MADITRACE

Architecture Definition for PoC Implementation - Final Report

Deliverable D3.6

Version N°1

Authors: Doruk Sahinel (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.

Funded by
the European Union

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 – 30 June 2026 (42 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	Doruk Sahinel (Spherity)
Due Date	M36
Submission Date	30/01/2026
Dissemination level	PU

History

Date	Version	Submitted by	Reviewed by	Comments
02/12/25	0.1	Doruk Sahinel	-	Table of Contents, First structure of the document added
24/01/26	0.2	Doruk Sahinel	Rouwaida Abdallah	First Draft Version completed
26/01/26	0.3	Doruk Sahinel	Daniel Monfort	Final validation
27/01/26	0.4	Doruk Sahinel	Anne-Marie Desaulty	MFP Review
30/01/26	0.5	Doruk Sahinel		
30/01/26	1	Duivon Laurine	-	Final Review and Submission

Funded by the European Union

Table of contents

1. Introduction 9
2. Update on References and Standards 11
2.1. Regulatory Context 11
2.2. Ecosystems and Interoperability Initiatives 12
2.3. DPP Standardization Context: CEN/CENELEC JTC 24 12
2.4. Technical Standards and Definitions 14
2.5. Material Evidence and Certification Schemes 14
3. Use Case Definitions and Requirements 15
3.1. Material Lifecycle & Traceability Use Cases 15
Use Case 1: Digitalized Origin Verification with Material Fingerprinting 16
Use Case 2: Creation of UNTP Traceability Events 21
Use Case 3: Linked DPP Data Sharing 23
3.2. Governance, Trust, & Interoperability Use Cases 25
Use Case 4: Automated Dataspace Onboarding via Wallets 26
Use Case 5: Verifiable Data Exchange over Dataspace Protocols 28
Use Case 6: Decentralized Red Flag Governance 30
4. PoC Architecture Evaluation 32
4.1 Alignment of the PoC with Architecture Principles 32
4.2 PoC Building Blocks and Their Utilization Across Use Cases 33
4.3 Summary Matrix: Use Case vs. Component Utilization 36
5. Raw Material DPP Data Model 37
5.1 Data Model Structure and Semantics 37
5.2. Data Categories and Attributes 38
5.3. Example Payload: Spodumene Concentrate Batch 40
6. Conclusions 40
7. References 42
8. Appendix 44

Funded by
the European Union

List of figures

Figure 1 - MaDiTraCe Physical-Digital Linking Workflow 17
Figure 2 - Workflow to Support Origin Claims with MFP Credentials in Raw Material DPP 18
Figure 3 - Raw Material DPP frontend view of Material Fingerprinting Origin Probabilities 19
Figure 4 - Raw Material DPP frontend view of the Material Fingerprinting Certificate 20
Figure 5 - Sequence Workflow for Recording a Traceability Event 21
Figure 6 - Linked Raw Material DPP Identifiers across Tiers 23
Figure 7 - Automated dataspace onboarding via OIDs 26
Figure 8 - Catena-X Data Exchange Framework with Eclipse Dataspace Connector and Asset Administration Shell (Catena-X, 2023) 28
Figure 9 - Sequence workflow for issuing a traceability event as a Verifiable Credential ... 31
Figure 10 - MaDiTraCe Traceability Architecture Components 34
Figure 11 - Raw Material DPP Frontend with did:web-based identifiers, credential verification, and data access options for a raw material batch 38
Figure 12 - Raw Material DPP Core Data Elements 40

List of Tables

Table 1 - Use case to Architecture Component Mapping 36

Funded by the European Union

Summary

This final report presents the architectural framework envisioned for critical raw material supply chains, which leverage self-sovereign identity and verifiable credentials to ensure secure traceability. The report builds on the framework described in the intermediate report "D3.4 Architecture definitions for Proof of Concept (POC) implementation" and aims to describe how the high-level architecture components described in this report are utilized in raw material supply chain traceability use cases. The report first updates the regulatory and interoperability context since the intermediate deliverable, including key EU regulations, standards work, and ecosystem initiatives that influence the POC design. It then presents six use cases as practical case studies showing how material fingerprinting, United Nations Traceability Protocol (UNTP)-aligned traceability events, cross-tier DPP linking, and governed dataspace participation can be implemented using the architecture components. Finally, the report specifies the Raw Material DPP data model based on the implemented DPP examples. This deliverable is intended for technical experts, industry stakeholders, and policymakers, guiding them toward creating traceable raw material supply chains.

