility, collaboration, and value creation across the entire supply chain.

6.1 ACCURATE Portal

The ACCURATE Portal serves as the primary user interface for the Federated Catalogue, facilitating the publication, discovery, and exchange of services, as well as contract negotiation and data service management. This decentralized interface streamlines the management of participants and resources within the manufacturing data space, enhancing overall usability and efficiency. The Portal acts as a local graphical user interface and participant agent (in DSSC terms).

Key features of the ACCURATE Portal include:

1. Open and Decentralized Marketplace:
    - Supports seamless exchange and monetization of data assets and digital services.
    - Enables integration and seamless interoperability with various data spaces in the Pontus-X ecosystem.
    - Provides a transparent, intermediary-free environment for data and service transactions.
    - Ensures regulatory compliant data exchanges and services, crucial for the manufacturing sector.
2. Modular Architecture:
    - Allows for the integration of additional portals with their own content management systems (e.g., company-specific portals) in later project stages.
    - Leverages core components like the Catalog, Identity and Access Management, and Registry across multiple portal instances.

The ACCURATE portal [55] is based on the Ocean Market [56], a customizable reference Graphic User Interface (GUI) for a decentralized marketplace built on top of the Ocean Protocol framework, where users can publish, discover, manage, and consume services based on the components and services. The portal is being adapted to allow seamless integration with the Gaia-X services and the Pontus-X ecosystem, and to meet the needs of a Business-2-Business environment.

The ACCURATE Portal plays a crucial role in making the data space accessible and usable for participants across the manufacturing ecosystem, from large OEMs to SMEs and research institutions.

Note: The ACCURATE portal is currently under development and will be available to the consortium at the end of September.

6.2 Data and Software Integration

The ACCURATE solution provides seamless integration points for existing and future enterprise systems in the manufacturing sector, ensuring:

1. Compatibility:
    - Supports a wide range of business applications common in manufacturing environments., such as Manufacturing as a Service, Production Data Sharing, Inventory Sharing, Product Information Sharing, Product Carbon Footprint Calculation, Asset Administration Shell Integration, Specification Document Exchange, and more.
    - Integrates with various data types, including IoT sensor data, portable simulation models, model input data, CAD files and product specifications, production schedules, quality control metrics and analytics results relevant to the production.
    - Enables integration of data analysis software, AI and machine learning models relevant to manufacturing processes and necessary to simulate changes in and across supply-chains.
2. Flexible Deployment:
    - Offers deployment options across cloud, on-premises, or edge environments to suit diverse manufacturing setups.
    - Supports hybrid infrastructures common in the manufacturing industry.
3. Multi-tier Visibility and Collaboration:
    - Facilitates seamless data exchange across the entire manufacturing supply chain, from OEMs to Tier 1, 2, and beyond.
    - Addresses the ACCURATE project's requirement for efficient multi-tier collaboration and visibility in complex manufacturing networks.
4. Versatile Data and Service Management:
    - Enables publication, discovery, and consumption of diverse data sources via URL, REST APIs, GraphQL, IPFS, and other protocols relevant to manufacturing data.
    - Supports future publication, discovery, and consumption of software services via Docker containers, particularly useful for deploying specialized manufacturing applications.
    - Allows combination and orchestration of data sources and software services to create new data products for collaborative use cases, leveraging the Compute-to-Data feature in future iterations.
5. Flexible Data Hosting:
    - Supports data located in the cloud, on-premises, or on edge devices, ensuring compatibility with various enterprise infrastructures common in manufacturing environments.
    - Enables reuse of existing infrastructure investments in the manufacturing sector.

By providing these integration capabilities, the ACCURATE project enables manufacturing participants to leverage their existing infrastructure while benefiting from the advanced features of the data space. This approach facilitates the digital transformation of manufacturing processes while ensuring interoperability, data sovereignty, and value creation across the entire supply chain.

6.3 Identity Wallets

In the ACCURATE project, identity management is crucial for ensuring secure, verifiable, and controlled access to the manufacturing data space. The project currently leverages asymmetric cryptography and Web3 wallet solutions, primarily MetaMask [57], and Nautilus, for user identification and allow listing. This approach aligns with the decentralized nature of the data space while providing a cryptographically secure and “battle-tested” method of identity management which can be used with high-confidence to secure user identities and assets.

