



MADITRACE

Architecture definitions for POC implementation - Intermediate Report

Deliverable D3.4

Version N°1.0

Authors: Johannes Ebert (Spherity), Doruk Sahinel (Spherity), Ricky Thiermann (Spherity)



Disclaimer

The content of this report reflects only the author's view. The European Commission is not responsible for any use that may be made of the information it contains.





Document information

Grant Agreement	101091502
Project Title	Material and digital traceability for the certification of critical raw materials
Project Acronym	MaDiTraCe
Project Coordinator	Daniel Monfort, BRGM
Project Duration	1 January 2023 – 31 December 2025 (36 months)
Related Work Package	WP3
Related Task(s)	T3.3: Architecture and components for traceability implementation
Lead Organisation	Spherity GmbH
Contributing Partner(s)	BRGM, DMT, ULEI, Spherity, Funditec
Authors	Johannes Ebert (Spherity), Doruk Sahinel (Spherity), Ricky Thiermann (Spherity)
Due Date	M24
Submission Date	--
Dissemination level	PU





History

Date	Version	Submitted by	Reviewed by	Comments
10/10/24	0.1	Johannes Ebert		Table of Contents
07/11/24	0.2	Doruk Sahinel	Rouwaida Abdallah	First Draft
25/11/24	0.3	Doruk Sahinel	Daniel Monfort	After first feedback
20/01/25	0.4	Doruk Sahinel	Daniel Monfort	Final validation
28/01/25	0.4	Daniel Monfort	Mariana Terreros	Quality Check





Table of contents

1.	Introduction	12
2.	Driving Factors	15
2.1.	Conformity Credentials	15
2.2.	Data Spaces	16
2.3.	Digital Product Passport (DPP)	17
2.4.	Governance and Trust	19
2.5.	SSI	20
2.6.	Traceability	22
3.	Relevant EU Regulations	24
3.1.	European Battery Regulation and Battery Passport Technical Guidance	24
3.2.	Corporate Sustainability and Due Diligence Directive	25
3.3.	Ecodesign for Sustainable Products Regulation (ESPR)	26
4.	Ecosystems and standards initiatives	28
4.1.	Joint Technical Committee - JTC 24	28
4.2.	Battery Pass Consortium	30
4.3.	CIRPASS	33
4.4.	Global Battery Alliance	35
5.	Technical Standards	38
5.1.	W3C Verifiable Credentials	38
5.2.	Decentralized Identifiers	39
5.3.	Verifiable Credentials API	40
5.4.	DID Comm	41
5.5.	Eclipse Data Space Connector	42
5.6.	Asset Administration Shell	43
6.	Reference Architectures	44
6.1.	EUDI Wallet Architecture Reference Framework	44





6.1.1. Scope	45
6.1.2. Adoption and Relevance	45
6.1.3. Relevance for supply chain traceability	46
6.2. Catena-X Data Space Architecture.....	46
6.2.1. Scope	47
6.2.2. Adoption and Relevance	48
6.3. UN Transparency Protocol	48
6.3.1. Scope	48
6.3.2. Adoption and Relevance	48
7. Architecture Principles	50
7.1. Accessibility	50
7.2. Data Accuracy	50
7.3. Interoperability	51
7.4. Modularity	51
7.5. Verifiability	51
8. High-Level Architecture Components	53
8.1. Architecture Overview	53
8.2. Traceability Architecture Components	55
8.2.1. Data Exchange Protocol	55
8.2.2. Digital Twin / Data Catalogue	56
8.2.3. Enterprise Credential (LPID)	57
8.2.4. Organization Identity Wallet	57
8.2.5. Semantics Layer	58
8.2.6. SSI Authorization and Access Control	59
8.2.7. Trust Chain (Root Credential)	60
8.2.8. Verifiable Data	61
8.3. Traceability Monitoring Tools	62
8.3.1. Internal Database	62



8.3.2. Quality Investigation Process	62
8.3.3. Monitoring UI.....	63
9. Use Case Sequence Descriptions	65
9.1. Use Case A: Create Traceability Event	65
9.2. Use Case B: Request Mine Audit.....	66
9.3. Use Case C: Data Sharing.....	67
9.4. Use Case D: Data Verification	69
10. Discussion and Future Work.....	70
10.1. Blockchain and Smart Contracts.....	70
10.2. Evaluation and Next Steps.....	70
11. Conclusions.....	72
12. References	74

List of figures

Figure 1 - Interaction of Actors in the SSI Model	20
Figure 2 - Battery Pass Digital Data Chain in a Traceability System (Battery Pass Consortium, 2024)	30
Figure 3 - Battery Passport Technical Guidance Principal System Architecture (Battery Pass Consortium, 2024).....	32
Figure 4 - Structural View of DPP System with Structure, Actors and Components (CIRPASS, 2024)	34
Figure 5 - Global Battery Alliance PoC Tracing Data Example	37
Figure 6 - Overview of DID architecture and the relationship of the basic components (W3C, 2022)	39
Figure 7 - Catena-X Data Exchange Framework with Eclipse Dataspace Connector and Asset Administration Shell (Catena-X, 2023).....	42
Figure 8- eIDAS2, UNTP, and Catena-X References in Maditrace PoC Architecture	44
Figure 10 - Building Blocks of the Maditrace PoC Architecture	53
Figure 11 - Create Traceability Event Use Case.....	65
Figure 12 - Request Mine Audit Use Case	67





Figure 13 - Data Sharing Use Case 68

Figure 14 - Data Verification Use Case 69

Summary

This intermediate report presents an architectural framework designed to ensure traceability in critical raw material supply chains. The driving factors and concepts that set the foundation towards the architecture such as conformity credentials, data spaces and self-sovereign identities (SSI) are introduced. Then the relevant initiatives, regulations, standards, ecosystems and specifications are presented and their integration into the architecture is explained together with the architectural principles that stem from these standards.

This proposed architecture recognises the significant advances made in the last few years in creating standards and ecosystems around all the different building blocks of the traceability and Digital Product Passport (DPP) architecture. A modular architecture structured around these building blocks is proposed, and all components are clearly defined with their objective, functions and the interactions with other building blocks. The use case sequence diagrams are presented as case studies to highlight how these architectural components can be exploited to creating secure and verifiable supply chains. The potential relations between the provided architecture and smart contracts are given in the discussion section together with the evaluation and next steps towards building the final architecture. The conclusions highlight key aspects of the report. This deliverable is intended for technical experts, industry stakeholders, and policymakers, guiding them toward creating traceable raw material supply chains.

Keywords

Compliance, Critical Raw Materials (CRM), Digital Product Passport (DPP), Self-Sovereign Identity (SSI), Proof-of-Concept Architecture, Verifiable Credentials (VC), Traceability

Abbreviations and acronyms

AAS	Asset Administration Shell
API	Application Programming Interface
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CERTEX	EU Customs Single Window
CMAG	Critical Minerals Advisory Group



CoC	Chain of Custody
CRM	Critical Raw Materials
DID	Decentralized Identifier
DLT	Distributed Ledger Technology
DPP	Digital Product Passport
DRMP	Digital Raw Material Passport
DSP	Dataspace Protocol
EDC	Eclipse Data Space Connector
eIDAS	Electronic Identification, Authentication and Trust Services Regulation
ERP	Enterprise Resource Planning
ESPR	Ecodesign for Sustainable Products Regulation
EU	European Union
EUDI	European Digital Identity
EV	Electric Vehicle
EWC	EU Digital Identity Wallet Consortium
GBA	Global Battery Alliance
GDPR	General Data Protection Regulation
GPS	Global Positioning System
HTTP	Hypertext Transfer Protocol
IDS	International Data Spaces
IDTA	Industrial Digital Twin Association
IEC	International Electrotechnical Commission
IoT	Internet of Things
ISO	International Organization for Standardization
IT	Information Technology
JTC	Joint Technical Committee
KYC	Know Your Customer
LPID	Legal Person Identifier
NGO	Non-Governmental Organization
OID	Organization Identity
POC	Proof of Concept
PDP	Policy Decision Point





QR	Quick Response
RBAC	Role-based Access Control
RDF	Resource Description Framework
REO	Responsible Economic Operator
REST	Representational State Transfer
RFC	Request for Comments
RFID	Radio-Frequency Identification
SHACL	Shapes Constraint Language
SSI	Self-Sovereign Identity
UI	User Interface
UID	Unique Identifier
UN/CEFACT	United Nations Centre for Trade Facilitation and Electronic Business
UNTP	United Nations Traceability Protocol
URI	Uniform Resource Identifier
VC	Verifiable Credentials
VDR	Verifiable Data Registry
W3C	World Wide Web Consortium





1. Introduction

In light of the European Critical Raw Materials Act (European Commission, 2024), which aims to ensure a secure and sustainable supply of critical raw materials, MaDiTraCe seeks to provide necessary data models, traceability tools, Digital Product Passports (DPP), and a related management system within a well-defined architectural framework. In MaDiTraCe, the DPP concept guides our strategy for collecting and linking information on tracking, transport, and processing of critical raw materials (CRM) in a decentralized manner. One of the project's main technical goals is to design an architecture that certifies all relevant information generated by verifiable and trusted organizations, stores this information as verifiable credentials (VCs), and links trusted organizations through decentralized information-sharing methods. The DPP also serves as the interface with the CERA 4in1 certification scheme, which will be extended in MaDiTraCe to cover complete supply chains.

The purpose of this deliverable is to present a comprehensive architectural framework that facilitates the implementation of traceability in critical raw material supply chains, based on self-sovereign identities for managing verifiable product information and aligning with the objectives set forth in the European Critical Raw Materials Act. By providing a detailed overview of the modular architecture and how its components ensure compliance with CERA 4in1 standards through data vocabulary, attributes, and accessibility, this document serves as a practical guide for stakeholders involved in the management and certification of critical raw materials. It emphasizes the importance of integrating Digital Product Passports and verifiable credentials into existing systems to enhance transparency and compliance. The document is intended for technical experts, researchers, industry stakeholders, and policymakers involved in the critical raw materials supply chain, and it aims to support their ongoing efforts by illustrating how the proposed architecture can be adapted and utilized in real-world CRM traceability scenarios.

The architecture proposed in this document recognizes the significant advances made in the last few years in creating standards and ecosystems around all the different building blocks of the traceability and DPP architecture. Based on the principles of accessibility, data accuracy, interoperability, modularity, and verifiability, we propose a Proof-of-Concept (POC) architecture, which is structured around the driving factors of decentralized digital identity frameworks, and shaped by the relevant standards, regulations, ecosystems, and initiatives. The goal of this document is to explain how all these factors contribute to architecture and to define clearly each building block. This will allow stakeholders to a) gain



a better understanding of the architectural landscape, and b) prioritize subsets of the architecture, and c) switch out different building blocks as needs evolve. This is particularly important since the landscape is evolving rapidly.

In order to identify the key prerequisites, procedures, and methodologies needed to establish a digital material passport within the raw material supply chain, we first analyzed the critical concepts, standards, and ecosystems to define our design goals for the architecture. It can be assumed that there will be convergence on a single standard or ecosystem within the raw materials for battery sector, for instance on the Catena-X dataspace; however, this convergence might be limited by geographical boundaries. It is therefore important to inform the reader of different options as well as their adoption and advancement. Bringing together this information and the requirements of the CRM supply chain identified in the previous deliverables of MaDiTraCe to define our architectural principles, we concluded that the architecture for POC comprises of the following technical blocks: Data Exchange Protocol, Digital Twin, Enterprise Credential, Organization Identity Wallet, Semantics Layer, SSI Authorization and Access Control, Trust Chain (Root Credential), and Verifiable Data.

By taking a layered approach that starts with the most general concepts and progresses to the specific details of architectural components, the document is structured as follows:

- **Section 1, Introduction,** outlines the goals of the MaDiTraCe project in establishing traceability in critical raw material supply chains, defines the aim and the intended audience of the document, and briefly introduces the sections of the deliverable.
- **Section 2, Driving Factors,** discusses the foundational concepts that inform the architectural framework; namely conformity credentials, data spaces, digital product passport, governance and trust, self-sovereign identity (SSI), and traceability.
- **Section 3, Relevant Regulations,** provides the scope and the relevance of applicable regulations, including the European Battery Regulation and their implications for the proposed architecture.
- **Section 4, Ecosystems and Standards Initiatives,** details various ecosystems and initiatives that aim to provide a manufacturer-independent and standardized implementation in the diverse environment of the Digital Product Passport (DPP).



- **Section 5, Technical Standards,** presents the technical standards essential for developing the architecture and discusses how these can be adopted to the project framework.
- **Section 6, Reference Architectures,** introduces existing reference architectures that align with the project's goals, focusing on the fundamental modular components that shape the generic architecture presented in this document.
- **Section 7, Architecture Principles,** highlights the principles guiding architecture, including accessibility, data accuracy, and interoperability with a discussion on why they are selected as a design goal.
- **Section 8, High-Level Architecture Components,** describes the modular architecture and its key components for traceability. The objective and functions of the building block is given together with the interfaces that allow its interaction with other building blocks.
- **Section 9, Use Case Sequence Descriptions,** offers examples of use cases for cobalt, lithium, and other materials and defines how the architecture ensures a verifiable and trusted framework for these materials.
- **Section 10, Discussion and Future Work,** explores the potential integration of blockchain and smart contracts into the architecture, discusses the next steps and suggests evaluation methods to analyse how architecture design goals can be reached.
- **Section 11, Conclusions,** summarizes the report's findings and recommendations.



2. Driving Factors

This section presents the driving factors to establish a digital identity management architecture for traceability in critical raw material supply chains and discusses the impact of these concepts on the architectural framework in an alphabetical order.

2.1. Conformity Credentials

Definition and Rationale

Conformity credentials are credentials issued by a third-party about any relational object within a company. These credentials can be related to various aspects such as the legal entity itself, a company facility, a product model, or a specific product item. They play a crucial role in ensuring transparency, trust, and compliance within the supply chain and are integral to the functionality of DPPs.

Legal Identity Credentials

Legal identity credentials verify the authenticity and legal standing of a company or organization. They are typically issued by governmental or accredited bodies and provide a foundational layer of trust in digital interactions. In the context of Digital Product Passports, these credentials ensure that the entities involved in the production, supply, and exchange of data are legitimate and recognized by the law. This reduces the risk of fraud and enhances the credibility of the entire supply chain.

Ecosystem Membership Credentials

Ecosystem membership credentials validate an entity's participation in a specific industry ecosystem or consortium. These credentials, issued by industry groups or consortia, confirm that a company adheres to the standards and practices of the ecosystem. Data Spaces are also important issuers of Ecosystem membership credentials. In the realm of traceability and DPPs, they facilitate seamless data sharing and interoperability between members, promoting a cohesive and efficient supply chain network.

Certifications

Certifications like CERA4in1, ISO 14001, and EU Ecolabel can be turned into comprehensive conformity credentials that encompass multiple aspects of product and process compliance. CERA4in1, for instance, covers criteria such as conflict-free sourcing, environmental performance, social responsibility, and quality management. On the other



hand, regulatory frameworks like REACH require the declaration of the presence of certain chemicals and ensure compliance with chemical safety regulations. These certifications and declarations play a pivotal role in traceability by ensuring that products meet stringent industry standards and regulatory requirements. In DPPs, such certifications provide detailed proof of compliance, enhancing transparency and trust among stakeholders.

Product Conformity I - Safety

Product safety conformity credentials are essential for verifying that a product meets established safety standards and regulations. These credentials are often issued following rigorous testing and assessment by recognized safety certification bodies. For instance, a safety assessment for electronic devices ensures that the product is safe for consumer use and complies with safety regulations. In the context of DPPs, these credentials provide verifiable proof of product safety, enabling consumers and regulators to trust the product's compliance with safety standards.

Product Conformity II - Product Carbon Footprint

Product carbon footprint credentials quantify the greenhouse gas emissions associated with a product throughout its lifecycle. These credentials are issued by certification bodies and are crucial for assessing the carbon footprint of a product. In the framework of Digital Product Passports, carbon footprint credentials provide transparent and verifiable data on the environmental performance of a product. This information is vital for consumers, businesses, and regulators aiming to make informed decisions and promote sustainability within the supply chain.

2.2. Data Spaces

Data spaces are digital ecosystems designed to facilitate the secure and efficient exchange of data between different organizations and stakeholders. They operate on principles of data sovereignty, meaning that data owners retain control over their data and decide how it can be used and shared.