Keywords

Critical Raw Materials (CRM), Dataspaces, Decentralized Identifiers (DID), Digital Product Passport (DPP), Self-Sovereign Identity (SSI), Verifiable Credentials (VC), Traceability

Abbreviations and acronyms

AAS	Asset Administration Shell
B2B	Business-to-Business
CAHRA	Conflict-Affected and High-Risk Areas
CAS	Chemical Abstracts Service
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CoC	Chain of Custody
CRMA	Critical Raw Materials Act
CRM	Critical Raw Materials
CSDDD	Corporate Sustainability and Due Diligence Directive
DCC	Digital Conformity Credential

DIA	Digital Identity Anchor
DID	Decentralized Identifier
DCP	Decentralized Claims Protocol
DPP	Digital Product Passport
DSP	Dataspace Protocol
EDC	Eclipse Data Space Connector
ERP	Enterprise Resource Planning
ESG	Environmental, Social, and Governance
ESPR	Ecodesign for Sustainable Products Regulation
EU	European Union
EUCC	European Union Company Certificate
GTIN	Global Trade Item Number
HS Code	Harmonized System Code
ISO	International Organization for Standardization
JSON-LD	JavaScript Object Notation for Linked Data
JTC	Joint Technical Committee
JWS	JSON Web Signatures
LPID	Legal Person Identifier
MFP	Material Fingerprinting
OECD	Organisation for Economic Co-operation and Development
OEM	Original Equipment Manufacturer
OID	Organization Identity Wallet
POC	Proof of Concept
QR	Quick Response
REACH	Registration, Evaluation, Authorisation and Restriction of Chemicals
SSI	Self-Sovereign Identity
UC	Use Case
UNTP	United Nations Traceability Protocol
VC	Verifiable Credentials
W3C	World Wide Web Consortium

Funded by the European Union

1. Introduction

The increasing need for secure, transparent, and sustainable supply chains has driven the emergence of DPPs as key enablers of the circular economy. In particular, the European Critical Raw Materials Act (European Parliament and Council, 2024a), the EU Battery Regulation (European Parliament and Council, 2023), and the Ecodesign for Sustainable Products Regulation (ESPR) (European Parliament and Council, 2024b) drive traceability systems to ensure ethical sourcing and carbon footprint disclosure. However, existing DPP initiatives often lack mechanisms to securely and persistently bind physical material properties to their digital records. Traditional traceability approaches rely primarily on digital metadata, making them vulnerable to decoupling attacks, fraud, and raw material substitution.

To address this, MaDiTraCe ensures a persistent link between the physical properties of critical raw materials–verified via Material Fingerprinting–and their evolving digital identities. The purpose of this deliverable is to present concrete use cases that work as a Proof of Concept to facilitate the implementation of traceability, based on self-sovereign identities. While the intermediate report (D3.4) focused on presenting the theoretical architectural framework, this final report (D3.6) shifts the objective to reporting on the final implemented architecture. This document details the concrete implementation of the use cases and demonstrates how DID-based identifiers, verifiable evidence (such as material fingerprinting results and traceability events), and governed data exchange mechanisms function together to support trustworthy traceability across multi-tier raw material supply chains.

This document is organized to progress from the project's foundational requirements to the concrete details of the implemented Proof of Concept (PoC). The report is structured as follows:

- **Section 1, Introduction**, outlines the goals of the MaDiTraCe project in establishing trustworthy traceability for critical raw materials and defines the scope of this deliverable, emphasizing the transition from the intermediate architecture definition (D3.4) to the implemented Proof of Concept (PoC) and its validation through concrete use cases.
- **Section 2, Update on References and Standards**, summarizes the foundational concepts introduced in the intermediate report and provides updated context on the regulatory and ecosystem landscape shaping the final PoC. It highlights key

regulations, interoperability initiatives, and supporting technical standards such as W3C DIDs, W3C Verifiable Credentials, and UNTP.