6.3.1 Current Implementation: Web3 Wallets and Cryptographic Principles

The use of Web3 wallets, such as MetaMask, in the ACCURATE project is fundamentally based on asymmetric cryptography, specifically Elliptic Curve Cryptography (ECC). Here's a detailed look at the underlying technical principles:

1. Public-Private Key Pairs:
    - Each user's identity is represented by a public-private key pair.
    - The private key is a randomly generated 256-bit number, serving as the root of the user's identity.
    - The public key is derived from the private key using the secp256k1 elliptic curve algorithm, which is the same curve used in Bitcoin and Ethereum.
2. Key Generation and Management:
    - MetaMask generates the private key using a cryptographically secure random number generator.
    - The private key is encrypted and stored locally on the user's device, never leaving it unencrypted.
    - The encryption key for the private key is derived from the user's password using a key derivation function (typically PBKDF2).
3. Address Derivation:
    - The Ethereum address, which serves as the user's identifier in the ACCURATE data space, is derived from the public key.
    - Specifically, it's the last 20 bytes of the Keccak-256 hash of the public key.
4. Digital Signatures:
    - When interacting with the ACCURATE data space (e.g., accessing resources, signing transactions), the wallet uses the private key to create digital signatures.
    - These signatures are created using the Elliptic Curve Digital Signature Algorithm (ECDSA) [58].
    - The signature proves ownership of the private key without revealing it, providing non-repudiation.

5. Transaction Signing Process:
    - When a user initiates a transaction or data access request: a. The transaction details are hashed (typically using Keccak-256). b. This hash is signed with the user's private key using ECDSA. c. The resulting signature, along with the transaction details and the user's public key, is sent to the network.
    - Nodes in the network can verify the signature using the public key, confirming the transaction's authenticity without knowing the private key.
6. Hierarchical Deterministic (HD) Wallet Structure:
    - MetaMask implements HD wallet functionality based on BIP-32, BIP-39, and BIP-44 standards.
    - This allows for the generation of multiple addresses from a single seed phrase, enhancing privacy and key management capabilities.

6.3.2 Implications for ACCURATE

The use of this cryptographic system in ACCURATE offers several advantages:

1. Decentralized Identity:
    - Users maintain sole control over their private keys, eliminating the need for a centralized identity provider.
    - This aligns with the project's goals of data sovereignty and decentralized control.
2. Cryptographic Security:
    - The use of ECC provides strong security with relatively short key lengths, making it efficient for blockchain-based systems.
    - The 256-bit key space is sufficiently large to make brute-force attacks infeasible with current and foreseeable computing power.
3. Allow listing and Access Control:
    - The Ethereum addresses derived from public keys can be easily added to access control lists in smart contracts to allow or forbid interactions.
    - Access control can be implemented by verifying signatures in smart contracts, enabling granular, cryptographically secure permissions.
4. Interoperability:
    - The use of standard cryptographic primitives ensures compatibility with other blockchain networks and Web3 applications.
5. Non-repudiation:
    - Digital signatures provide cryptographic proof of data origin and integrity, crucial for audit trails in manufacturing processes.

6.3.3 Future Developments and Enhancements

To fully align with the requirements of the Gaia-X Framework and European Digital Identities, the ACCURATE project will implement a comprehensive Self-Sovereign Identity (SSI) integration. This development, part of Task 6.2, will create an open digital identity ecosystem within the ACCURATE data space framework. The following enhancements are planned:

1. Full SSI Integration:

    - Implementation of a complete SSI stack, including key components such as: a. Verifiable Data Registry (VDR): A decentralized system for storing and retrieving decentralized identifiers (DIDs) and associated DID documents. b. Issuer: Entities authorized to create and sign verifiable credentials. c. Verifier: Components that validate verifiable presentations. d. Holder (Wallet): User-controlled applications for storing and managing verifiable credentials and creating verifiable presentations.
2. OpenID Connect for Verifiable Presentations (OIDC4VP) [59]:
    - Integration of OpenID Connect 4 Verifiable Presentations standard to enable secure, interoperable presentation of verifiable credentials.
    - This will facilitate standardized communication between holders, issuers, and verifiers in the manufacturing data space.
3. OpenID Connect for Credential Issuance:
    - Implementation of protocols for standardized issuance of verifiable credentials, ensuring interoperability with various identity providers and services.
4. ODRL and REGO Policy Enforcement:
    - Development of capabilities to process and enforce Open Digital Rights Language (ODRL) and REGO policies through SSI verifiers.
    - This will enable fine-grained access control and rights management for manufacturing data and services.
5. Gaia-X Compliance:
    - Ensuring all SSI implementations align with Gaia-X Trust Framework requirements, facilitating seamless integration with other Gaia-X compliant services and data spaces.
6. European Digital Identity Alignment:
    - Adapting the SSI solution to be compatible with emerging European Digital Identity standards and regulations.
    - This includes potential integration with the European Digital Identity Wallet initiative.