Data Exchange

Data spaces use standardized protocols and formats to ensure that data from different sources can be integrated and understood by all participants. This enables seamless data sharing and collaboration across various platforms and systems.





Data spaces also serve as a hub for data schemas, standards, and ontologies, which are formal and structured representations of knowledge in a specific domain, defining concepts, their relationships, and properties. These schemas define the structure, relationships, and semantics of data, ensuring consistency and interoperability across the ecosystem. By maintaining and providing access to standardized data schemas, data spaces help participants understand and utilize shared data more effectively.

2.3. Digital Product Passport (DPP)

Digital Product Passports (DPPs) are comprehensive digital records that provide detailed information about a product's lifecycle, including its origin, production processes, and environmental impact. They play a crucial role in enhancing transparency, traceability, and sustainability across various industries.

Intermediate Digital Raw Material Passports

Intermediate Digital Raw Material Passports (DRMPs) are a subset of DPPs focused specifically on raw materials used in production processes. These passports document the origin, extraction, processing, and transportation of raw materials, providing a clear and traceable path from the source to the final product. This level of traceability is essential for ensuring that raw materials are sourced responsibly and sustainably, and it supports various compliance and certification requirements.

DRMPs facilitate the exchange of critical information about raw materials between different stakeholders in the supply chain. This information includes data on material composition, environmental impact, and compliance with sustainability standards. By maintaining detailed records of raw materials, companies can improve their supply chain transparency, reduce environmental impact, and support ethical sourcing practices.

The EU Battery Passport

Battery Passports are DPPs specifically designed for batteries, particularly those used in electric vehicles (EVs) and industrial applications. These passports are mandated by the EU Battery Regulation, which will take effect in February 2027. The regulation requires that all batteries placed on the European market must include a Battery Passport (European Commission, 2023), which provides comprehensive information about the battery's supply chain, environmental impact, and lifecycle.





The Battery Passport is created by the economic operator that places the product on the European market. This operator is responsible for collecting and consolidating information from various stages of the supply chain and ensuring that the data is accurate and reliable. The Battery Passport distinguishes between public and confidential data, providing transparency while protecting sensitive information.

Key data attributes included in the Battery Passport, as specified in Article 77 of the EU Battery Regulation¹, are:

- General Information: Basic details about the battery, including its manufacturer, model, and specifications.
- Labels and Certifications: Information about the certifications and labels the battery has received, ensuring compliance with relevant standards.
- Product Carbon Footprint: Data on the greenhouse gas emissions associated with the battery's production, helping to assess its environmental impact.
- Supply Chain Due Diligence: Documentation of the supply chain processes and practices, ensuring that the materials used are sourced responsibly.
- Materials and Composition: Detailed information about the materials used in the battery, including their origin, processing methods, and recycled content.
- Circularity & Resource Efficiency: Data on the battery's recyclability and resource efficiency, supporting circular economy initiatives.
- Performance & Durability: Information about the battery's performance metrics and expected lifespan, ensuring that it meets quality and durability standards.

A QR code on the battery will provide access to its digital passport, allowing consumers and professionals along the value chain to easily retrieve detailed information and make informed decisions. This digital transparency aims to support the circular economy for batteries by enabling efficient recycling and responsible disposal practices.

For a complete list of attributes and more detailed guidance, you can consult the Battery Pass content guidelines linked below:

EU Battery Regulation Article 77

¹ https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32023R1542#anx_XIII





By implementing Battery Passports, the EU aims to enhance the sustainability and transparency of the battery industry, supporting broader environmental and economic goals.

2.4. Governance and Trust

Governance & Trust Ecosystem

Clear rules and policies are established to manage data access, usage rights, and compliance with relevant regulations. This governance framework ensures that data is used ethically and legally.

Trust and Transparency

Data spaces are built on trust among participants. Mechanisms such as verifiable credentials and audit trails provide transparency and accountability, ensuring that data transactions are reliable and traceable.

New data space participants usually undergo onboarding services and Know Your Customer (KYC) processes to verify their identity. This enhances trust and ensures that only authorized entities can access and share data. It can also serve as a proxy Legal Entity Identity in other contexts.

Legal Person Identity

Legal organizational identity plays a foundational role in traceability and the digital product passport in two key ways:

First, the exchange of data between two parties must be secure and efficient, particularly for sensitive traceability data. This exchange needs to happen in a peer-to-peer manner rather than aggregating data about an entire supply chain in a central database. Therefore, both parties must properly authenticate each other before initiating a data exchange.

The eIDAS2 regulation in Europe (EU Regulation 2024/1183, 2024), which includes a digital wallet for enterprises, will facilitate this authentication process by making it digital, automated and secure. Pilots, such as the large-scale EWC pilot, are already testing the issuance of digital credentials directly from official commercial registries as part of the eIDAS2 regulation.

Data spaces depend on automated and digital authentication between partners. In the absence of current organizational digital identity, they provide onboarding services where





a digital credential is issued to an organization after a manual KYC process by an onboarding service provider. This credential can then be used for authentication and interactions within the data space.

Second, legal organizational identity provides a root of trust for all data that is created and exchanged. With legal organizational identity, the digital signatures of every single data point can be traced back to an official legal identity. This is crucial for increasing data trust, combating fraud, and significantly reducing the compliance risk and cost of due diligence for all stakeholders involved.

2.5. SSI

Self-Sovereign Identity (SSI) is an innovative identity management model that empowers users with full control over their personal data and identity credentials. Unlike traditional identity management systems, where organizations or third-party providers control users' identities, SSI enables direct connectivity between users and organizations. This model emphasizes user ownership and control through the use of digital wallets, which securely store verifiable credentials and decentralized identifiers that facilitate a cryptographically verifiable digital identity (Naik & Jenkins, 2020).

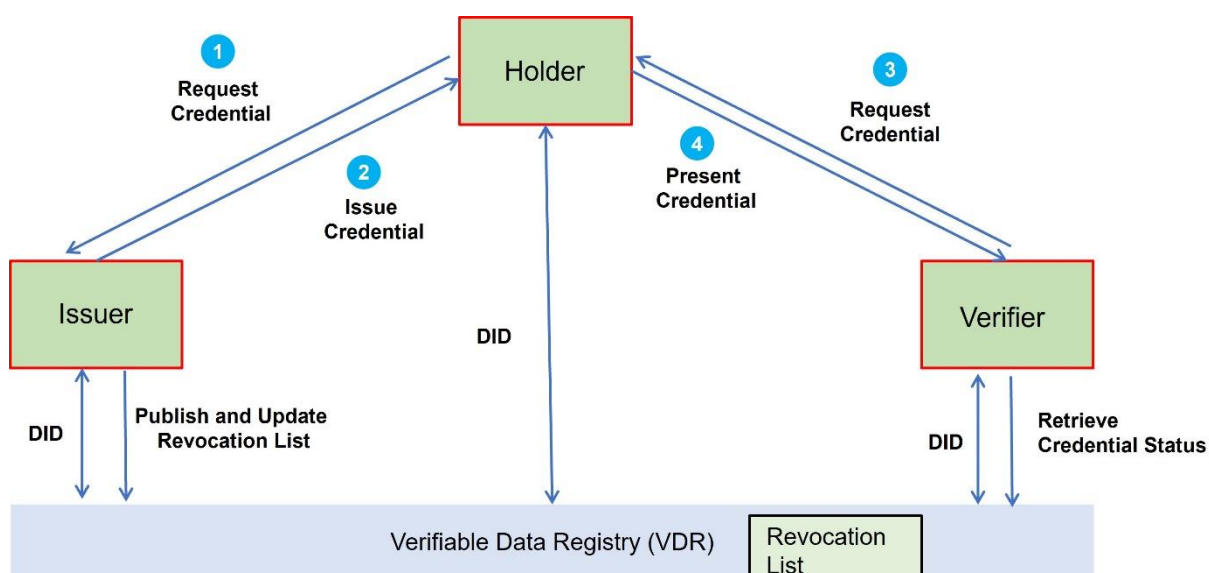


Figure 1 - Interaction of Actors in the SSI Model

The SSI model assigns three key roles: the Issuer, the Holder, and the Verifier. The Issuer is responsible for creating and issuing credentials to the Holder. The Holder then receives these credentials and shares them with the Verifier, who verifies the credentials presented by the Holder. This framework not only enhances privacy but also supports transparency



and trust in digital interactions (Allen, 2016). In the architecture presented in Figure 1, entities are identified by their DIDs. This includes issuers, holders and verifiers. This ensures transparency and accountability, as requests and presentations can be traced back to the individuals who initiated the process. DIDs can be anchored in a Verifiable Data Registry (VDR), which is a decentralized, secure system that stores and provides access to cryptographically verifiable data, thus ensuring its authenticity and integrity. Consequently, DIDs can be resolved by querying the corresponding VDR. Furthermore, a VDR permits the publication of revocation status for credentials in a privacy-preserving manner.

According to Christopher Allen (Allen, 2016), the guiding principles of SSI include:

- **Existence:** Users must have an independent existence, with their identity not solely defined in digital form.
- **Control:** Users have the authority to manage their identities, allowing them to refer to, update, or hide their information as they see fit.
- **Access:** Users should always be able to retrieve their data without gatekeepers or hidden information.
- **Transparency:** Systems governing identities must be open and easily understandable, fostering trust.
- **Persistence:** Identities should be long-lived, allowing users to maintain their identities over time.
- **Portability:** Users must be able to transport their identities across different platforms without being tied to a single provider.
- **Interoperability:** Identities should be usable across various systems and contexts, enhancing their value.
- **Consent:** Users must consent to any sharing of their identity information, ensuring that they have control over their data.
- **Minimalization:** The disclosure of claims must be minimized, sharing only what is necessary for a given transaction.
- **Protection:** The rights of users must be prioritized over the needs of the identity network, ensuring freedoms and rights are preserved.

Overall, SSI presents a transformative approach to identity management that aligns with modern demands for privacy, control, and security in an increasingly digital world. By leveraging the principles of SSI, organizations can build systems that not only enhance user sovereignty but also support ethical data practices.





2.6. Traceability

Definition and Rationale

Traceability involves identifying the provenance of materials and who has handled them, allowing for the determination of where and from which circumstances the materials originate. Traceability depends on the processes of tracking the history, location, and application of products, materials, and components throughout the supply chain. It is essential for determining the proof of origin of materials, due diligence requirements, and calculating important metrics, such as the product carbon footprint, at both the item and product levels. Without traceability, it is impossible to accurately determine the mass balances of raw materials, each with different carbon footprints, and subsequently calculate the carbon footprint of the final product.

The paper trail that records the sequence of individuals and companies that take custody of the minerals in the process of moving along the supply chain is called the chain of custody (CoC). Traceability is also crucial for due diligence requirements and for certification bodies that issue CoC certifications, like the CoC that is part of CERA4in1. These certifications require detailed data on the provenance and journey of materials to ensure compliance with sustainability and ethical standards.

Traceability Events

Traceability events are specific actions or occurrences that are recorded to track the flow of materials and products through the supply chain. According to the UN Transparency Protocol², there are several key types of traceability events, each with its own set of data requirements and implications for supply chain transparency:

- **Transaction Events:** These events capture the transfer of ownership or custody of goods from one party to another. They are crucial for maintaining accurate records of where and when products change hands.
- **Transformation Events:** These events document the conversion of raw materials into finished or intermediate goods. They provide detailed insights into the production process, ensuring that the origins and transformation of materials are traceable.

² <https://uncefact.github.io/spec-untp/>





- **Aggregation Events:** These events track the grouping of individual items into larger units, such as cases or pallets, and their subsequent disaggregation. This is important for managing inventory and logistics.
- **Association Events:** These events capture the relationships between different products or components, such as assembling parts into a final product. They help in tracking the composition and assembly of complex products.

By recording these events, companies can maintain a comprehensive and transparent record of their supply chains, which is essential for compliance, quality control, and sustainability efforts.





3. Relevant EU Regulations

This chapter provides an overview of regulations relevant to the implementation of Digital Product Passports, highlighting their scope, adoption, and significance across various industries, in line with the European Green Deal (European Commission, 2019).

3.1. European Battery Regulation and Battery Passport Technical Guidance

The regulatory framework established by the European Battery Regulation and the accompanying technical guidance are summarized in this section. As mentioned in Section 2.5, European battery regulation makes critical raw material traceability a key regulatory requirement. The regulation (European Commission, 2023) states that critical raw materials present in the battery shall be publicly available via the battery passport and information on responsible sourcing as indicated in the report on battery due diligence policy. The report mentioned in the regulation shall cover, where relevant, access to information, public participation in decision-making and access to justice in environmental matters in relation to the sourcing, processing and trading of the raw materials present in batteries. On the other hand, the Battery Passport Technical Guidance (European Commission, 2024) provides detailed specifications and standards for implementing digital battery passports as required by the EU Battery Regulation. It outlines the necessary data attributes, technical infrastructure, and compliance requirements to create and manage digital product passports for batteries.

The Battery Passport Technical Guidance is crucial for the battery industry, particularly for manufacturers of EV and industrial batteries. With the regulation coming into effect in 2027, this guidance helps companies prepare for compliance by detailing the required information and technical standards. The guidance promotes sustainability and circularity by ensuring that all relevant data, from carbon footprints to supply chain due diligence, is accurately captured and reported. The critical raw material traceability architecture is an essential component of this process, as it aims to ensure that the origin and journey of raw materials used in battery production are transparent and verifiable, thus supporting responsible sourcing practices and regulatory compliance.



3.2. Corporate Sustainability and Due Diligence Directive

The Corporate Sustainability and Due Diligence Directive (European Parliament and Council, 2024a) complements the European Battery Regulation from a product-related value chain due diligence perspective, highlighting the mitigation processes for adverse human rights and environmental impacts in their value chains. This directive aims to improve corporate governance practices to better integrate risk management and mitigation processes in their own operations and value chains. The risks considered here include human rights issues such as forced labour, child labour, inadequate workplace health and safety, exploitation of workers, and environmental impacts such as greenhouse gas emissions, pollution, or biodiversity loss and ecosystem degradation. Other main objectives of the directive are to avoid fragmentation of due diligence requirements and to increase corporate accountability for adverse impacts by ensuring coherence for companies regarding obligations under existing and proposed EU initiatives on responsible business conduct.

The directive extends the supply chain due diligence policies of the Battery Regulation by introducing a value chain due diligence related to raw materials that are not covered in that regulation but without requiring certification for placing the products on the EU market. The directive covers all adverse human rights and environmental impact throughout the lifecycle of production and use and disposal of product or provision of services, at the level of raw material sourcing, manufacturing, or at the level of product or waste disposal, but it is not limited to the companies' own operations, subsidiaries, and products. It covers all activities related to the production of a good or provision of services by a company, including the development of the product or the service and the use and disposal of the product. The directive encompasses all related activities of upstream and downstream business relationships of the company. The upstream established direct and indirect relationships refer to the design, extraction, manufacturing, transportation, storage and supply of the raw material, products, parts of products and the relevant services to carry out the company's activities. The downstream relationships include established direct and indirect business relationships that use or receive products, parts of products or services from the company up to the end of life of the product, including the distribution of the product to retailers, the transport and storage of the product, dismantling of the product, its recycling, composting or landfilling.



3.3. Ecodesign for Sustainable Products Regulation (ESPR)

Emphasizing the need for a secure supply of raw materials, the Ecodesign for Sustainable Products Regulation (European Parliament and Council, 2024a) is in line with the EU's transition target to reduce the overall material footprint, which refers to the total amount of raw materials extracted to meet final consumption demands. To reduce the dependency in raw materials and embed circularity across the economy, the regulation aims to promote the use of recycled and recovered critical raw materials to improve the product in terms of reaching the sustainability targets.

This Regulation establishes a legislative framework and provides for the setting of new eco-design requirements to increase the energy and resource efficiency of products, including the possibility of recovery of strategic and critical raw materials, reduce their expected generation of waste and increase the recycled content in products, while ensuring their performance and safety. In meeting performance requirements, the regulation underscores the digital product passport as a crucial tool for enhancing product sustainability and compliance with the standards, and to improve the traceability of products along the value chain.