- **Section 3, Use Case Definitions and Requirements**, details the functional scenarios driving the PoC design and implementation by describing a coherent set of six use cases across the traceability lifecycle. It covers: (UC1) material fingerprinting as verifiable origin evidence, (UC2) UNTP-aligned traceability events for chain-of-custody, (UC3) explicit linking of Raw Material DPP identifiers across tiers, and the governance/interoperability mechanisms required to operationalize traceability at scale with (UC4) automated dataspace onboarding, (UC5) sovereign evidence exchange via dataspace protocols, and (UC6) red-flag governance for enhanced due diligence use cases.
- **Section 4, Final Architecture Overview,** reviews the final PoC architecture by mapping the architecture principles and building blocks defined in the intermediate report (D3.4) to the implemented use cases UC1–UC6. It explains how core components such as the Organizational Identity Wallet, Enterprise Credentials, Trust Chain, semantics layer, and dataspace exchange protocols are utilized across the use cases, and provides a consolidated component-by-component analysis and summary matrix demonstrating their role in enabling verifiable, interoperable, and governed raw material traceability.
- **Section 5, Raw Material DPP Data Model**, provides the technical specification of how raw material DPP information is structured and represented in the PoC. It explains the DID-based identifier approach, the use of JSON-LD contexts for semantic interoperability, and the separation of DPP information into domain-specific credential payloads. The section further derives and illustrates the key data categories and attributes based on the implemented Raw Material DPP examples (Spodumene Concentrate and Lithium Hydroxide) and references UC1 and UC3 to connect the data model to material fingerprinting evidence and cross-tier DPP linking.
- **Section 6, Conclusions**, summarizes the main outcomes of the implemented PoC architecture, reflects on the relevance of the approach against the initial traceability and trust goals, and outlines potential next steps for scaling, piloting, and ecosystem integration.

Funded by the European Union

2. Update on References and Standards

This section summarizes the key reference points and standards introduced in the intermediate report (D3.4) and provides updated context on the regulatory landscape, ecosystem initiatives, and technical foundations shaping the final MaDiTraCe Proof of Concept. Specifically, it details the requirements from the emerging CEN/CENELEC JTC 24 draft standards for EU DPP framework alignment. The section also highlights ongoing interoperability efforts in industrial ecosystems and dataspaces, and describes the open standards used in the PoC implementation, including W3C Decentralized Identifiers, W3C Verifiable Credentials, and UNTP-aligned traceability concepts.

2.1. Regulatory Context

The MaDiTraCe technical work is framed by the European regulatory context for critical raw material traceability and Digital Product Passports. The following regulations define the overarching objectives and information requirements that motivate the PoC architecture.

- **Critical Raw Materials Act (CRMA) (European Parliament and Council, 2024a):** Formally adopted as Regulation (EU) 2024/1252, the CRMA establishes the legal necessity for secure and resilient raw material supply chains. It mandates robust monitoring of strategic raw materials and explicitly encourages the use of digital tools to certify the sustainability and origin of these resources.
- **EU Battery Regulation (European Parliament and Council, 2023):** Regulation (EU) 2023/1542 remains the primary driver for the battery-specific use cases in this project. It mandates the "Battery Passport" by February 2027, requiring specific data attributes regarding chemistry, carbon footprint, and due diligence.
- **Corporate Sustainability and Due Diligence Directive (CSDDD) (European Parliament and Council, 2024c):** The CSDDD complements the EU Battery Regulation by introducing mandatory value-chain due diligence requirements that address adverse human rights and environmental impacts. It aims to harmonize due diligence obligations across the EU, and strengthen corporate accountability across value chains, including raw material sourcing, manufacturing, distribution, use, and end-of-life activities.
- **Ecodesign for Sustainable Products Regulation (ESPR) (European Parliament and Council, 2024b):** Adopted as Regulation (EU) 2024/1781, the ESPR generalizes

the Digital Product Passport (DPP) concept to all physical goods. It sets the horizontal requirements for the DPP system, including the need for a persistent unique identifier and a decentralized data storage model.