As mature, production-ready, and Gaia-X compliant SSI implementation and reference infrastructures are still rare and just emerging in a rapidly evolving landscape this integration and architecture is still subject to change. Furthermore Gaia-X is undergoing a transition to new Verifiable Credential models (Loire, Gaia-X Compliance 24.04.) [60] in Q4 2024/Q1 2025, which has not been finally specified until the date of submission of this report.

6.4 Publication and Consumption Flow

The Publication and Consumption Flow in the ACCURATE data space outlines how data and software services are securely published and consumed. This process ensures that participants can easily share, monetize, and access datasets, algorithms, and external services while maintaining control over access rights and privacy. By using tokenization, Compute-to-Data (CtD), Docker containers, and flexible access controls, the ACCURATE data space enables secure collaboration within the manufacturing ecosystem.

6.4.1 Connecting to the Marketplace

Participants begin by connecting their MetaMask wallets to the ACCURATE Marketplace. This connection provides access to decentralized services, allowing users to manage the publication and consumption of data and software assets.

6.4.2 Publishing Data and Software Assets

Participants in the ACCURATE data space can publish three types of assets: Datasets, Algorithms, and Software as a Service (SaaS). Each asset type follows a structured publication process that collects metadata, defines access controls, and sets pricing.

Metadata Definition:

- Asset Type: Select between Dataset, Algorithm, or Software as a Service.
- Title and Description: Provide key information about the asset.
- Tags and Gaia-X credentials (optional): These can be added to enhance discoverability and compliance with Gaia-X standards.

6.4.3 Docker Container Support

For algorithms published in the ACCURATE Marketplace, the support of Docker containers is critical. Docker containers allow developers to package their AI/ML models or analytics tools into portable, deployable units that can be run on various platforms, including in the Compute-to-Data (CtD) environment.

- Algorithm Asset Definition: When publishing an algorithm asset, developers must define the Docker image in the metadata. This Docker container will be used to execute the algorithm within the CtD framework.
- Compute-to-Data: Docker containers are particularly useful for Compute-to-Data (CtD) scenarios, where data privacy and sovereignty are paramount. The algorithm runs directly on the data without exposing the raw data to external parties. This is crucial for enabling machine learning models or simulations on sensitive manufacturing data.

6.4.4 Policies and access controls

Policies and Access control are key elements in the publication process, allowing asset owners to define how and by whom their assets can be accessed or used.

- Download Access: This option allows users to download the data or software for local use.
- Compute Access (CtD): For algorithm assets, access is provided through Compute-to-Data, where the algorithm runs directly on the data in a secure environment without moving the data.

Asset owners can also define advanced access controls such as allowlists, deny-lists, and user-specific parameters to ensure their data is accessed by the right participants under appropriate conditions.

6.4.5 Software as a Service (SaaS) Integration

In addition to datasets and algorithms, the ACCURATE data space also supports Software as a Service (SaaS) offerings. SaaS assets represent external cloud services and are defined by providing a URL to the service.

- SaaS Asset Definition: When publishing a SaaS asset, participants include the URL to an external cloud service, which can be integrated into the ACCURATE data space. These services can be accessed by other participants, and the interaction is governed by ACCURATE's data space decentralized contracting and monetization mechanisms.

Unlike algorithm assets, SaaS offerings do not rely on Docker containers; instead, they provide access to third-party platforms or user interfaces, making them suitable for cloud-hosted applications or external services.

6.4.6 Pricing Information

Participants can define the pricing of their assets using DataTokens, which are priced in EUROe (or made free if desired). Tokenized access allows for automated payment and governance through smart contracts.

- DataTokens: These ERC-20 tokens facilitate access to datasets, algorithms, or SaaS offerings. The tokenized model ensures that all transactions are transparent, traceable, and compliant with predefined terms.

For testing or non-monetary environments, such as the Pontus-X Testnet, test tokens may be used to simulate real transactions without actual monetary exchange.

6.4.7 Consumption Flow

The consumption flow allows participants to discover, purchase, and access published assets seamlessly. The marketplace's catalogue provides a searchable interface for discovering datasets, algorithms, and software services.

- Discover Assets: Users can search the marketplace for available assets using metadata filters and tags.
- Purchase or Access Assets: After selecting an asset, participants can acquire DataTokens to access the asset according to the defined access type (e.g., download, compute). Smart contracts govern the interaction, ensuring secure transactions.
- Access Control: Asset providers maintain control over who can access their assets by defining detailed access policies, including permissions for specific users or groups.