Essential requirements for the DPP system are defined in Articles 8 to 13 of the draft text of the regulation. The main characteristics of the DPP system are:

- A persistent unique product identifier (Art.9 (1a))
- A machine-readable data carrier (Art.9 (1b) & (1c)) based on standards
- Use of open standards (Art.9 (1d))
- An open interoperable data exchange network without vendor lock-in (Art.9 (1d))
- Technical, semantic and organisational aspects of end-to-end communication and data transfer
- Interoperable and machine-readable data formats (Art.10 (1a))
- Free of charge and easy access, based on defined access rights (Art.10 (b))
- No secondary use without consent (data usage control) (Art.9 (1da))
- Decentralized data storage, meaning information stored by the Registered Entity Operators or a certified independent third-party product passport service providers authorised to act on their behalf (Art.10 (c) & (d))





- Archiving: Availability of a back-up copy through a certified independent third-party DPP service provider (Art. 9 (3a))
- DPP information points may be either static or dynamic (updatable)
- DPP information points may be either public or have restricted access conditions.

The information requirements in the regulation shall provide that products can only be placed on the market or put into service if a DPP is available, and the DPP must be linked through a data carrier to a persistent unique product identifier. Furthermore, the technical design and operation of the digital product passport must meet the interoperability, accessibility, storage, availability, data integrity, security and privacy requirements. All data in the passport must be based on open standards without vendor lock-in and access to the data in the passport must be regulated according to specific access rights.

By July 19, 2026, the European Commission will create a secure digital registry that stores at least the unique identifiers for products. For products intended for customs procedure 'release for free circulation', the registry will also store the corresponding commodity code and unique identifiers for batteries. Economic operators responsible for placing products on the market must upload the required data to the registry. Upon uploading data, the registry will automatically communicate a unique registration identifier to the economic operator. In addition, the European Commission will establish and manage a publicly accessible web portal that enables stakeholders to search for and compare data contained in DPPs.





4. Ecosystems and standards initiatives

This section explores various ecosystems and standardization initiatives that play a critical role in the development and implementation of DPPs and traceability solutions. These initiatives aim to address the demands of EU regulations, and they contribute to the integration of DPPs into existing systems by establishing common frameworks, guidelines, and standards that enable seamless interoperability, data exchange, and compliance with regulations.

While these organizations play crucial roles in developing and promoting standards for battery DPPs, the degree of regulatory mandates they operate under depends on the incorporation of their standards into binding regulations. The JTC 24's standards become mandatory when adopted into legislation; however, the adoption of these standards is voluntary. The Battery Pass Consortium's work is closely aligned with the EU Battery Regulation's requirements, providing a framework for compliance. CIRPASS also aligns with the EU Battery Regulation guidance but is without regulatory authority, unless their work is referenced in legislation. Global Battery Alliance standards and guidelines are voluntary and serve as recommendations provides voluntary recommendations.

4.1. Joint Technical Committee - JTC 24

European Committee for Standardization (CEN) and European Committee for Electrotechnical Standardization (CENELEC) are two key organizations responsible for developing and maintaining European standards across various sectors for different product categories, including essential attributes for transparency and compliance with EU regulations. The compliance of DPPs with new regulations outlined in Chapter 3, such as the EU Battery Regulation and the Ecodesign for Sustainable Products Regulation, falls under the scope of standardization bodies. Consequently, the European Commission has issued a standardization request to ensure alignment with these regulatory requirements (European Commission, 2024).

As required by the draft Standard Requirements, the CEN-CENELEC Joint Technical Committee (JTC 24) was established in December 2023 to develop the standards and a harmonized technical framework for the DPP systems, facilitating the implementation of traceability and sustainability across various sectors, particularly focusing on products like batteries and electronics. This decision was made due to the timing requirements set forth in the Battery Regulation demand the availability of an operational DPP system for batteries





by 18 February 2027. As a result, there is a strict deadline for the availability of technical standards on DPP by 31 December 2025. This would provide stakeholders in the battery industry just under 14 months for the implementation, testing and launch of their DPP system.

JTC 24 focuses on the development of deliverables for the DPP framework and system, based on but not limited to standards on: unique identifiers, data carriers and links between physical product and digital representation, access rights management, information, system security, and business confidentiality, interoperability (technical, semantic, organisation), data processing, data exchange protocols and data formats, data storage, archiving, and data persistence; data authentication, reliability, integrity, Application Programming Interfaces (APIs) for the product passport lifecycle management and searchability, the data delivering system, and data specification method while ensuring cross-sectoral and cross-system interoperability.

JTC 24 is part of a broader regulatory ambition to ensure products contribute to circular economies and sustainability goals. The focus of JTC 24 is to ensure interoperability between DPPs across sectors, making it easier for stakeholders to access and utilize product information, thus promoting sustainability and reducing environmental impact. The committee's work will be vital in supporting the transition toward more transparent and responsible production and consumption practices within the EU market.



4.2. Battery Pass Consortium

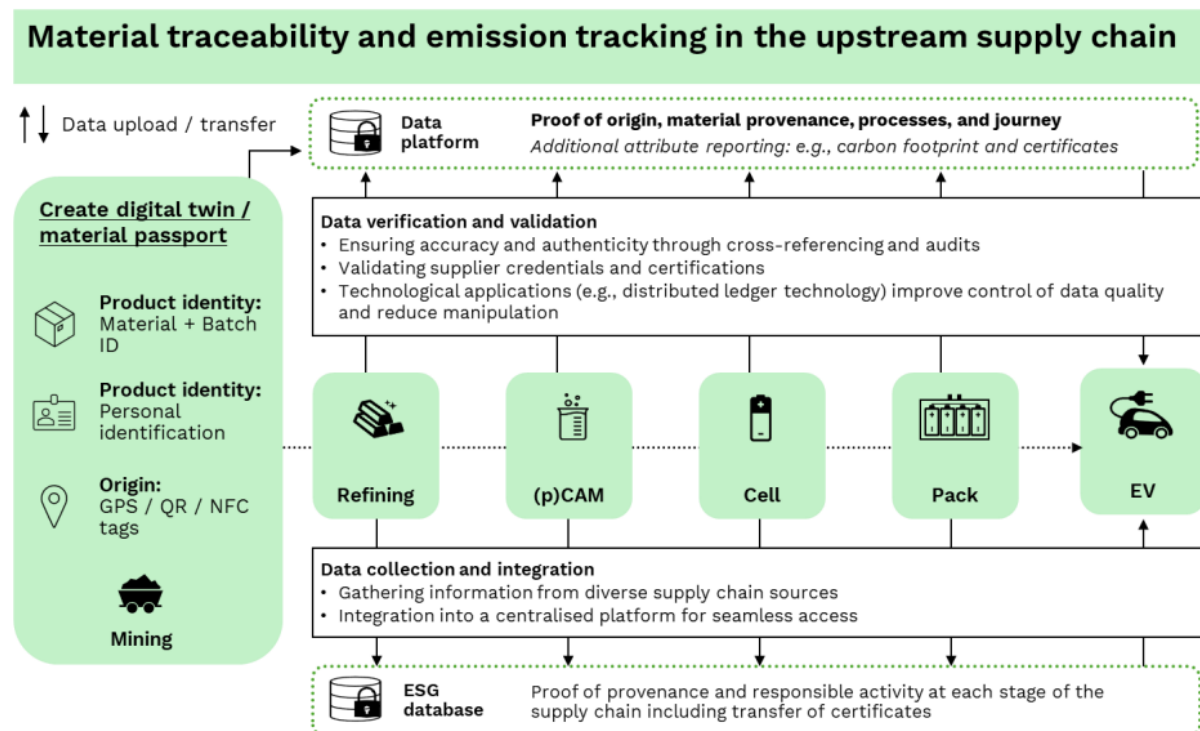


Figure 2 - Battery Pass Digital Data Chain in a Traceability System (Battery Pass Consortium, 2024)

The Battery Pass Consortium is dedicated to developing the technical standards and content guidance necessary for the implementation of the EU Battery Passport, which is mandated by the EU Battery Regulation (see Section 3.1). The consortium comprises leading organizations from industry, technology, and academia, and it focuses on enhancing sustainability and circularity in the battery value chain. In this section, Battery Pass Consortium's system architecture and the supply chain data acquisition concepts presented in Battery Passport Technical Guidance (Battery Pass Consortium, 2024) are summarized.

Battery Passport Technical Guidance outlines the essential technical standard building blocks necessary for the implementation of a DPP system, called Technical Standard Stack. The document also proposes that the Technical Standard Stack not only applies to battery passports but serves as a foundation for digital product passports in general. The Technical Standard Stack comprises of the following building blocks:

1. Domain Data Ecosystem: Describes the ecosystem of relevant data for battery passports and their interrelations.



2. Responsibilities and Rules: Outlines the roles and rules governing data management within the DPP system.
3. Processes: Discusses the processes involved in the DPP system.
4. Core Passport Software Services and Application Programming Interfaces: Focuses on software services and APIs required for the DPP.
5. Identity and Access Management: Details the systems for managing user identities and access rights.
6. Data Integration, Distribution, Exchange, and Protocols: Covers how data is integrated and exchanged across the system.
7. Data Storage and Persistence: Addresses the methods for storing DPP data securely.
8. Data Processing: Discusses how data within the DPP is processed.
9. Data Models and Data Formats: Focuses on the structures and formats of data used in the DPP.
10. Unique Identifiers: Details the identifiers used to uniquely reference products.
11. Data Carriers: Discusses the physical media used to store DPP information.
12. Policy Management and Enforcement: Covers the rules governing the DPP.
13. IT Governance: Discusses the governance structures for IT within the DPP system.
14. Security Infrastructure: Addresses the security measures necessary for protecting DPP data.

The DPP system architecture proposed in Battery Passport Technical Guidance is divided into three main components:

1. European Commission Central Services: These services are managed by the European Commission and are integral to the functioning of the DPP system. They serve as the foundational support for the overall architecture. Some examples are Identity and access control, data services, registry, and policy management services.
2. Distributed DPP System Services: These services must be established and operated by economic operators or designated service providers. They are crucial for the decentralized operation of the DPP, allowing for effective data management and accessibility. Some examples are distributed data repositories and economic operator portal.
3. Third-Party Services: These services are provided by independent third-party operators and are essential for supporting the DPP system, particularly regarding data backup and management.



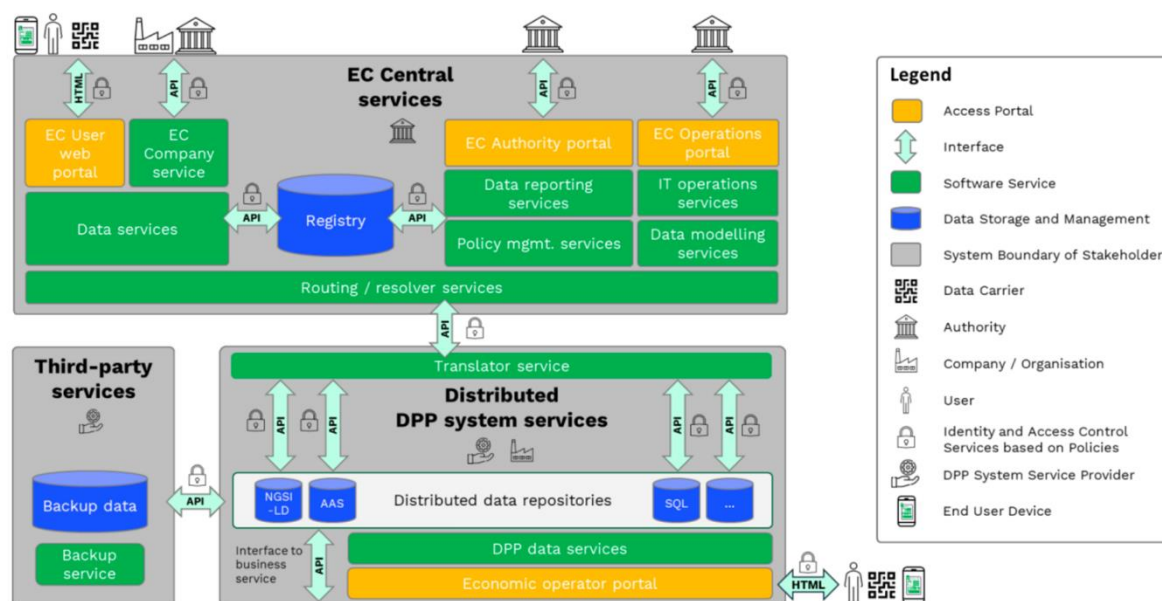


Figure 3 - Battery Passport Technical Guidance Principal System Architecture (Battery Pass Consortium, 2024)

The battery passport architecture shows that there are several different APIs necessary to operate the battery passport ecosystem. In general, we distinguish three different categories of APIs:

1. APIs operating with the implementation of a technology agnostic canonical data model of the battery passport.
2. APIs operating with the implementation of individual data models from different co-existing standard APIs, e.g. the Asset Administration Shell (implemented in Catena-X)
3. Other supporting APIs. No selection or recommendation of standard APIs is currently possible for supporting APIs.

Apart from DPP system architecture, Battery Passport Technical Guidance also defines a supply chain transparency system as a mechanism or set of processes and tools that enables tracking and tracing the flow of products, materials, and information across the various stages of a supply chain by integrating data, tracking product components and raw material, and sharing information. Existing and upcoming regulations require the following information from an effective supply chain transparency system:

- **Data Collection and Integration:** Gathering information from various supply chain sources, which involves consolidating this data into a centralized system.



- **Data Verification and Validation:** Ensuring the accuracy and authenticity of the data collected, which may involve audits and cross-referencing.
- **Digital Records and Identification:** Assigning unique identifiers to products or batches, which are linked to relevant data points for tracking. This can be a unique serial number encoded with optical machine-readable digital identifiers such as barcode, QR code, or RFID tags.
- **Tracking and Tracing:** As products move through the supply chain, digital identifiers are scanned at different checkpoints to maintain a chronological record of the product's journey and associated data, such as material origin and carbon footprint.
- **Real-Time Visibility:** Utilizing modern technologies like IoT sensors and GPS tracking for up-to-date tracking of products within the supply chain.
- **Data sharing and collaboration:** Supply chain transparency involves collaboration among different stakeholders, including suppliers, manufacturers, logistics partners, and consumers.
- **Distributed ledger technology (optional):** Some supply chain transparency systems leverage distributed ledger technology (DLT) to enhance data security
- **Reporting and analytics:** The collected data are analysed to generate insights and reports and to mitigate risks through early insights which helps to strengthen the resilience of supply chains.
- **Transparency for consumers:** Data from supply chain transparency systems can be aggregated to individual data points in the battery passport to extend visibility to end consumers.

4.3. CIRPASS

The CIRPASS project is focused on the development and implementation of DPPs. One of the project's key objectives is to define a cross-sectoral product data model for DPPs that aligns with circular economy principles. The project emphasizes the need for a robust data exchange protocol tailored to the needs of circular economy stakeholders.

The D3.2 DPP System Architecture document (CIRPASS, 2024) outlines the information system architecture for Digital Product Passports (DPP), focusing on two primary architectures based on HTTP URIs and DIDs. The requirements for the DPP System, such as a persistent unique product identifier, a machine-readable data carrier, and compliance with open standards, stem from the ESPR regulation summarized in Section 3.3. Based on these requirements, CIRPASS builds its system architecture on basic design principles such





as a decentralized approach, in which data is primarily stored with the product creator but is also accessible through a central registry. This design incorporates user stories to accommodate various stakeholders, including customs authorities and market authorities, as depicted in Figure 5. The DPP structure includes multiple components such as the responsible economic operator (REO), data users, and the European registry. The REO plays a crucial role in managing access rights and ensuring that accurate information is recorded and maintained.