2.2. Ecosystems and Interoperability Initiatives

To ensure the MaDiTraCe architecture is not an isolated solution, it aligns with the major industrial ecosystems currently defining the interoperability landscape for the European market.

- **Battery Pass Consortium (Battery Pass Consortium, 2024):** The PoC leverages the content guidance and technical framework developed by the Battery Pass Consortium. Specifically, it aligns with their defined data attributes for material composition and the governance model for separating public and restricted data.
- **CIRPASS (CIRPASS, 2024):** As the flagship EU initiative for Digital Product Passports, CIRPASS defines the cross-sectoral requirements for interoperability. MaDiTraCe aligns with the CIRPASS architectural reference by ensuring the system is vendor-neutral and utilizes open standards for identifiers and data carriers.
- **Catena-X (Catena-X, n.d.):** As the leading data ecosystem for the automotive industry, Catena-X provides a reference architecture for the dataspace components of the PoC. The solution utilizes Dataspace Governance principles to ensure that raw material data can be exchanged securely within the automotive value chain using the Eclipse Dataspace Connector (EDC).
- **UN/CEFACT (UN/CEFACT, 2026):** UN/CEFACT is an intergovernmental body under UNECE that develops trade facilitation recommendations and e-business standards to enable interoperable, cross-border data exchange. MaDiTraCe aligns in particular with the UN Transparency Protocol (UNTP) as a common framework for standardized digital traceability and transparency across diverse supply chain stakeholders.

2.3. DPP Standardization Context: CEN/CENELEC JTC 24

The CEN/CENELEC Joint Technical Committee (JTC 24) provides the harmonized technical framework for implementing DPP systems in the EU. These EU DPP obligations are not yet broadly binding for standalone raw materials; however, the MaDiTraCe PoC aligns with the six key draft standards (prEN 18216– prEN 18223) that define the technical, semantic, and

Funded by the European Union

security requirements for compliant data exchange and complement them with raw-material-specific approaches to address traceability needs of raw material supply chains.

- **prEN 18216 – Data Exchange Protocols (CEN/CENELEC JTC 24, 2025a):** This standard mandates secure, non-repudiable data exchange, without prescribing a specific protocol or reference implementation. The PoC aligns with this by using secure protocols (e.g., EDC) as an implementation choice to realize data exchange over data spaces, to ensure neither the sender nor the receiver can deny the exchange of data, establishing a legally robust audit trail essential for B2B supply chain automation.
- **prEN 18219 – Unique Identifiers (CEN/CENELEC JTC 24, 2025a):** This standard defines the principles for globally unique and persistent identifiers. The PoC adopts Decentralized Identifiers (DIDs) (ID Scheme 5.3) for products and organizations, ensuring that the unique identifier remains resolvable and verifiable even if the issuing economic operator ceases operations.
- **prEN 18220 – Data Carriers (CEN/CENELEC JTC 24, 2025c):** This standard governs the physical–digital link. The PoC ensures that the physical carrier (e.g., a QR code on a material batch) encodes a unique identifier (DID) that resolves to the Raw Material DPP. Verification endpoints confirm that the carrier's encoded value corresponds exactly to a registered identifier, preventing fraudulent re-marking.
- **prEN 18221 – Data Persistence (CEN/CENELEC JTC 24, 2025d):** To meet the requirement for long-term data availability, the architecture includes mechanisms for secure storage and archiving. This ensures that historical data (e.g., provenance records) remains immutable and retrievable for market surveillance, utilizing tamper-evident audit trails (e.g., hash chains) to prove data integrity over time. In the PoC, these mechanisms are assumed to be complemented by additional controls to mitigate the risk that a privileged actor could rewrite history.
- **prEN 18222 – APIs (CEN/CENELEC JTC 24, 2025e):** The PoC supports API-based retrieval of DPP data and linked verifiable evidence and enables credential-based authorization for access to restricted information to support auditability and controlled sharing across the supply chain.
- **prEN 18223 – System Interoperability (CEN/CENELEC JTC 24, 2025f):** This standard ensures semantic consistency. The PoC utilizes a hierarchical semantic

model and JSON-LD serialization to ensure that data payloads are machine-readable and interoperable across different sectors and IT systems. The architecture supports validation of issued payloads against versioned schemas to prevent deviations.