6.4.8 Programmatic Publication and Automation with Nautilus

Nautilus is a TypeScript-based library designed to simplify and automate the publication, management, and consumption of assets in the ACCURATE data space. It enables developers to

streamline metadata configuration, define pricing schemes, manage access controls, and automate workflows, reducing manual intervention and enhancing efficiency.

6.4.8.1 Key Features of Nautilus

1. Simplified Metadata Configuration: Nautilus uses a builder pattern to streamline the setup of metadata for datasets, algorithms, and services, making the process more readable and maintainable. This simplifies the publication process for assets and ensures consistency in how assets are configured.
2. Complete Asset Management: Nautilus supports the full lifecycle of assets, including publication, editing, and deletion. It enables the integration of Compute-to-Data (CtD) functionality for algorithms, ensuring secure computations on sensitive data without moving the raw data.
3. Automated Data Flows and Event Listening: Developers can use Nautilus to implement event listeners or webhooks that trigger automated actions when specific conditions are met. For example, when new data is published, it can automatically trigger a model run, updating workflows without manual input. This capability supports automated data pipelines and ensures that processes are responsive to real-time changes.
4. Seamless Compute Jobs: Nautilus enables developers to start, monitor, and retrieve results from Compute-to-Data jobs directly from their development environment. This ensures that algorithms can securely process sensitive data and return results without exposing the raw data.
5. Pricing and Access Control Automation: Nautilus allows for programmatic management of pricing schemes and access control policies, automating the setup of allowlists, deny-lists, and dynamic pricing models. This reduces errors and improves flexibility for asset monetization.
6. Enhanced Developer Experience: By simplifying interactions with the ACCURATE Marketplace, Nautilus improves the developer experience. It automates complex tasks such as smart contract interactions, tokenization, and data privacy management, enabling developers to focus on building data-driven applications.

6.5 Licenses and Open-Source Components

The ACCURATE architecture is built on a foundation of open-source software (see Figure 9) and cloud-agnostic design principles, ensuring flexibility, and avoiding vendor lock-in. Key aspects of the licensing approach include:

1. FOSS License for Core Components: All core components of the ACCURATE architecture are provided under Free and Open-Source Software (FOSS) licenses, primarily the Apache 2.0 license. This approach promotes transparency, community involvement, and continuous improvement of the ecosystem (see Figure 9).
2. Cloud-Agnostic Design: The infrastructure is designed to be agnostic to the underlying cloud environment, supporting deployments across public clouds, on-premise installations, and IoT/edge environments. This flexibility ensures that participants can choose the

infrastructure that best suits their needs without being constrained by proprietary technologies.