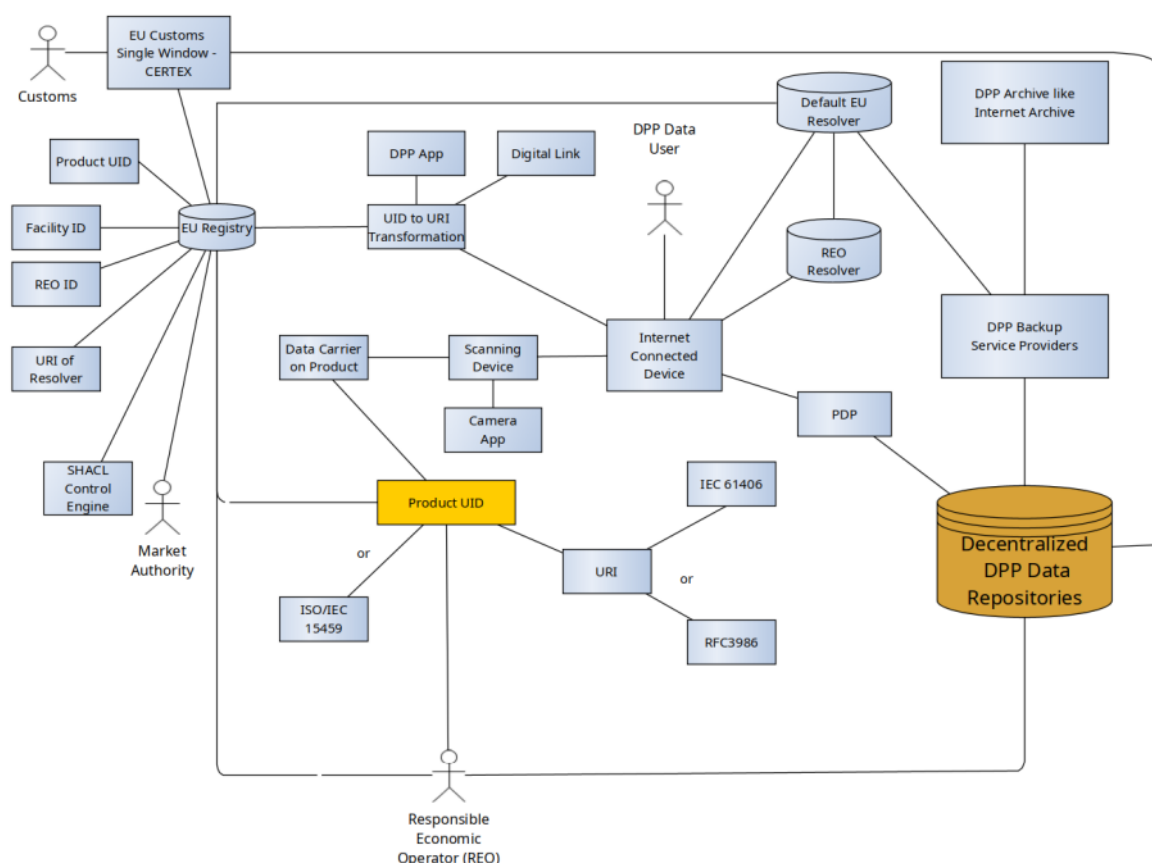


Figure 4 - Structural View of DPP System with Structure, Actors and Components (CIRPASS, 2024)

In CIRPASS System Architecture, the DPP is conceptualized as a knowledge graph, which organizes information in the form of semantic triples (subject, predicate, object). This structure allows for dynamic updates and enhances interoperability through linked data principles. As any Object can become the Subject of a new assertion, graphs can grow as new information is added. 'Subjects' and 'Objects' are referred to as "nodes" of the graph, whereas 'Predicates' are referred to as "edges" of the graph. When each Subject, Predicate, and Object of each assertion is defined by a URI, the knowledge graph is expressed in the form of Linked Data

The DPP knowledge graph is data organized as a graph, and Vocabularies describe what the semantics in that graph mean. Once the vocabularies are defined, ontologies allow to describe the relation between certain objects in the graph or between objects of distinct graphs. This can be very useful when merging data from several sources. But it is not limited to merging and fuels reasoners that can automatically draw conclusions from semantics and relations as encoded in vocabularies and ontologies.

The knowledge graph puts data points in relation to each other with this structure, resulting in a higher interoperability. The proposed architecture aims to create an interoperability layer that does not impose specific rules but utilizes existing web technologies. This layer facilitates the transformation of data formats, promoting collaboration across different systems without vendor lock-in. The document proposes the use of Resource Description Framework (RDF) as the data format, but other solutions are not ruled out. Furthermore, a validation engine is proposed to ensure the correctness of the DPP data through the use of standards like RDF Schema and Shapes Constraint Language (SHACL), allowing various stakeholders to verify compliance efficiently.

4.4. Global Battery Alliance

The Global Battery Alliance (GBA) is a public-private collaboration platform established in 2017 at the World Economic Forum. It aims to create a sustainable battery value chain by 2030, bringing together international organizations, including NGOs, industry players, academics, and government representatives³. The guiding principles of GBA emphasize key aspects including transparency regarding the sourcing and recycling of battery materials, maximizing resource productivity, and promoting a circular economy. These principles align with the digital passport concept by facilitating the tracking of raw materials, thus enabling stakeholders to verify compliance with sustainability and ethical standards throughout the battery lifecycle. Furthermore, the GBA launched the Critical Minerals Advisory Group (CMAG) in 2022 to ensure that critical materials are produced, sourced, processed, transported, manufactured and recycled in a responsible and sustainable manner.

The GBA is developing the Battery Passport to enhance transparency in the battery value chain, facilitating the tracking of materials, carbon footprints, and compliance with sustainability standards. In 2023, at the Annual Meeting of the World Economic Forum, the Global Battery Alliance officially launched the world's first battery passport proof-of-concept

³ <https://www.globalbattery.org/about/>



pilots (Global Battery Alliance, 2023a), that contain key sustainability performance indicators related to the battery carbon footprint and child labour and human rights due diligence as set out in the Greenhouse Gas rulebook (Global Battery Alliance, 2023b) and the Child Labour (Global Battery Alliance, 2022a) and Human Rights (Global Battery Alliance, 2022b) indices. The key observations from the battery passport proof-of-concept pilots can be summarized as follows:

- **Transparency in the Value Chain:** The Battery Passport aims to provide a digital twin of physical batteries, enhancing transparency regarding material provenance, chemical composition, and sustainability performance. The pilots highlighted the importance of accurate data collection for ensuring material provenance and sustainability performance.
- **Data Collection and Reporting:** The piloted greenhouse gas calculation method achieved advancements in accurately assessing emissions during the immediate assembly process and enabled tracking of greenhouse gas emissions for specific materials and processes.
- **Interoperability:** The key observation regarding interoperability from the GBA pilots is that while technical challenges were anticipated, addressing basic content readiness proved to be more complex. Significant efforts were made to establish data taxonomy and consistent units across geographies. The pilots demonstrated the feasibility of aggregating data from multiple IT solutions, though data governance issues remain.
- **Pilot Results:** The report Proof-of-concept pilots demonstrated the feasibility of the Battery Passport, showcased the successful end-to-end tracking and tracing capabilities for materials like cobalt and lithium. These pilots involved collaboration among industry stakeholders, including mining companies, battery manufacturers, and technology providers. An example of the battery passport pilot is illustrated in Figure 5⁴.

⁴ <https://www.globalbattery.org/battery-passport-poc-pilots/pilot-3/>






BATTERY		MATERIALS		ESG	DATA
VALUE CHAIN	IDENTITY	MATERIAL FLOW	ESG DATA	DATA VERIFICATION	MATERIAL FLOW AGGREGATION
Mining	known	traced	estimated	(1/3) basic	individual battery
Refining	known	traced	estimated		
Precursor	known	traced	estimated		
CAM	known	traced	estimated	TRACEABILITY (2/3) med	START OF PERIOD 11/1/2021
Cathode	known	traced	estimated		END OF PERIOD 12/1/2022
Anode	known	partial	estimated		
Cell	known	traced	reported	INTEROPERABILITY (0/3) low	DATA COLLECTION ASSURED BY 
Module	known	traced	reported		
Battery	known	traced	reported		

Figure 5 - Global Battery Alliance PoC Tracing Data Example

- **Continuous Improvement:** The pilots identified lessons learned and areas for improvement, underscoring the importance of stakeholder collaboration and standardized data reporting.



5. Technical Standards

5.1. W3C Verifiable Credentials

W3C Verifiable Credentials (W3C, 2021) are tamper-evident credentials whose authorship can be cryptographically verified, allowing them to serve as reliable digital representations of physical credentials. They can encapsulate the same information found in traditional credentials, enhanced by technologies like digital signatures, which increase their trustworthiness and resistance to tampering. A verifiable credential comprises one or more claims made by a single entity, accompanied by identifiers and metadata detailing aspects such as the issuer, validity periods, representative images, and status information. Examples of verifiable credentials include digital employee IDs, driver's licenses, and educational certificates, all designed to support the creation of verifiable presentations that can also be cryptographically validated.

Verifiable credentials express properties related to one or more subjects and the credentials themselves. The specification defines several key properties, including *@context*, which provides the context of the credential; *id*, which serves as a unique identifier; *type*, indicating the category of the credential; and *name* and *description* for human-readable details. Additionally, properties like *issuer*, which denotes who issued the credential, and *credentialSubject*, specifying the subject of the claims, are included. Other relevant properties cover validity periods (*validFrom* and *validUntil*), *status*, which indicates the current state of the credential, and *credentialSchema*, detailing the structure of the credential. The specification also allows for the inclusion of a *refreshService* for updates, *termsOfUse*, and evidence to support the claims made. Moreover, verifiable credentials can be customized with additional properties through an extensibility mechanism.

As explained in Section 2.5 for the SSI model, the trust model of the verifiable credentials' ecosystem assigns three key roles: the Issuer, the Holder, and the Verifier. The Issuer is responsible for creating and issuing credentials to the Holder. The holder of a verifiable credential operates in a triangle of trust, in which the issuer trusts the holder, the holder trusts the verifier, and the verifier trusts the issuer.

The Verifiable Credentials Data Model v1.1 (W3C, 2021) outlines a standardized method for expressing secure, privacy-respecting, and machine-verifiable credentials on the web. It details essential components such as issuer information, subjects, claims, and cryptographic proofs to ensure data integrity, making it adaptable for various credential types. The



subsequent version, Verifiable Credentials Data Model v2.0 (W3C, 2023), builds on this foundation by refining the specifications and enhancing privacy considerations. This iteration facilitates improved interoperability and expands the mechanisms for credential verification, thereby enabling secure digital interactions across multiple platforms. Together, these frameworks provide a robust structure for managing digital identities effectively

5.2. Decentralized Identifiers

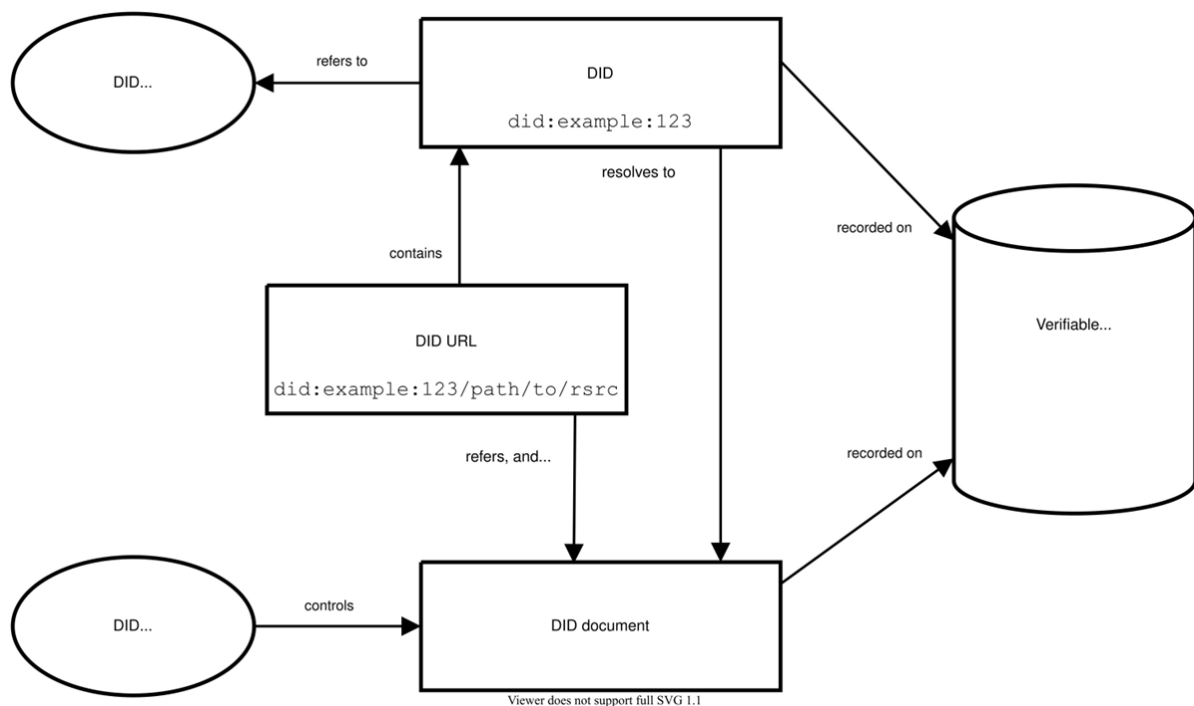


Figure 6 - Overview of DID architecture and the relationship of the basic components (W3C, 2022)

A Decentralized Identifier (DID) is a globally unique identifier, which is resolvable with high availability and cryptographically verifiable (W3C CCG, 2020). DIDs are typically associated with cryptographic material, such as public keys, and service endpoints, for establishing secure communication channels. DIDs are useful for any application that benefits from self-administered, cryptographically verifiable identifiers. Current commercial deployments of W3C Verifiable Credentials heavily utilize Decentralized Identifiers to identify people, organizations, and things and to achieve a number of security and privacy-protecting guarantees.

W3C DID specification (W3C, 2022) details the framework for decentralized identifiers, including the architecture, data model, and representation of DIDs, and highlights their role



in enabling individuals and organizations to create identifiers without relying on a centralized authority. According to this document, a DID is a simple text string consisting of three parts: 1) the did URI scheme identifier, 2) the identifier for the DID method, and 3) the DID method-specific identifier. As shown in Figure 5, DIDs are linked to DID documents, which contain essential information about the DID and its subject, including verification methods and services for interaction. A DID URL extends this concept by adding URI components, allowing for the identification of specific resources, such as cryptographic keys. The subject of a DID is the entity it identifies, which can range from individuals to organizations, while the DID controller is the entity authorized to modify the DID document, often through cryptographic keys.

DIDs are stored in verifiable data registries, such as distributed ledgers or peer-to-peer networks, enabling their resolution to DID documents. This resolution process is managed by a DID resolver, which converts a DID into its corresponding document. Similarly, a DID URL dereferencer transforms a DID URL into a resource. The framework for creating, updating, and deactivating DIDs is defined by specific DID methods, which are documented separately.

5.3. Verifiable Credentials API

The W3C Credentials Community Group Verifiable Credential APIs are a set of RESTful API definitions conforming with the OpenAPI 3.0 Specification that support Verifiable Credential Lifecycle Management such as Issuing, Holding/Presentation/Exchange, and Verification for the roles of Issuer, Holder, and Verifier as described in the Verifiable Credential Data Model specification (W3C CCG, 2023). The API aims to facilitate interoperability across various implementations and enhance privacy and security measures in handling digital credentials.

The architecture of VC API is structured around three primary roles: the Issuer, the Holder, and the Verifier. Each role interacts with various services designed to manage Verifiable Credentials throughout their lifecycle. The architecture supports different services such as:

- Issuer Service: Manages the issuance of Verifiable Credentials, requiring access to private keys for creating cryptographic proofs.
- Verifier Service: Handles the verification of credentials and presentations, ensuring authenticity and timeliness.





- Holder Service: Facilitates the creation of Verifiable Presentations from stored credentials.
- Status Service: The Status Service provides a mechanism for checking and publishing the status of issued Verifiable Credentials in a privacy-preserving manner, aiding Verifiers in assessing credential validity

Additionally, the architecture incorporates a Storage Services for securely storing credentials. The document also acknowledges the need for configuration and management interfaces for the various components of the API, although specifics on these interfaces are currently out of scope.

5.4. DID Comm

The purpose of DIDComm Messaging is to provide a secure, private communication methodology based on the decentralized design of DIDs (DIDComm Messaging, 2023). DIDComm Messaging enables higher-order protocols that inherit its security, privacy, decentralization, and transport independence for decentralized identity solutions by facilitating peer-to-peer exchanges.