2.4. Technical Standards and Definitions

The implementation of the architecture relies on open, global technical standards. The following core technologies form the foundation of the PoC:

- **Self-Sovereign Identity (SSI):** An identity management model where entities (individuals, organizations, or devices) control their own digital identities and verifiable data without relying on a single central authority (Allen, 2016). In MaDiTraCe, SSI enables supply chain actors to manage, issue, and present trusted traceability evidence in a decentralized manner.
- **Verifiable Credentials (VCs):** Cryptographically signed digital statements used to express tamper-evident claims (W3C, 2021). In the PoC, VCs are the standard mechanism to represent traceability-relevant evidence such as material fingerprinting results, UNTP-aligned traceability events, and compliance or governance signals that can be linked to Raw Material DPPs.
- **Decentralized Identifiers (DIDs):** Globally unique, cryptographically verifiable identifiers that can be resolved to DID Documents containing keys and service endpoints (W3C, 2022). DIDs are used to identify organizations and material batches and to bind them to verifiable credentials and wallet-based identity operations.
- **JSON-LD (JavaScript Object Notation for Linked Data):** A W3C standard for representing Linked Data using JSON (W3C, 2020), enabling structured payloads to carry explicit semantic meaning through shared vocabularies and contexts. In MaDiTraCe, JSON-LD is used to model Raw Material DPP attributes and verifiable credential payloads in a machine-readable and interoperable way. This supports consistent interpretation of traceability, sustainability, and compliance data across organizations and IT systems.

2.5. Material Evidence and Certification Schemes

Beyond digital standards, the PoC also supports traceability evidence that reflects the physical and compliance reality of raw materials. In MaDiTraCe, such evidence is

Funded by the European Union

represented in a verifiable and machine-readable form so it can be linked to Raw Material DPPs and validated across supply chain tiers.

- **Material Fingerprinting (MFP):** To support origin verification, the PoC integrates material fingerprinting results derived from chemical, isotopic, mineralogical or crystallographic attributes. These results provide scientifically grounded evidence for provenance assessment (Gäbler et al., 2020), and can differentiate between distinct geological sources, with outcomes expressed as probability-based origin attribution and linked to the DPP as verifiable evidence.
- **Third-Party Conformity and Sustainability Certification:** The architecture supports the integration of external audit and certification outcomes relevant to ESG and responsible sourcing, e.g., CERA 4in1 (Nowaz et al., 2025). These certifications may apply either at the company level (e.g., company practices) or at the commodity level (e.g., material shipment). In both cases, such certificates can be represented as Verifiable Credentials and attached to Raw Material DPPs, enabling downstream actors to validate issuer authenticity, integrity, and the presence of supporting evidence without relying on unstructured document exchange.

3. Use Case Definitions and Requirements

This section defines the functional use cases and derived requirements that drive the implementation of the MaDiTraCe PoC. The selected use cases cover the key steps required to establish trustworthy traceability for critical raw materials across multi-tier supply chains, combining material-level evidence, chain-of-custody event modeling, and verifiable data exchange. In addition to material lifecycle scenarios (UC1–UC3), the section also introduces governance, trust, and interoperability mechanisms (UC4–UC6) that enable scalable participation in data ecosystems, controlled sharing of DPP evidence, and risk-based compliance workflows.

3.1. Material Lifecycle & Traceability Use Cases

This subchapter describes the material lifecycle and traceability use cases that establish how raw material evidence is generated and connected across tiers, including origin verification, chain-of-custody event creation, and explicit linking of upstream and downstream Raw Material DPP identifiers.

Use Case 1: Digitalized Origin Verification with Material Fingerprinting

Material fingerprinting strengthens digital traceability by creating a robust physical–digital link between a raw material and its Raw Material Digital Product Passport (DPP). If traceability relies only on digital identifiers and documents, the digital record may become separated from the physical material it is meant to describe, e.g., through copying, re-labeling, or reusing identifiers across batches or containers. UC1 addresses this vulnerability by using analytical material properties as verifiable evidence that can be cryptographically protected and linked directly to the raw material DPP, making origin claims significantly harder to falsify.