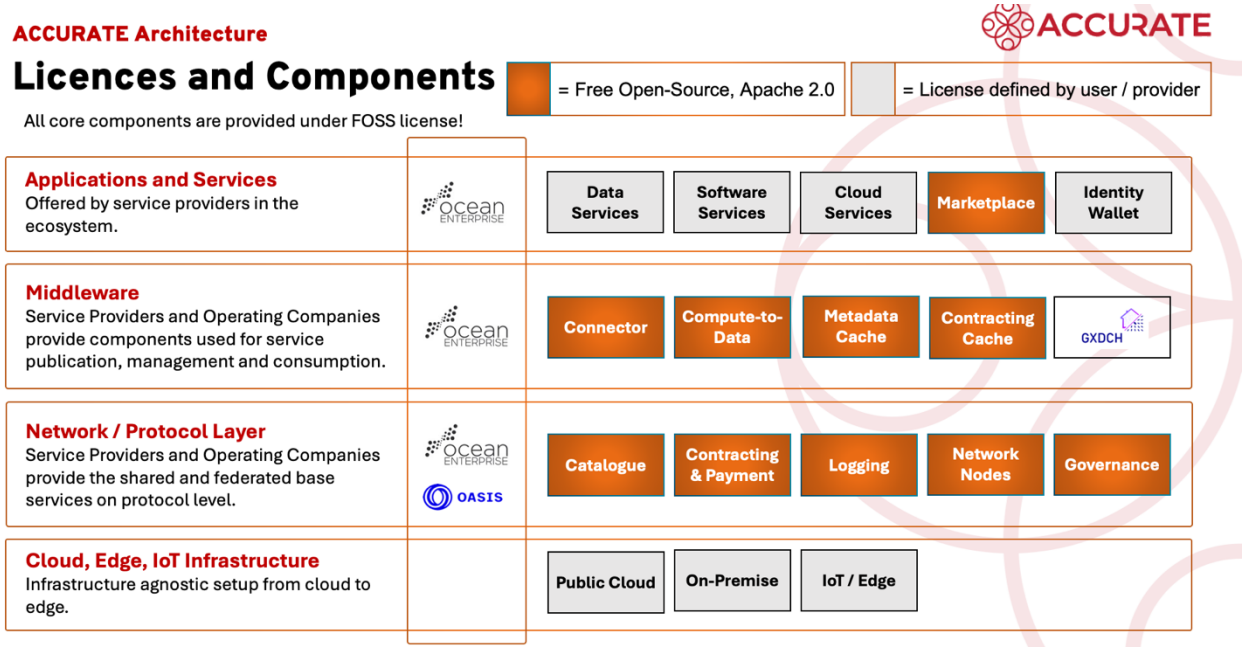


Figure 9: Licenses and Components of the ACCURATE Architecture (Source: deltaDAO)

7 Gaia-X Trust Framework and Compliance Integration

The ACCURATE project integrates essential services of the Gaia-X Trust Framework to ensure compliance, semantic interoperability, and trust across the manufacturing data space ecosystem. This integration is designed to interact with multiple Gaia-X Digital Clearing Houses (GXDCH) for each service, enhancing decentralization and avoiding single points of failure. The implementation of these services establishes a foundation for a robust, sovereign, and standardized data exchange environment in the manufacturing sector. Currently the system is following the 22.10 version of Gaia-X Compliance. The transition to the 24.04 version [60] is expected in 2025.

7.1 Gaia-X Registry

The ACCURATE project incorporates the Gaia-X Registry, utilizing its decentralized database structure as a backbone for ecosystem governance. The implementation provides:

- Access to critical information including Trust Anchors, Trust Service Providers (TSPs), validation processes, and schemas for Gaia-X Verifiable Credentials (VCs),
- Seamless access to verifiable information for all ACCURATE participants,
- Capability to interact with multiple GXDCHs for registry services, enhancing system resilience and decentralization.

7.2 Gaia-X Notarization

The Gaia-X Notarization Service is integrated as a mandatory component to create participant credentials and meet the minimal Gaia-X requirements within the ACCURATE ecosystem. Key features include:

- Validation of all registration numbers provided by participants in their self-descriptions,
- Enhanced security and reliability in participant identification and authentication processes,
- Utilization of multiple GXDCHs for notarization, ensuring service continuity and avoiding single points of failure.

7.3 Gaia-X Compliance

The Gaia-X Compliance Service is integrated to ensure that Gaia-X Credentials can be verified through the GXDCH, and compliance credentials can be retrieved. This service provides:

- Validation of the shape, content, and signature of Gaia-X Credentials,
- Issuance of Gaia-X Compliance Credentials attesting compliance results,
- Flexibility to utilize multiple GXDCHs for compliance checks, contributing to the overall decentralization and resilience of the solution.

7.4 Credential Event Service (CES)

The Credential Event Service acts as a cross-ecosystem catalogue for all Gaia-X ecosystems. While its usage is optional and not in scope for the initial implementation of ACCURATE, future iterations may leverage this service for:

- Registration of Gaia-X Compliance Credentials,
- Discovery of services across catalogues,
- Cross-ecosystem discovery through Gaia-X compliant service credentials.

7.5 Trust Service Providers (TSPs)

To comply with Gaia-X minimum requirements, the use of Gaia-X accredited TSPs for identity assurance is mandatory in the ACCURATE project. The implementation ensures:

- Each participant credential [62] is signed by a participant identified through a TSP [9].
- TSPs perform identification and issue X.509 certificates, binding RSA keys with checked identities.
- For the ACCURATE ecosystem, participant credentials can be issued by a designated authority, but it is recommended that each participant undergoes identification by a TSP.
- Identification through a TSP is necessary for the publication of services in the ecosystem.