The design of DIDComm Messaging focuses on several key principles: it aims to be secure by ensuring message integrity, authenticity, and the use of advanced cryptography, allowing both repudiable and non-repudiable messages, while also enabling outcomes similar to perfect forward secrecy. Privacy is prioritized by preventing unauthorized third parties from accessing the content and allowing sender anonymity. The protocol is decentralized, relying on control of decentralized identifiers for trust rather than centralized authorities like certificate authorities or identity providers, and it is transport-agnostic, functioning over various channels such as HTTPS, WebSockets, and even offline methods. DIDComm Messaging is also routable, enabling communication between parties without direct connections, while ensuring interoperability across different programming languages, platforms, and cryptographic schemes. It supports extensibility for developers, allowing easy customization and the creation of higher-level protocols that inherit its security guarantees, all while maintaining efficiency in resource usage.



5.5. Eclipse Data Space Connector

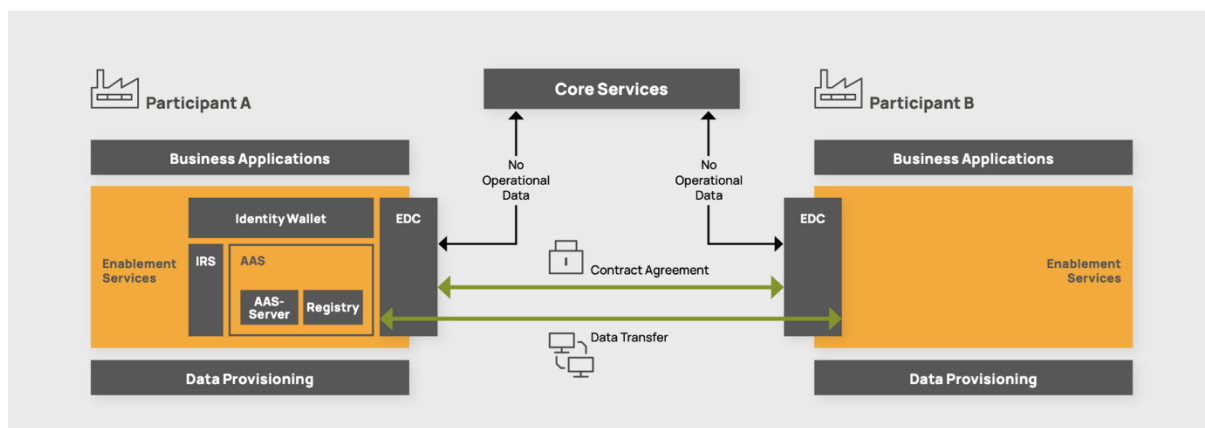


Figure 7 - Catena-X Data Exchange Framework with Eclipse Dataspace Connector and Asset Administration Shell (Catena-X, 2023)

The Eclipse Data Space Connector (EDC) serves as a central communication component for the Catena-X ecosystem, enabling secure, sovereign data exchange between organizations while emphasizing principles like simplicity, interoperability, and decentralization. It maintains a minimal core with few external dependencies, ensuring that necessary software components reside on the partners' side and that data is only exchanged under agreed contracts, highlighting that data protection takes precedence over data sharing. It establishes consistent semantics to support interoperability and digital value creation, and seeks to automate all processes, from identity verification to data transmission, leveraging existing standards and protocols such as GAIA-X. Ongoing developments aim to enhance flexibility, including the integration of self-sovereign identity solutions and expanded backend services. It can be assembled as a connector that serves all the requirements of the Catena-X data space.

The EDCs provide a framework, based on the Dataspace Protocol (DSP) specification, for sovereign, interorganizational data exchange. This framework contains modules for performing data queries, data exchange, policy enforcement, monitoring, and auditing. Specifically, it can be integrated with existing identity, data catalog, and transfer technologies to provide compliance, policy, and control capabilities across the network.

The EDC is split up into Control Plane and Data Plane, whereas the Control Plane functions as administration layer and has responsibility of resource management, contract negotiation and administer data transfer. The Data Plane is responsible for transferring and receiving data streams. With this architecture, the EDC facilitates both metadata and data



transfers through separate channels and supports various transmission protocols to enhance throughput rates.

5.6. Asset Administration Shell

The Asset Administration Shell (AAS) is a fundamental concept in Industry 4.0, serving as a standardized digital representation of physical assets (Catena-X, 2023). Maintained by the Industrial Digital Twin Association (IDTA), the AAS is a set of API methods and resources to have standardized interfaces and semantics to access digital twins. As seen in Figure 6, the AAS plays a pivotal role within the Catena-X ecosystem in enhancing interoperability and data exchange.

To support use cases based on digital twins, participants can register their digital twins in a Digital Twin Registry following the AAS standard. The Digital Twin Registry provides a central source of information like a phone book, where all digital twins and their sub models that contain various aspects of relevant information and services within the data ecosystem, are registered. In addition to registering new digital twins, they can also be found and viewed at this point along with their sub models. The agreed content can be viewed and clearly linked in the Semantic Hub of Catena-X.





6. Reference Architectures

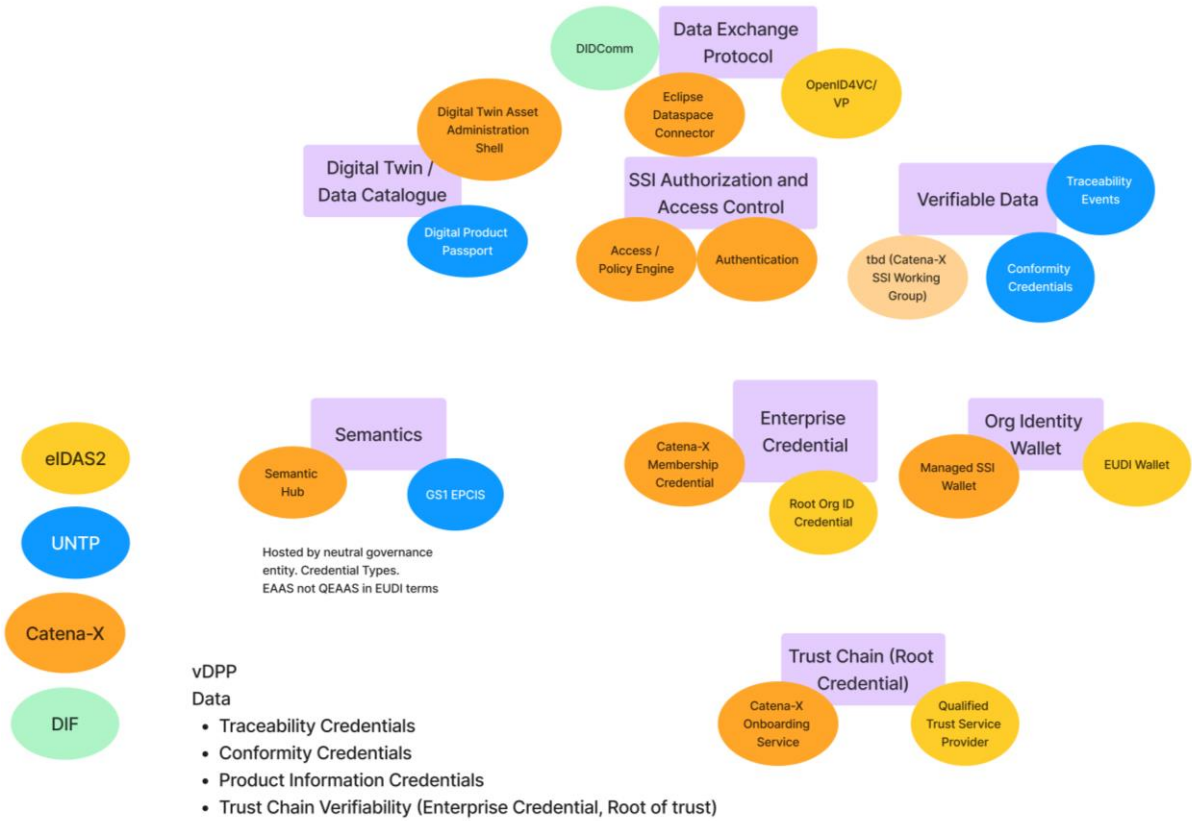


Figure 8- eIDAS2, UNTP, and Catena-X References in Maditrace PoC Architecture

In this section, the existing reference architectures that align with the Maditrace PoC goals, namely European Digital Identity (EUDI) Wallet, Catena-X Data Space, and UN Transparency Protocol are presented. Figure 8 represents a schema that displays how these references architectures are mapped to the Maditrace PoC architecture components, which are detailed in Section 8. The legend with the colours on the left bottom side of the picture shows which concept used in the Maditrace architecture belongs to which reference architecture. Apart from the three references architectures presented in this chapter, DIDComm Messaging explained in Section 5.4 is represented with a separate colour.

6.1. EUDI Wallet Architecture Reference Framework

The European Digital Identity (EUDI) Wallet (European Parliament and Council, 2024b) aims to establish a unified and secure digital identity system across the European Union. This



section explores its overarching scope, its anticipated adoption timeline, and the significant role it plays in advancing traceability through secure, verifiable data handling and interoperability.

6.1.1. Scope

The EUDI Wallet Architecture is designed as a general-purpose digital identity framework, intended to facilitate trusted interactions between individuals, organizations, and government entities across Europe. While its initial aim is to standardize individual digital identities, the EUDI Wallet's scope has expanded to support organizational identities, fostering more secure and reliable interactions within and across industries.

- **Organizational Focus:** The EUDI Wallet's design includes capabilities to issue and manage credentials specific to organizations, enabling businesses and institutions to establish verifiable digital identities. By leveraging open standards (such as Verifiable Credentials and Decentralized Identifiers), the EUDI Wallet can manage a range of organization-specific credentials (e.g., business licenses, ISO certifications), paving the way for its integration into regulatory compliance processes in the supply chain.
- **Interoperability and Security:** The architecture supports secure data exchanges within and beyond the EU, making it suitable for industries with strict data protection requirements. The wallet enables the secure transfer of digital credentials with full traceability, ensuring compliance with EU data regulations and enhancing organizational trust in cross-border transactions.

6.1.2. Adoption and Relevance

The EUDI Wallet is part of the EU's broader Digital Identity framework, supported by the eIDAS regulation to enable cross-border digital identification and authentication. The adoption timeline is structured in phases:

- **Pilot Projects and Early Adoption (2023-2024):** Initial rollout involves pilot projects funded by the EU to test the wallet's utility across sectors, including finance, health, and supply chains. These pilot projects focus on technical interoperability, user acceptance, and organizational feasibility.





- **General Adoption Phase (2025-2027):** Following pilot evaluations, a broader rollout is anticipated, where organizations and individuals can adopt the wallet for official interactions. This phase will likely include governmental mandates for certain sectors, making the wallet a standard tool for regulatory compliance across the EU.
- **Long-Term Integration (Post-2027):** As adoption spreads, the EUDI Wallet is expected to become integral to many sectors, evolving with regulatory updates and potentially influencing digital identity standards globally. This long-term adoption phase will focus on refining the wallet's use cases, including integration with emerging technologies for seamless digital interactions.

6.1.3. Relevance for supply chain traceability

The EUDI Wallet is expected to play a transformative role in traceability within the EU, especially for sectors reliant on supply chain transparency and regulatory compliance.

- **Conformity Credentials:** Since organizations will receive and store their foundational legal entity identity credentials on the EUDI wallet, it is also ideal for storing other relevant organizational conformity credentials such as ISO certifications or Cera4in1. These credentials would then be verifiably linked with the organization's foundational legal identity due to being issued to the same identifier.
- **Digital Product Passports:** Beyond storing credentials, the EUDI wallet also enables organization to create verifiable digital signatures. It can therefore be used for the issuance of verifiable Digital Product Passports, allowing to link a DPP with the responsible economic operator that issued it.
- **Global Case Study:** Given its robust infrastructure and compliance with EU standards, the EUDI Wallet serves as a leading example of digital identity at a jurisdiction level. It can set a strong precedent for other jurisdictions looking to establish similar frameworks for supply chain accountability and traceability.

6.2. Catena-X Data Space Architecture

Catena-X is an initiative aimed at creating a collaborative and secure data ecosystem for the automotive industry. This project focuses on enhancing the efficiency and transparency of the automotive supply chain by facilitating seamless data exchange among manufacturers, suppliers, and service providers. Here are some key features of Catena-X:





1. **Data Ecosystem:** Catena-X provides a standardized platform for data sharing, reducing data silos and improving supply chain visibility.
2. **Collaboration:** It encourages collaboration among various players in the automotive sector, fostering innovation and operational efficiencies.
3. **Interoperability:** The initiative emphasizes interoperability through standardized data formats and protocols, ensuring different systems can work together seamlessly.
4. **Security:** Ensuring data security and privacy is a core aspect, with mechanisms in place to protect sensitive information and comply with regulatory standards.
5. **Sustainability:** Catena-X supports sustainability efforts by providing transparency in the supply chain, helping companies track and reduce their environmental impact.
6. **Industry Support:** Major automotive manufacturers and suppliers back the initiative, highlighting its potential impact on the industry.

By leveraging Catena-X, the automotive industry aims to achieve greater efficiency, innovation, and sustainability through improved data sharing and collaboration and the outcomes of the project is relevant for many concepts that shape the Maditrace architecture.

6.2.1. Scope

In terms of the DPP building blocks, Catena-X provides Data Space modules. Firstly, it provides governance and trust ecosystem services.

- **KYC - Establishing Organizational ID:** Every organisation that wants to become part of Catena-X undergoes a KYC process conducted by a Catena-X onboarding service provider. After successful KYC, the onboarding service issues a Catena-X membership credential to the organisation. The organisation can then use this credential to authenticate itself when interacting with other organisations.
- **Standardised data formats and protocol**
- **Data templates -** Catena-X provides a semantic hub, containing standardized data structures for common data such as the Product Carbon Footprint. This facilitates data exchange and interoperability





6.2.2. Adoption and Relevance

Data space infrastructures that provide the services outlined above are crucial, as they enable secure, automated, and standardized data exchanges. Currently, Catena-X stands as the foremost collaborative and open data ecosystem for the automotive industry, connecting all participants along the value chain. This prominence is reflected in the adoption of Catena-X standards for battery passports, which are essential for tracking and optimizing battery lifecycle management (BASF, 2023).

This indicates a strong recognition of Catena-X. However, adoption, especially in the upstream supply chain has so far been slow. This can change with the certain deadlines of Battery Regulation requirements approaching and improved Catena-x compliant software products addressing the needs of the diverse landscape of supply chain stakeholders.

6.3. UN Transparency Protocol

The UN Transparency Protocol (UNTP) is an initiative developed by UN/CEFACT to support digital transformation and ensure transparency in global trade processes (UN/CEFACT, 2024). As a foundational framework, it emphasizes the importance of data standardization and interoperability to enable seamless information exchange across diverse industries and geographies. By fostering trust and collaboration among stakeholders, the UNTP aligns with international efforts to promote sustainability, ethical practices, and regulatory compliance.

6.3.1. Scope

The UNTP establishes a standardized framework for digital traceability across various industries. It defines the structure and types of traceability events—transaction, aggregation, association, and transformation—ensuring consistent and reliable data tracking throughout supply chains. The protocol facilitates transparency and accountability by providing a common language for traceability events.

6.3.2. Adoption and Relevance

The UNTP is adopted globally to enhance traceability and transparency in supply chains. Its relevance spans multiple industries, including agriculture, pharmaceuticals, and manufacturing, where accurate traceability data is essential for regulatory compliance and quality assurance. The protocol's standardized approach ensures that all stakeholders can





effectively track and verify product movements and transformations, thus supporting sustainability and ethical sourcing practices.





7. Architecture Principles

The architecture principles are designed to ensure that the Maditrace system is robust, adaptable, and effective for supply chain traceability. Each principle reflects key requirements for enabling secure, accurate, and interoperable data exchange.

7.1. Accessibility

Accessibility emphasizes an architecture that remains free from proprietary standards, enabling broad participation among stakeholders with minimal barriers. The system should utilize open standards and avoid unnecessary complexity to ensure accessibility to all value chain stakeholders, regardless of technological capacity or infrastructure limitations.

In Maditrace, this principle means balancing inclusivity with functionality. However, implementing accessibility can be challenging because some stakeholders, particularly smaller organizations, may lack sophisticated digital infrastructure. The system must therefore provide simplified access points, possibly through API-based solutions or lightweight interfaces, to ensure participation without burdening resources.