7.6 Integration Benefits and Compliance

The integration of the Gaia-X Trust Framework services described in Section 6.6, with the ability to interact with multiple GXDCHs for each service, establishes a solid foundation for a trustworthy, interoperable, and sovereign data space in the manufacturing sector. This approach addresses key requirements of the ACCURATE project:

1. Compliance: Meets the minimum requirements for Gaia-X ecosystems, positioning ACCURATE as a potential Gaia-X lighthouse project in the manufacturing domain.
2. Data Sovereignty: Ensures compliance with European data exchange regulations, focusing on data sovereignty principles crucial for sensitive manufacturing data.
3. Trust and Interoperability: Facilitates trust and interoperability across the complex ecosystem of the manufacturing industry, from large OEMs to SMEs.
4. Supply Chain Integration: Supports the creation of a digital ecosystem connecting manufacturers, OEMs, and SMEs to secure supply chain continuity through digital sovereign mechanisms.
5. System Resilience: Enhances system resilience and decentralization, critical for a production environment based on real manufacturing data and deployed users.
6. Semantic Interoperability: Supports cross-ecosystem semantic interoperability by describing participants and services following Gaia-X de-facto standards, crucial for the diverse landscape of manufacturing technologies and processes.

The ACCURATE architecture and its data space base services (see Figure 10) enable authentication and authorization, a catalogue, a marketplace and trust and compliance mechanisms based on the

PONTUS-X and Ocean Protocol tech stack, facilitating seamless interaction between service providers and consumers through decentralized contracting and settlement systems. This architecture, by incorporating the Gaia-X Credential Event Service and GXDCH, ensures alignment with European Data Space initiatives, providing a sovereign and secure environment for data exchange in the manufacturing sector, while maintaining interoperability and compliance with Gaia-X standards.

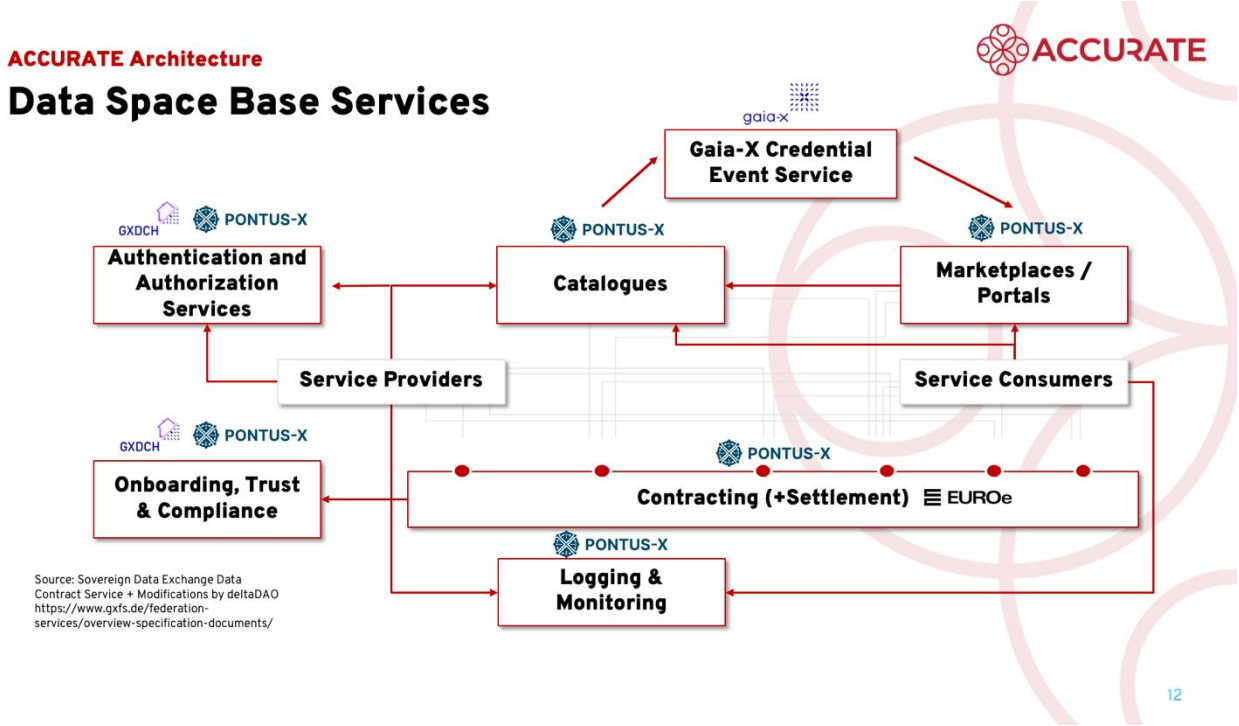


Figure 10: Data Space Base Services (Source: deltaDAO)

8 Conclusion

The decentralized data space infrastructure of the ACCURATE project's represents a significant advancement for secure, interoperable, and sovereign data sharing in European manufacturing. Key achievements include:

1. Reference Implementation Readiness: The current architecture fully aligns with the requirements identified in ACCURATE and is prepared for reference implementation.
2. Service Development Initiation: With the architecture in place, service development and testing can commence as planned.
3. Open-Source and Cloud-Agnostic Foundation: The ecosystem's basic services are built on free, open-source software and designed to be cloud-agnostic.
4. Efficient Resource Utilization: By leveraging existing and tested open-source software components, the project proceeds in a resource-efficient manner with minimized risks.
5. Gaia-X Interoperability: The architecture ensures a high level of interoperability with other Gaia-X lighthouse initiatives and relevant projects from its inception.
6. Validated Architecture: Successful validation within ACCURATE and other relevant initiatives demonstrates the robustness and effectiveness of the architecture.
7. Decentralization and Trust: By avoiding single points of failure and control, the architecture addresses potential adoption barriers and fosters long-term trust among participants.
8. Accessibility and Data Sovereignty: The architecture features very low entry barriers, making it accessible to small and medium enterprises, while enabling the highest level of technical data sovereignty.

As the project progresses, several crucial next steps are planned:

1. Portal Release: Launch of a user-friendly interface for non-developers to interact with the architecture, featuring data discovery, publication, and consumption. The portal will complement the data space toolkit Nautilus, which provides programmatic interaction with the architecture. Comprehensive guides on getting started with both the portal and Nautilus will be provided, ensuring accessibility for users with varying technical expertise.
2. Pilot Partner Onboarding: Engagement of initial pilot partners for testing and feedback, followed by gradual onboarding of additional participants to validate and refine the data space.
3. Task 5.3 (M14 – M26): Development of a secure Compute-to-Data environment, culminating in Deliverable D5.2.
4. Task 5.4 (M14 – M26): System integration and decentralization efforts, focusing on connecting diverse data sources.
5. Task 6.2 (M14 – M26): Implementation of trust mechanisms, including SSI and automated contracting, contributing to Deliverable D5.3.
6. Interoperability Testing: Ensuring seamless interactions with other Gaia-X compliant data spaces.
7. Regulatory Alignment: Ongoing adaptation to evolving European data governance and digital identity standards.

These steps will transform the architectural blueprint into an operational ecosystem in an iterative, agile approach. The release of the portal will significantly improve accessibility for stakeholders, driving adoption and innovation. As a result of these developments, ACCURATE will be a major contributor to the digital transformation of European manufacturing, boosting innovation and setting new standards for secure data exchange in industry.

Bibliography

[1] ACCURATE Project Website, https://accurateproject.eu/

[2] Gaia-X Architecture Document 24.04., https://docs.gaia-x.eu/technical-committee/architecture-document/24.04/

[3] Pontus-X Digital Service Ecosystem, https://www.pontus-x.eu/

[4] OASIS Sapphire Confidential EVM, https://oasisprotocol.org/sapphire

[5] Ocean Enterprise, https://www.oceanenterprise.io/

[6] EUROe Stablecoin, https://www.euroe.com/

[7] European E-Money Directive (2009/110/EC), https://finance.ec.europa.eu/consumer-finance-and-payments/payment-services/e-money_en#legislation

[8] European Digital Identity, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en

[9] Gaia-X Trust Framework 22.10, https://docs.gaia-x.eu/policy-rules-committee/trust-framework/22.10/

[10] deltaDAO AG Website, https://www.delta-dao.com/

[11] European Production Giganet (EuProGigant) Website, https://euprogigant.com/en/

[12] Gaia-X Digital Clearing House (GXDCH), https://gaia-x.eu/gxdch/

[13] Gaia-X Digital Clearing Houses (GXDCH) Status Page, https://docs.gaia-x.eu/framework/?tab=clearing-house

[14] Gaia-X 4 Future Mobility, https://www.gaia-x4futuremobility.de/en/home

[15] COOPERANTS Website, https://cooperants.de/en/

[16] European GDPR Regulation 2016/679, https://eur-lex.europa.eu/eli/reg/2016/679/oj

[17] European Data Act Regulation 2023/2854, https://eur-lex.europa.eu/eli/reg/2023/2854

[18] Data Spaces Support Centre (DSSC), https://dssc.eu/

[19] European Data Governance Act (DGA) 2022/868, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868

[20] European AI Act (AIA) 2024/1689, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL_202401689

[21] EU Markets in Crypto Assets Regulation (MICAR) 2023/1114, https://eur-lex.europa.eu/eli/reg/2023/1114/oj

[22] Gaia-X Registry Service, https://docs.gaia-x.eu/technical-committee/architecture-document/24.04/gx_services/#gaia-x-registry