7.2. Data Accuracy

Data accuracy requires that every data point within the system can be traced back to an issuer responsible for the data, even if the issuer did not originally generate it. This principle also supports verifiable third-party certifications, allowing conformity credentials to validate the systems and processes behind the data's creation, thereby enhancing trust.

In Maditrace's use cases, ensuring data accuracy is critical as stakeholders need reliable information to comply with regulatory requirements. Challenges include ensuring that data sources are correctly linked to their respective issuers and managing third-party certifications. The architecture must allow for streamlined verification processes including the control of origin and material analytical controls (Material fingerprinting) and establish clear accountability at each stage of the supply chain, making data reliability a practical goal.





7.3. Interoperability

Interoperability aims to prevent isolated systems that increase compliance burdens and data discrepancies. The architecture is therefore built on interoperable, open standards that facilitate seamless data exchange across different platforms and stakeholders.

For Maditrace, interoperability minimizes redundancy and aligns stakeholders on a common data framework. This principle also addresses challenges in data verifiability, as isolated systems can make tracking data lineage difficult. The primary challenge here is integrating legacy systems or disparate software while maintaining data consistency and quality. Open standards like W3C Verifiable Credentials should be central, ensuring smooth communication across varied systems.

7.4. Modularity

Modularity allows stakeholders to adopt and implement the architecture incrementally. By clearly identifying independent building blocks and their respective interfaces, the architecture enables phased implementation and minimizes vendor lock-in, encouraging long-term adaptability.

In the context of Maditrace, modularity increases adoption likelihood as stakeholders can implement specific aspects without overhauling existing systems. This reduces upfront investment costs and lowers the risk associated with adopting new technology. The challenge lies in ensuring that each module can operate independently yet integrates smoothly within the overarching system, maintaining coherence without imposing full-scale adoption requirements.

7.5. Verifiability

Verifiability ensures that all data within the system is authentic, issued by a legitimate source, and traceable back to a verifiable identity. Verifiability enables users to:

- Confirm that data was issued by a valid issuer.
- Validate the issuer's authorization for that data.
- Check that data remains active and unrevoked.
- Verify the issuer's real-world identity.





In Maditrace use cases, verifiability directly addresses regulatory compliance needs and deters misinformation, fraud or "greenwashing." It holds stakeholders accountable for the accuracy of their data and provides a reliable basis for enforcement actions. The challenges include implementing cryptographic and material fingerprinting solutions that are secure but also accessible to a broad range of stakeholders, as well as managing verification workflows efficiently to ensure smooth operation within supply chain timelines.



8. High-Level Architecture Components

8.1. Architecture Overview

Based on the architecture principles identified in Section 7, the architecture designed for traceability in critical raw material supply chains emphasizes a modular and interoperable framework that integrates various components essential for data management and the use of digital product passports. This architecture also aims to enable stakeholders to effectively track raw materials through their lifecycle, ensuring compliance with regulatory requirements and promoting transparency. Key architectural principles include the separation of data exchange protocols in control and data planes, the establishment of a digital twin for real-time data access, and the use of verifiable credentials to authenticate data provenance and integrity.

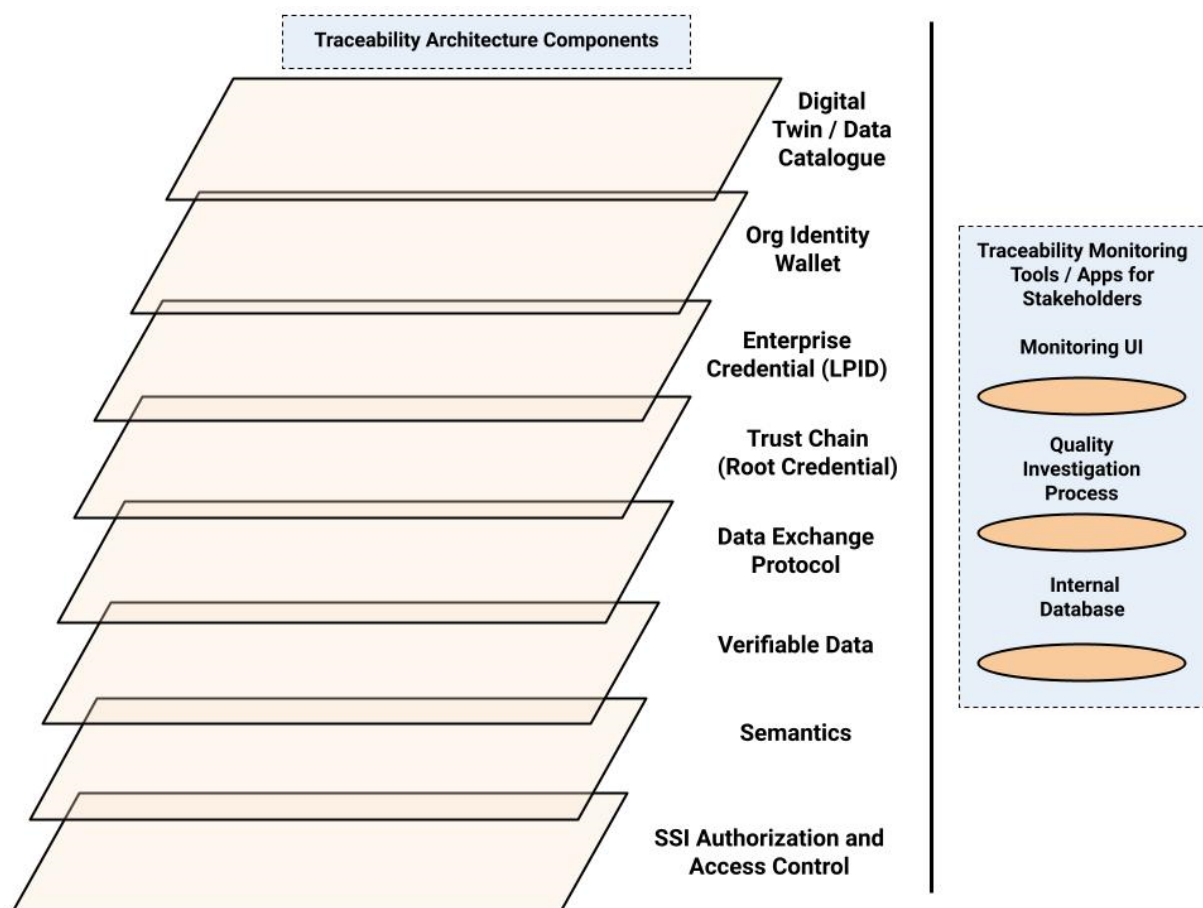


Figure 9 - Building Blocks of the Maditrace PoC Architecture

As depicted in Figure 10, the building blocks of the system architecture can be summarized as follows:



1. **Data Exchange Protocol:** This component facilitates secure and seamless data transfers between different systems and stakeholders, consisting of a Control Plane for policy management and a Data Plane for high-speed data flow.
2. **Digital Twin / Data Catalogue:** This serves as a digital representation and structured repository for raw material data, allowing real-time tracking and providing a complete digital record of materials throughout their lifecycle.
3. **Enterprise Credential (LPID):** The Legal Person Identifier (LPID) is a state-issued digital credential that uniquely identifies an organization, playing a crucial role in establishing trust and supporting secure data exchanges.
4. **Organization Identity Wallet:** This secure digital repository stores, manages, and presents organizational credentials, such as the LPID and compliance certificates, facilitating verified participation in data exchanges.
5. **Semantics Layer:** This component ensures that data is interoperable by defining standardized data structures and meanings, promoting effective communication among diverse systems.
6. **SSI Authorization and Access Control:** This component enables decentralized, credential-based authorization, allowing verified entities to access or share sensitive data while managing permissions through self-sovereign identity principles.
7. **Trust Chain (Root Credential):** Establishes a hierarchy of trust by linking credentials back to a trusted authority, ensuring that all credentials are authentic and supporting secure interactions within the ecosystem.
8. **Verifiable Data:** Refers to data embedded with cryptographic/chemical proofs that confirm its authenticity and integrity, ensuring that shared information can be trusted across the supply chain.

In addition to traceability architecture components, the system architecture also defines the following traceability monitoring tools and applications for the stakeholders that want to make use of the traceability data:

1. **Internal Database:** A foundational component of the stakeholder (i.e., the economic operator or the organization) for storing, managing, and retrieving data related to raw materials, providing an organized record that supports traceability efforts.
2. **Quality Investigation Process:** A structured workflow designed to analyze and address quality issues within the supply chain, utilizing data to ensure compliance with standards and regulatory requirements.





3. **Monitoring User Interface (UI):** This user interface provides real-time visibility into raw material data and traceability information, allowing stakeholders to monitor compliance and quality metrics through an accessible dashboard.

The components within the architecture interact seamlessly to facilitate secure data exchanges and maintain traceability. The Data Exchange Protocol governs the flow of data between systems, ensuring that only verifiable information is shared. The Digital Twin/Data Catalogue interacts with other components by providing up-to-date records that are essential for decision-making. The Organization Identity Wallet stores credentials that support the authentication processes defined by the SSI Authorization layer. The Trust Chain verifies the legitimacy of these credentials, while the Verifiable Data concept ensures that all data exchanged retains its integrity and authenticity, promoting trust among all stakeholders in the supply chain.

8.2. Traceability Architecture Components

The main objective of this section is to present the building blocks of the architecture and their functions. Furthermore, the interfaces of every building block are listed together with their interactions to other building blocks.

8.2.1. Data Exchange Protocol

A. Building Block Definition

In any complex architecture supporting raw material tracing, the Data Exchange Protocol is critical for enabling secure, seamless data transfers between different systems and stakeholders. This protocol organizes how data moves within the system (Data Plane) and how it's managed and controlled (Control Plane).

Control Plane: The Control Plane is responsible for managing the data exchange by setting and enforcing policies on how data is shared and who has permission to access it. It governs the protocols for authentication, authorization, and routing, ensuring that data exchange follows specified security and compliance rules.

Data Plane: The Data Plane is the part of the protocol that handles the actual data exchange, allowing for high-speed and efficient data flow. It takes care of the content itself—transmitting raw material data across the architecture. This layer ensures that data arrives in a usable format, whether it's raw data for processing, enriched metadata, or encrypted data for secure transactions.



Together, the Control Plane and Data Plane create a balanced system that facilitates both the management and secure transfer of data. For instance, when tracking raw materials, data like origin, processing stages, and quality certifications may need to be shared between different companies. The Control Plane makes sure each company only has access to the necessary information, while the Data Plane efficiently transfers this data.

Using an existing protocol ensures interoperability in raw material tracing by enabling secure, standardized data exchange across diverse systems. This allows the Control Plane to enforce consistent access policies while the Data Plane efficiently manages high-speed data transfers, reducing compatibility issues, streamlining integration, and building trust among stakeholders—examples include DIDComm and the International Data Spaces (IDS) Protocol.

B. Interfaces and Interaction with other Building Blocks

The essential interfaces with the Data Exchange Protocol involve:

- Digital Twin / Data Catalogue
- Enterprise Credential (LPID)
- Organization Identity Wallet
- Semantics Layer
- SSI Authorization and Access Control
- Trust Chain (Root Credential)
- Verifiable Data

These components are directly relevant as they either secure, standardize, or directly provide and validate data in the data exchange process.

8.2.2. Digital Twin / Data Catalogue

A. Building Block Definition

The Digital Twin/Data Catalogue serves as a digital representation and structured repository for raw material data, capturing details such as origin, processing stages, and compliance information throughout the material's lifecycle. This building block enables real-time tracking, traceability, and data-driven decision-making by providing a complete digital record accessible to authorized stakeholders. In the context of raw material tracing, this digital representation allows companies to simulate, analyze, and optimize processes based on accurate, current data.





8.2.3. Enterprise Credential (LPID)

A. Building Block Definition

The Enterprise Credential or Legal Person Identifier (LPID) is a state-issued digital credential that uniquely identifies an organization as a legal entity. It is not a standalone component within the raw material tracing architecture but rather a verifiable credential that can be securely stored and managed within the Organization Identity (OID) Wallet. This credential serves as a foundational element for establishing trust, supporting secure data exchanges, and verifying an organization's identity across the ecosystem.

As part of the OID Wallet, the LPID is integral to verifying organizational identities within the decentralized ecosystem, enabling secure and authorized participation in raw material tracing activities.

B. Interfaces and Interaction with other Building Blocks

- Data Exchange Protocol: Verifies organizational identities for secure data access and exchanges.
- Organization Identity Wallet (OID Wallet): Stores and manages the LPID for identity verification.
- SSI Authorization and Access Control: Uses LPID for access control based on verified legal identity.
- Trust Chain (Root Credential): Validates the LPID's legitimacy via trusted authority verification.
- Traceability Monitoring Tools: Assures identity of data contributors for reliable tracking.
- Verifiable Data: Ensures data integrity by linking it to a legally recognized entity.

8.2.4. Organization Identity Wallet

A. Building Block Definition

The Organization Identity Wallet is a secure, digital repository designed to store, manage, and present credentials unique to an organization, such as the Enterprise Credential (LPID), compliance certificates, and other verifiable organizational documents. Unlike a Natural Person Wallet, which is personalized for individual identity, the Organization Identity Wallet is optimized for legal entities, prioritizing cloud-based storage, high availability, and automated credential handling to meet the complex demands of business operations.





Key functions of the Organization Identity Wallet include:

- **Credential Storage and Management:** Safely stores verifiable credentials issued to the organization, such as compliance and regulatory certificates, and ensures they are readily accessible for verification.
- **Automated Access and Authorization:** Automates credential presentation and verification processes, allowing for seamless data exchanges and efficient access control across distributed systems.
- **Cloud-Based Deployment and High Availability:** Deployed in a cloud environment to ensure that credentials are always accessible, even across multiple geographic locations, and provide high availability for enterprise-level operations.
- **Interoperability with Business Systems:** Integrates with existing organizational systems, allowing for credential-based authentication in business workflows and cross-system data interoperability.

This wallet is essential for enabling verified and efficient participation in data exchanges within the supply chain, supporting secure, automated, and globally accessible identity management for organizations.

B. Interfaces and Interaction with other Building Blocks

- **Data Exchange Protocol:** Verifies and presents organizational credentials for secure data exchanges.
- **Enterprise Credential (LPID):** Manages storage and access of the LPID for identity verification.
- **SSI Authorization and Access Control:** Automates access management based on organizational identity.
- **Trust Chain (Root Credential):** Validates the authenticity of stored credentials.
- **Semantics Layer:** Ensures standardized data formats for interoperability.
- **Traceability Monitoring Tools:** Provides verified identity data for enhanced traceability.

8.2.5. Semantics Layer

A. Building Block Definition

The Semantics Layer is a conceptual framework that ensures data consistency and interoperability across the supply chain by standardizing the meaning and structure of





shared information. It uses JSON-LD Contexts, established vocabularies, and trusted schema registries to provide a common semantic foundation, allowing all entities to interpret and utilize data in a consistent way.

Key functions of the Semantics Layer include:

- **Data Standardization:** Establishes a common format, such as JSON-LD, to structure data uniformly across systems, enabling seamless data exchange.
- **Vocabulary Management:** Maintains consistent terminology and definitions by referencing established vocabularies, ensuring clear communication throughout the ecosystem.
- **Schema Validation with Trusted Registries:** Uses trusted schema registries to validate data structures, enhancing the trustworthiness and integrity of shared data.

B. Interfaces and Interaction with other Building Blocks

- **Data Exchange Protocol:** Ensures that all data exchanged follows standardized formats and vocabularies, facilitating seamless and consistent communication between entities.
- **Digital Twin / Data Catalogue:** Provides standardized data schemas to ensure that the Digital Twin's information is structured and interpretable across systems.
- **Organization Identity Wallet:** Uses semantic standards to ensure that credentials and identity data are formatted uniformly, supporting interoperability and verification.
- **Verifiable Data:** Applies consistent vocabularies and schemas to verifiable data, ensuring that all data with cryptographic proofs is easily understood and validated.
- **Trust Chain (Root Credential):** Ensures that credential data aligns with trusted semantic definitions, supporting reliable verification and interpretation of identity information.

8.2.6. SSI Authorization and Access Control

A. Building Block Definition

The SSI Authorization and Access Control component enables decentralized, credential-based authorization, ensuring that only verified entities access or share sensitive data within the supply chain. Using SSI principles, this building block allows permissions to be managed





through verifiable credentials, empowering organizations to control data access independently.