[23] Gaia-X Notarization Service, https://docs.gaia-x.eu/technical-committee/architecture-document/24.04/gx_services/#gaia-x-notary-lrn-legal-registration-number

[24] Gaia-X Compliance Service, https://docs.gaia-x.eu/technical-committee/architecture-document/24.04/gx_services/#gaia-x-compliance

[25] Gaia-X and Catalogues Blog Article, https://gaia-x.eu/news-press/gaia-x-and-catalogues/

[26] Gaia-X Credential Event Service (CES) Repository, https://gitlab.com/gaia-x/lab/credentials-events-service

[27] Gaia-X Trust Service Providers and Trust Anchors, https://docs.gaia-x.eu/policy-rules-committee/trust-framework/22.10/trust_anchors/

[28] Pontus-X Logging Service, https://explorer.pontus-x.eu/pontusx/test

[29] Oasis Protocol Website, https://oasisprotocol.org/

[30] Polygon Developer Website, https://polygon.technology/developers

[31] Polkadot Developer Website, https://polkadot.com/developers

[32] Avalanche Developer Website, https://www.avax.network/developers

[33] Hyperledger Website, https://www.hyperledger.org/

[34] Arbitrum Developer Documentation, https://docs.arbitrum.io/build-decentralized-apps/quickstart-solidity-hardhat

[35] Oasis Privacy Layer (OPL), https://oasisprotocol.org/opl

[36] Oasis Sapphire ParaTime Documentation, https://docs.oasis.io/dapp/sapphire/

[37] Pontus-X Documentation, https://docs.pontus-x.eu/

[38] Ocean Protocol Documentation, https://docs.oceanprotocol.com/

[39] Ocean Protocol Architecture Documentation, https://docs.oceanprotocol.com/developers/architecture

[40] W3C Decentralized Identifiers (DIDs) v1.0 Specifications, https://www.w3.org/TR/did-core/

[41] ERC-20 Token Standard, https://ethereum.org/de/developers/docs/standards/tokens/erc-20/

[42] EUROe Transparency and Regulation, https://www.euroe.com/transparency-and-regulation

[42] Ocean Aquarius Infrastructure, https://docs.oceanprotocol.com/developers/old-infrastructure/aquarius

[43] Ocean DDO Specification, https://docs.oceanprotocol.com/developers/old-infrastructure/aquarius

[44] Ocean Enterprise and Pontus-X Draft DDO Specifications, https://docs.pontus-x.eu/docs/ddo_credential/ddo_intro

[45] Ocean Provider Documentation, https://docs.oceanprotocol.com/developers/old-infrastructure/provider

[46] Eclipse Cross Federation Service Components, https://projects.eclipse.org/projects/technology.xfsc

[47] Walt.id Documentation, https://docs.walt.id/home

[48] W3C ODRL Information Model 2.2 Specifications, https://www.w3.org/TR/odrl-model/

[49] Open Policy Agent (OPA) Website, https://www.openpolicyagent.org/

[50] Ocean Protocol Subgraph Documentation, https://docs.oceanprotocol.com/developers/old-infrastructure/subgraph

[51] Gaia-X Participant Credential according to 22.10 Version of the Trust Framework, https://www.delta-dao.com/.well-known/2210_gx_participant.json

[52] Nautilus Documentation, https://nautilus.delta-dao.com/

[53] Nautilus GitHub Repository, https://github.com/deltaDAO/nautilus

[54] Nautilus npm Package, https://www.npmjs.com/package/@deltadao/nautilus

[55] ACCURATE Portal GitHub Repository, https://github.com/deltaDAO/portal-accurate

[56] Ocean Enterprise GitHub Repository, https://github.com/OceanProtocolEnterprise

[57] MetaMask Documentation, https://docs.metamask.io/

[58] W3C Data Integrity ECDSA Cryptosuites v1.0, https://www.w3.org/TR/vc-di-ecdsa/

[59] OpenID Connect 4 Verifiable Presentations Specification Draft 21, https://openid.net/specs/openid-4-verifiable-presentations-1_0.html

[60] Gaia-X Compliance Specifications 24.04 Draft, https://docs.gaia-x.eu/policy-rules-committee/compliance-document/24.04-prerelease/

[61] W3C Verifiable Credentials Data Model 2.0, https://www.w3.org/TR/vc-data-model-2.0/

[62] Gaia-X Participant Credential Attributes, https://docs.gaia-x.eu/policy-rules-committee/trust-framework/22.10/participant/