Functions include decentralized access management, role-based access control (RBAC) for assigning rights based on organizational roles, and dynamic, real-time permissioning aligned with credential status. Additionally, it supports privacy compliance (e.g., GDPR) by verifying identities and authorizing access without exposing unnecessary data, securing interactions within the supply chain.

B. Interfaces and Interaction with other Building Blocks

- Data Exchange Protocol: Enforces access control, ensuring only authorized entities participate in data exchanges.
- Organization Identity Wallet: Retrieves and verifies credentials stored in the wallet for access decisions.
- Enterprise Credential (LPID): Uses LPID for validating the organizational identity of users requesting access.
- Trust Chain (Root Credential): Confirms the authenticity of credentials, supporting trusted access control.
- Digital Twin / Data Catalogue: Regulates access to digital twin data based on verified permissions.

8.2.7. Trust Chain (Root Credential)

A. Building Block Definition

The Trust Chain (Root Credential) is a concept that establishes a hierarchy of trust by creating a trusted authority to which credentials can be traced. Trusted authorities, such as Chambers of Commerce for Legal Person Identifiers (LPID) or regulatory bodies like the British Columbia Government for mining permissions, issue foundational credentials that verify an organization's legitimacy and compliance. By providing a traceable path back to these authoritative sources, the Trust Chain ensures that credentials are authentic, supporting secure, compliant interactions and reliable credential validation across the supply chain ecosystem.

B. Interfaces and Interaction with other Building Blocks

- Data Exchange Protocol: Verifies authenticity of credentials in data exchanges by tracing back to the trusted root.





- Organization Identity Wallet: Stores and manages root-verified credentials, enabling secure access.
- Enterprise Credential (LPID): Links organizational identity to a trusted authority for validation.
- SSI Authorization and Access Control: Utilizes root-verified credentials to enforce access control policies.
- Digital Twin / Data Catalogue: Confirms that data sources are verified entities within the trusted chain.

8.2.8. Verifiable Data

A. Building Block Definition

Verifiable Data refers to data embedded with cryptographic proofs that confirm its authenticity, integrity, and origin. Rather than being a standalone component, it is a concept applied across the supply chain ecosystem to ensure that data shared between parties can be trusted without intermediaries. Verifiable Data is essential in environments where data integrity and provenance are critical, as it enables each party to verify that the information they receive is accurate and unaltered.

This concept is typically achieved through Verifiable Credentials and Digital Signatures, which bind data to its issuer, making it possible to confirm who issued it and that it hasn't been tampered with. Verifiable Data ensures secure, traceable exchanges and supports compliance requirements by allowing only data that can be authenticated to flow through the ecosystem.

B. Interfaces and Interaction with other Building Blocks

- Data Exchange Protocol: Ensures that only verifiable data with cryptographic proofs is exchanged between entities, maintaining data integrity.
- Organization Identity Wallet: Stores and manages verifiable credentials, enabling secure presentation and verification of data.
- SSI Authorization and Access Control: Uses verifiable data to enforce access control based on authenticated credentials.
- Trust Chain (Root Credential): Confirms that verifiable data originates from trusted sources within the hierarchy.
- Digital Twin / Data Catalogue: Integrates verifiable data to maintain trustworthy, up-to-date records of raw materials.





These interfaces enable secure, trustworthy data exchanges across the supply chain by ensuring data authenticity and integrity.

8.3. Traceability Monitoring Tools

In addition to traceability architecture components, the system architecture also defines the traceability monitoring tools and applications in this section for the stakeholders that want to make use of the traceability data.

8.3.1. Internal Database

The Internal Database is a foundational component for storing, managing, and retrieving data within the traceability monitoring system. This database securely archives records related to raw materials, including origin, processing stages, certifications, and compliance information. Serving as a centralized repository, it supports traceability efforts by providing an accessible and organized record of data that can be queried and analyzed as needed.

8.3.2. Quality Investigation Process

A. Building Block Definition

The Quality Investigation Process is a structured workflow designed to analyze, verify, and address quality issues within the supply chain. This process is essential for identifying inconsistencies or non-compliance in raw material data and for conducting root cause analyses when quality concerns arise. By leveraging data from various sources, it ensures that all materials meet regulatory standards and stakeholder requirements, thereby supporting both operational integrity and regulatory compliance.

B. Interfaces and Interaction with other Building Blocks

- Internal Database: Accesses historical and current data for analyzing quality issues and conducting root cause analysis.
- Traceability Monitoring Tools: Receives alerts and real-time data on material status to identify and track quality issues.
- Data Exchange Protocol: Facilitates secure data retrieval and updates, allowing investigation teams to access necessary information from other entities in the supply chain.
- Digital Twin / Data Catalogue: Provides up-to-date digital records for a comprehensive view of each material's lifecycle, aiding in quality assessment.





- Audit and Logging Services: Tracks investigation activities and corrective actions for accountability and transparency in quality management.

8.3.3. Monitoring UI

A. Building Block Definition

The Monitoring UI is a user interface that provides stakeholders with real-time visibility into raw material data and traceability information across the supply chain. This interface presents data in an accessible format, enabling users to monitor material status, compliance, and quality metrics. By consolidating data from various sources into a single dashboard, the Monitoring UI supports quick decision-making and enhances transparency for users involved in tracking and managing materials.

Key functions of the Monitoring UI include:

- Real-Time Data Visualization: Displays real-time information on material flows, compliance status, and quality metrics, allowing users to monitor and respond to changes immediately.
- Alert and Notification System: Provides alerts for potential quality issues, non-compliance, or deviations from expected parameters, enabling proactive management.
- Customizable Dashboards: Allows users to customize views based on specific metrics or materials, ensuring relevant data is readily accessible.
- Data Filtering and Search: Supports data filtering and search functions, enabling users to quickly locate specific records or monitor particular areas of interest within the supply chain.

B. Interfaces and Interaction with other Building Blocks

- Internal Database: Retrieves historical and current data to display material status, traceability information, and compliance metrics.
- Traceability Monitoring Tools: Integrates with tools that provide real-time tracking data, enabling visualization of material flows and status updates.
- Quality Investigation Process: Displays quality alerts and issue statuses from investigations, supporting proactive management and resolution tracking.
- Digital Twin / Data Catalogue: Accesses up-to-date digital records to present a comprehensive view of each material's lifecycle and attributes.





- Data Exchange Protocol: Facilitates secure access to external data sources, allowing users to view verified information from across the supply chain.



9. Use Case Sequence Descriptions

In this section, main traceability use cases; namely traceability event creation, mine audit request, data sharing, and data verification are presented to describe how the architecture components are utilized to ensure secure and verifiable critical raw material supply chains. These generic use cases cover all critical raw materials from of POC point-of-view, without going into the details of the supply chain characteristics of different critical raw materials.

9.1. Use Case A: Create Traceability Event

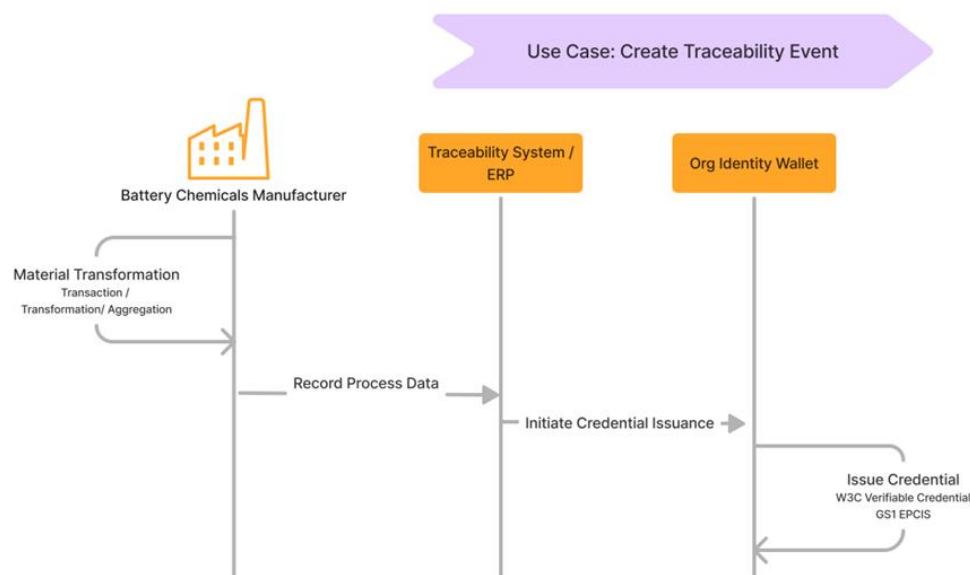


Figure 10 - Create Traceability Event Use Case

Aligned with the UN/CEFACT Verifiable Credentials specification (UN/CEFACT, 2024), a "traceability event" can be defined as the documentation of a specific action or change related to a product throughout its lifecycle. The traceability event consists of the following event types:

1. Transformation Event describes the manufacturing activities where input materials are consumed and combined to produce new output products.
2. Association Event establishes relationships between otherwise independent items, indicating how they are related or grouped.



3. Aggregation Event represents the grouping of a quantity of similar items, typically for transportation.
4. Transaction Event captures the transfer of products between organizations or facilities, marking a change of ownership or location.
5. Object Event reflects an action taken on an individual item or quantity of product, such as an inspection or quality test.

Figure 8 depicts how traceability events are created as a use case in Maditrace architecture with a transformation event example. This diagram illustrates the process for creating a traceability event related to the manufacturing of battery chemicals. The primary actor is the Battery Chemicals Manufacturer, which initiates the process for a Material Transformation Event. The event captures relevant data regarding the materials used and the processes involved in production and records the manufacturing activities such as transaction, transformation, or aggregation of materials. Once the event is created, the manufacturer records process data in a Traceability System/ERP. After recording the relevant product data, the system initiates the process of credential issuance. The final step in the use case is the actual issuance of the credential, which is a W3C Verifiable Credential compliant with the GS1 EPCIS (Electronic Product Code Information Services) standard. The issued credential is then stored in the Organizational Identity (OID) Wallet. This wallet securely holds verifiable credentials, enabling the manufacturer to manage and present these credentials as needed.

9.2. Use Case B: Request Mine Audit

The use case in Figure 9 highlights the integration of credential issuance and data exchange in the auditing process of a mining operation. The audit occurs through the data exchange framework between Mine and the Auditor, as depicted in Figure 6, using the Eclipse Data Connector and Asset Administration Shell as the underlying core components. The mine initiates the audit process by requesting the issuance of a mining permit credential through its OID wallet. The OID utilizes the data exchange protocol to facilitate communication and data transfer between the Mine and the Auditor to send a request for the issuance of a credential related to the mining permit.

The Auditor receives the mining permit credential request through its own OID wallet. The Auditor performs the on-site audit to validate the processes at the mine based on the provided information and creates the mining permit credential if the audit is successful.



The OID utilizes to facilitate communication and data transfer between the Mine and The Auditor also sends the mining permit credential over its OID wallet using the same data exchange protocol. The credential is stored in the OID wallet of the Mine, with the right to display the credential to third parties.

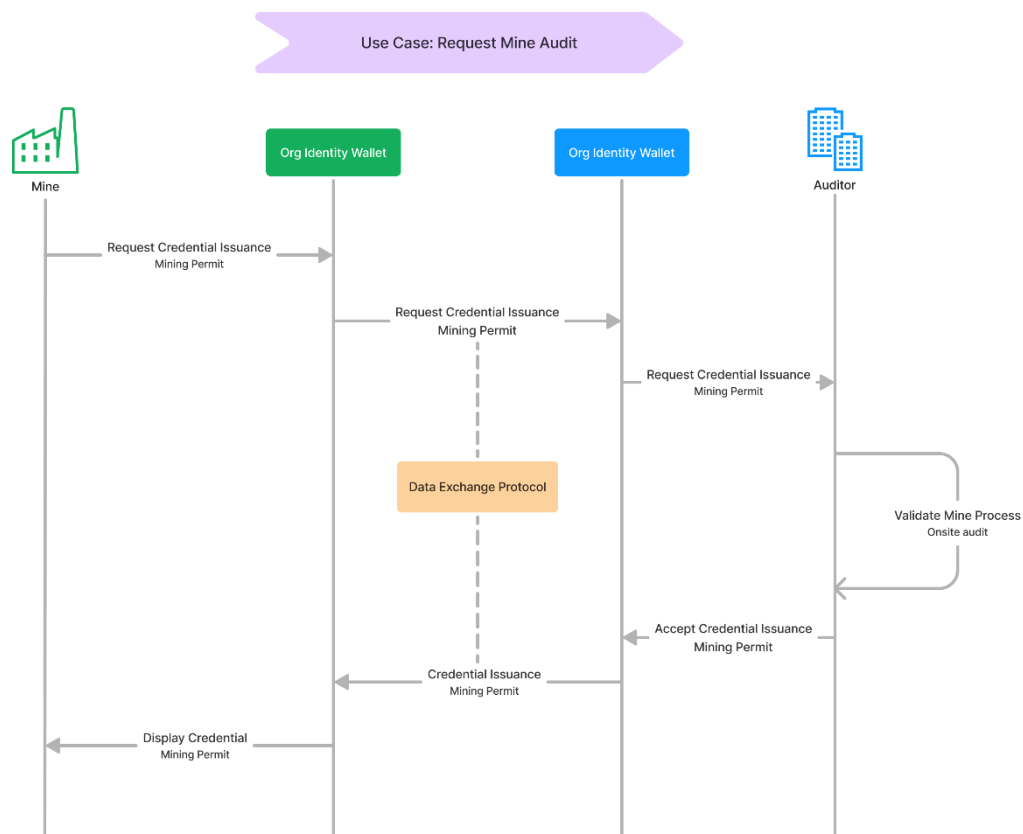


Figure 11 - Request Mine Audit Use Case

9.3. Use Case C: Data Sharing

Like the audit use case, the data sharing use case displayed in Figure 10 uses the data exchange framework provided by the Maditrace architecture. The process for data sharing occurs between a Refinery and a Battery Chemicals Manufacturer. The data transfer between two stakeholders is established over the Data Exchange Protocol defined in Section 8.2.1.

The process begins with the Refinery delivering material inputs to the Battery Chemicals Manufacturer and an order confirmation, which includes a link to the DPP, providing critical



material information. The battery chemicals manufacturer can then access and view the public DPP, that displays the available conformity credentials and certificates such as CERA 4 in1 together with the access policies. The public DPP is stored in the OID wallet of the Refinery. As next step, the Battery Chemicals Manufacturer can initiate a request for material information through a Verifiable Presentation request, allowing them to obtain verifiable data regarding the materials received from the Refinery. The OID Wallet at the Refinery evaluates the access request against established access policies.

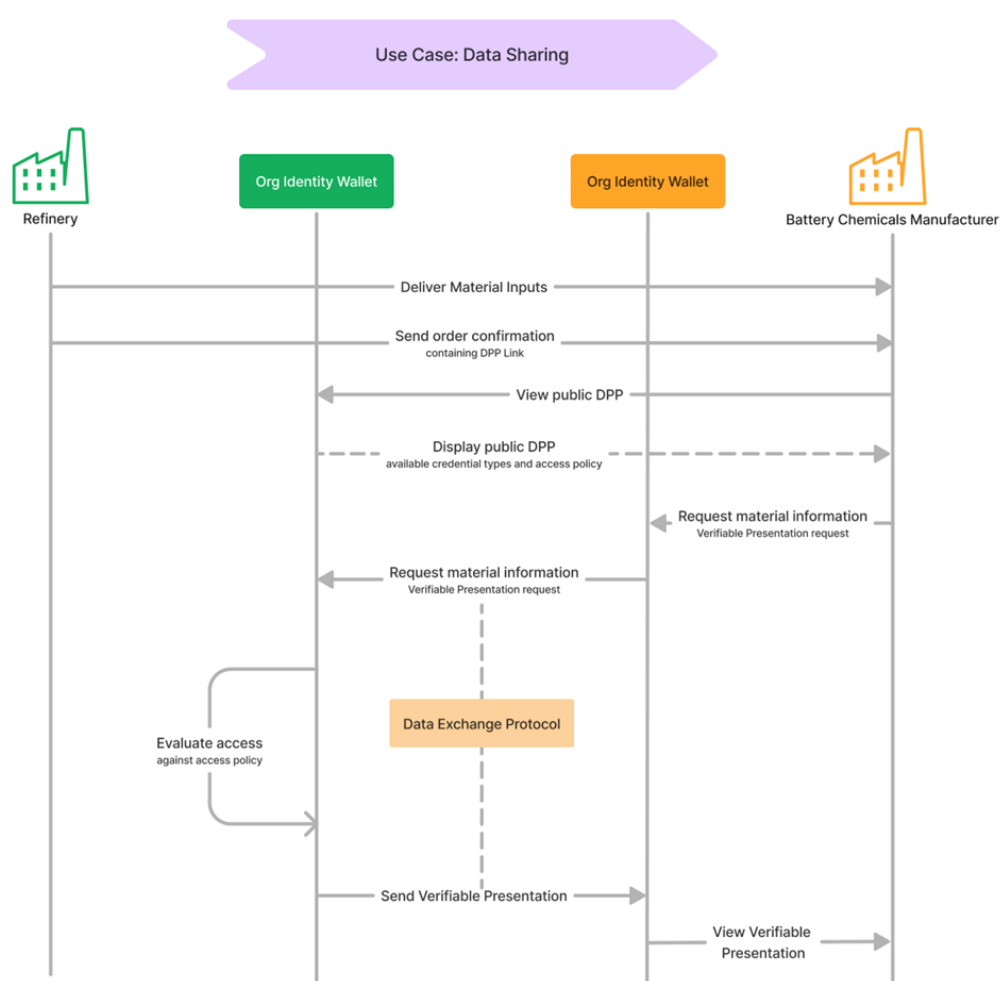


Figure 12 - Data Sharing Use Case

By utilizing OID Wallets and the DPP, both the Refinery and Battery Chemicals Manufacturer can ensure that essential information is accurately shared and verified, enhancing transparency and accountability throughout the process.

9.4. Use Case D: Data Verification

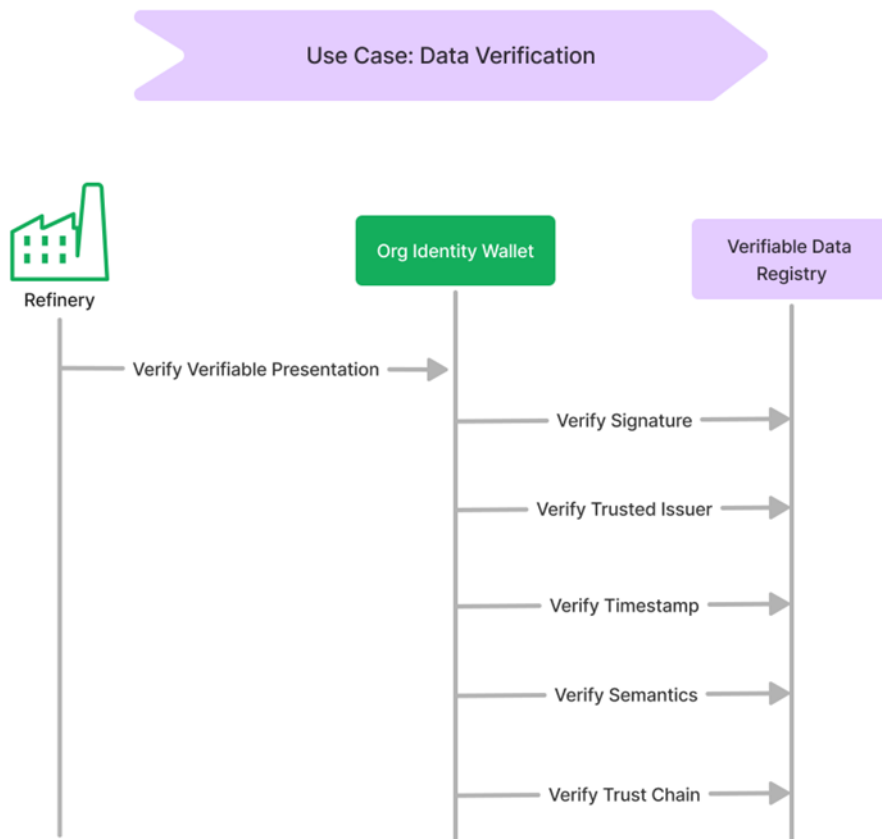


Figure 13 - Data Verification Use Case

The sequence diagram in Figure 11 illustrates the data verification process for traceability of critical raw materials, involving the Refinery and Verifiable Data Registry. This sequence diagram highlights the interaction necessary for ensuring the authenticity and traceability of critical raw materials in the supply chain. In this use case, the Refinery has the Verifier role in the SSI model as explained in Section 2.5 and wants to verify the presentation retrieved from the Holder. The Refinery initiates the verification by utilizing its Org Identity Wallet to validate this verifiable presentation. Subsequently, the Org Identity Wallet interacts with the Verifiable Data Registry to perform the verification checks, which involve signature verification, trusted issuer confirmation, timestamp validation, semantics verification, and trust chain integrity verification.



10. Discussion and Future Work

10.1. Blockchain and Smart Contracts

It is important to note that the architecture proposed in the previous chapter does not require Blockchain technology. However, this does not exclude the possibility of using Blockchain. In fact, Blockchains could be integrated into the technical infrastructure for specific modules. As illustrated in the previous section, the Verifiable Data Registry can be hosted on a Blockchain, which enhances long-term availability and privacy.

Additionally, the tamper-proof nature of Blockchains can be utilized to add a verifiable timestamp to credentials. For example, by creating a hash of a credential, such as a traceability event, and storing it on a Blockchain, a verifier can check whether this credential existed at the time of the Blockchain transaction's creation.

A practical use case for this is a yearly audit, where the auditor seeks to confirm when a specific data point was created. If a traceability data point reflecting a transaction that occurred six months ago was only created one week ago, this could indicate data tampering. Conversely, if the timestamp shows that the data point was created shortly after the transaction took place, it suggests that the data is legitimate.

Given all the abovementioned advantages and the suitability of the technology to project in use cases such as Verifiable Data Registry for data verification and credential timestamping, blockchain will be integral to Maditrace project. The integration of blockchain and smart contracts will be further detailed in *Deliverable D3.3 Guidelines for methodology implementation*, which focuses on smart contracts.

10.2. Evaluation and Next Steps

The deliverable *D3.4 - Architecture definition for POC implementation - Intermediate report* focuses on defining the architecture necessary for implementing a proof-of-concept (POC) and the core components necessary for the traceability of critical raw material (CRM) supply chains. Before concluding this deliverable, we would briefly want to highlight the future steps for Maditrace architecture development.

This report will form the basis of *D3.6, the final report on the POC architecture*. Until that report, the focus will be on implementing a prototype of a generic architecture to demonstrate how the defined architecture can be exploited in facilitating the selected use





cases. KPIs and evaluation methods will be defined to analyse whether architecture design goals are reached and to which extent the complexity of global supply chains are handled after end-to-end integration and pilot testing. Furthermore, the updates regarding the regulations and standards will be carefully tracked to ensure compliance and adaptability in evolving regulatory environments. The scientific and technical coordination and preparation of the project results in light of these regulations and standards will be part of the project's strategy in reaching the goal of enabling secure, peer-to-peer data exchanges and improve the traceability in CRM supply chain.

As this report only covers a POC architecture, only generic use cases that cover all critical raw materials are presented, without going into the details of the supply chain characteristics of different critical raw materials. This does not imply that this traceability use cases are standardized across all materials, as the traceability concept may vary for each material. Thus, it should be noted that the traceability concepts encompass various aspects such as material, location, and supply chain characteristics, and it is important to understand how they differ from one another. This will be an important next step to consider towards the final architecture.





11. Conclusions

Digital identity management architecture for traceability in critical raw material supply chains must be aligned with the driving factors in establishing digital identities. In other words, this architecture should make it possible to store and present conformity credentials, the most important being the legal identity credentials of a company or an organization, credentials in a specific industry ecosystem, such as a data space, proof of origin, ESG/due diligence certifications like CERA4in1, product safety conformity credentials and product carbon footprint credentials. Another driving factor for this POC is to create an architecture that can be transformed into a data space and/or a governance and trust ecosystem for organizations and stakeholders related to critical raw material traceability. The architecture shall also be interoperable with currently existing data spaces such as Catena-X, which is highly relevant to CRM due to battery DPP regulations. Another requirement of architecture is to enable direct connectivity between organizations, based on SSI principles. This is achieved using digital wallets to store verifiable credentials. Finally, the architecture should be able to respond to the traceability data requirements of transaction events, transformation events, aggregation events, and association events defined in UNTP.

In this context, the architecture should enable the use of traceability data in two types of DPPs: Digital Raw Material Passports and Battery Passports. Specifically, DRMPs are a subset of DPPs focused specifically on raw materials used in production processes. These passports document the origin, extraction, processing, and transportation of raw materials, providing a clear and traceable path from the source to the final product. On the other hand, EU battery regulation makes it compulsory for battery DPPs to involve Supply Chain Due Diligence, Materials and Composition, Product Carbon Footprint, and Circularity & Resource Efficiency information, which intersect with the CRM traceability data.

There are significant EU regulations that underpin the implementation of DPPs, including the European Battery Regulation, which mandates critical raw material traceability through battery passports, and the Corporate Sustainability and Due Diligence Directive, which addresses human rights and environmental impacts across product value chains. Additionally, the Ecodesign for Sustainable Products Regulation outlines requirements to promote sustainability and resource efficiency while utilizing DPPs as a crucial tool for traceability and compliance.





Standardization activities for the DPP framework and system is ongoing, and the ongoing efforts from JTC 24, Battery Pass Consortium, CIRPASS and Global Battery Alliance must be taken into consideration for traceability architecture development. The technical standards also shape the POC, as the integration of W3C Verifiable Credentials, Decentralized Identifiers (DIDs), Verifiable Credential APIs, DIDComm, Eclipse Data Space Connector (EDC), and Asset Administration Shell (AAS) are necessary as building blocks of the traceability and Digital Product Passport (DPP) architecture. Collectively, these components aim to establish a robust framework for managing digital identities, aligning with the EU's regulatory landscape and sustainability goals.

The architecture principles outlined for the Maditrace system are essential for ensuring robust and effective supply chain traceability. Key principles include accessibility, which advocates for open standards to facilitate participation across diverse stakeholders while addressing the technological limitations of smaller organizations. Data accuracy emphasizes the importance of traceable and reliable data linked to credible issuers, thereby enhancing trust and compliance with regulatory requirements. Interoperability focuses on creating a cohesive framework that prevents data discrepancies and minimizes compliance burdens through seamless data exchange among various platforms. The principle of modularity encourages incremental adoption, allowing stakeholders to integrate components gradually without significant disruption to existing systems. Finally, verifiability is critical for maintaining data integrity and accountability, ensuring that all information can be traced back to legitimate sources.

The architecture is composed of several critical building blocks, including the Data Exchange Protocol, which organizes data flow and management through distinct control and data planes. The Digital Twin/Data Catalogue serves as a comprehensive repository for tracking raw material data, while the Enterprise Credential (Legal Person Identifier) verifies organizational identities. Additional components include the Organization Identity Wallet for secure credential storage, the Semantics Layer for consistent data interpretation, and SSI Authorization for access control. The Trust Chain ensures that credentials are traceable to trusted authorities, while Verifiable Data guarantees the integrity and authenticity of the information exchanged.





12. References

Allen, C. (2016). Self-sovereign identity principles. [Online]. Available: <https://github.com/ChristopherA/self-sovereign-identity/blob/master/self-sovereign-identity-principles.md>

BASF. (2023). Steering Automotive's Digital Future with Catena-X. [Online]. Available: <https://automotive-transportation.basf.com/global/en/automotive/learn/stories/Steering-Automotive-s-Digital-Future-with-Catena-X.html>

Battery Pass Consortium. (2024). *Battery Passport Technical Guidance*. Retrieved from <https://cirpassproject.eu/wp-content/uploads/2024/05/D3.2v1.9.pdf>

Catena-X. (n.d.). *CX-0018 Dataspace Connectivity*. Retrieved from <https://catenax-ev.github.io/docs/next/standards/CX-0018-DataspaceConnectivity>

Catena-X. (2023). *Enablement Services Whitepaper*. Retrieved from https://catena-x.net/fileadmin/online_media/231006_Whitepaper_EnablementServices.pdf

CIRPASS. (2024). D3.2 - DPP System Architecture. Retrieved from <https://cirpassproject.eu/wp-content/uploads/2024/05/D3.2v1.9.pdf>

DIDComm Messaging. (2023). *DIDComm Messaging Specification v2.1*. Retrieved from <https://identity.foundation/didcomm-messaging/spec/v2.1/>

European Commission. (2019). *Communication from the Commission on the European Green Deal, COM/2019/640 final*. Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019DC0640>

European Commission. (2023). Regulation (EU) 2023/1542 of the European Parliament and of the Council of 30 July 2023 concerning batteries and waste batteries. Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1542>

European Commission. (2024). Implementing the EU digital battery passport: Opportunities and challenges for battery circularity. European Circular Economy Stakeholder Platform. Retrieved from <https://circulareconomy.europa.eu/platform/en/knowledge/implementing-eu-digital-battery-passport-opportunities-and-challenges-battery-circularity>

European Commission. (2024). Commission implementing decision of 31.7.2024 on a standardisation request to the European Committee for Standardisation, the European Committee for Electrotechnical Standardisation, and the European Telecommunications Standards Institute as regards digital product passports in support of Union policy on ecodesign requirements for sustainable products and on batteries and waste batteries. C(2024) 5423 final. Retrieved from [EUR-Lex](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024D0542)





European Parliament and Council. (2024a). *Regulation (EU) 2024/1781 of the European Parliament and of the Council of 13 June 2024 establishing a framework for the setting of ecodesign requirements for sustainable products, amending Directive (EU) 2020/1828 and Regulation (EU) 2023/1542 and repealing Directive 2009/125/EC*. Retrieved from [EUR-Lex](#).

European Parliament and Council. (2024b). *Regulation (EU) 2024/1183 of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework*. Retrieved from [\[https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1183\]](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1183)

European Union. (2024). *Regulation (EU) 2024/1183 of the European Parliament and of the Council of 6 June 2024 on establishing a Digital Product Passport framework for traceability of products, and repealing Regulation (EU) 1025/2012*. Official Journal of the European Union. Retrieved from <https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng>

Global Battery Alliance. (2022a). *GBA Battery Passport: The Child Labour Index - Version 1.0*. Retrieved from <https://www.globalbattery.org/media/publications/gba-childlaborindex-v1rev2.pdf>

Global Battery Alliance. (2022b). *GBA Battery Passport: The Human Rights Index - Version 1.0*. Retrieved from <https://www.globalbattery.org/media/publications/gba-humanrightsindex-v1rev2.pdf>

Global Battery Alliance. (2023a). *GBA Battery Passport: Pilot Project - Master Document*. Retrieved from <https://www.globalbattery.org/media/pilot/documents/gba-bp-pilot-master.pdf>

Global Battery Alliance. (2023b). *GBA Greenhouse Gas Rulebook: Generic Rules - Version 2.0*. Retrieved from <https://www.globalbattery.org/media/publications/gba-rulebook-v2.0-master.pdf>

Naik, N., & Jenkins, P. (2020). Self-Sovereign Identity Specifications: Govern Your Identity Through Your Digital Wallet using Blockchain Technology. 2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), Oxford, UK, 2020, pp. 90-95. doi: 10.1109/MobileCloud48802.2020.00021.

UN/CEFACT. (2024). *UN/CEFACT Unified Modeling Methodology*. Retrieved from <https://uncefact.github.io/spec-untp/docs/about/>

W3C. (2021). *Verifiable Credentials Data Model v1.1*. Retrieved from <https://www.w3.org/TR/vc-data-model-1.1/>

W3C. (2022). *Decentralized Identifiers (DIDs) v1.0*. Retrieved from <https://www.w3.org/TR/did-core/>





W3C. (2023). *Verifiable Credentials Data Model v2.0*. Retrieved from <https://www.w3.org/TR/vc-data-model-2.0/>

W3C CCG. (2020). *A Primer for Decentralized Identifiers*. Retrieved from <https://w3c-ccg.github.io/did-primer/>

W3C CCG. (2023). *Verifiable Credentials API v0.3*. Retrieved from <https://w3c-ccg.github.io/vc-api/>