The use case starts when an upstream supplier or economic operator needs to validate the declared origin of a raw material batch, for example to comply with due diligence requirements or to satisfy downstream purchasing and audit expectations. The supplier either performs material analysis internally or commissions a specialized third-party laboratory to analyze representative samples using chemical (trace elements detection), isotopic, or spectral measurements. The resulting analytical data is then transmitted securely to an authoritative assessment body such as BRGM (BRGM, 2026), which maintains validated reference datasets and baselines for origin comparison.

The authoritative body compares the analytical results received against its reference databases to evaluate whether the material's measured signature aligns with its declared geographic or geological origin. The assessment yields a probability-based result that expresses confidence in the origin attribution and makes scientific uncertainty explicit. This probability score becomes the central output of the material fingerprinting process and provides a practical basis for risk-oriented decision-making in traceability workflows.

To ensure the result can be trusted and reused across organizational boundaries, the authoritative body issues the outcome as a cryptographically signed Verifiable Credential. This makes the fingerprinting evidence tamper-evident, independently verifiable, and suitable for integration into a Raw Material DPP as a machine-readable proof of origin. Downstream actors can retrieve the credential from the DPP and verify its authenticity and integrity, then apply their own acceptance thresholds or escalation rules depending on risk appetite, regulatory exposure, and the sensitivity of the supply chain. In this way, material fingerprinting does not replace digital traceability records but it complements them by adding a high-assurance evidence layer by binding the physical material to its digital representation. Figure 1 depicts the MaDiTraCe physical–digital linking workflow, showing

Funded by the European Union

how material fingerprinting results are issued as verifiable evidence and attached to the Raw Material DPP for downstream verification.

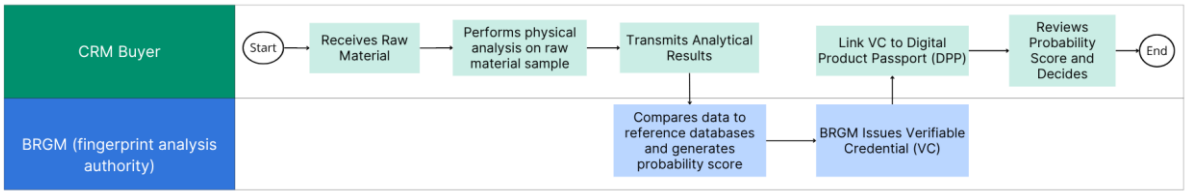

Figure 1 - MaDiTraCe Physical-Digital Linking Workflow

For the specific implementation of Use Case 1, the architecture is designed to solve the business problem of validating "Country of Origin" claims. The system defines four distinct actor roles with specific operational requirements:

- **Material Supplier (Requester):** Initiates the fingerprinting process for a specific material batch, provides the declared origin claim, ensures sampling is performed, and links the resulting fingerprint evidence to the Raw Material DPP for downstream reuse.
- **Third-Party Laboratory (Data Producer):** Performs the analysis of the sample and generates the analytical dataset used as the basis for origin assessment. Depending on the operating model, this role may be fulfilled by an independent laboratory or by the same organization that performs the authoritative assessment.
- **Authoritative Assessment Body (Issuer):** Maintains validated reference databases, compares analytical results against reference baselines, calculates the probability-based origin assessment, and issues the signed Fingerprint Credential as a VC.
- **Downstream Manufacturer / Auditor (Verifier):** Retrieves the Raw Material DPP and the fingerprint credential, verifies issuer authenticity and integrity of the evidence, and makes acceptance or escalation decisions based on internal risk thresholds and compliance requirements.

A standards-compliant preliminary prototype is implemented to display the core elements of the architecture, including a did:web-based material identifier for a lithium electrolyte lot, verifiable credential issuance, and DPP visualization. The prototype relies on W3C DID Core (W3C, 2022) and W3C Verifiable Credentials Data Model (W3C, 2021) for identity and credential management, with proofs expressed using JSON Web Signatures (JWS) (W3C, 2024). The prototype covers DID resolution and verification of linked VCs such as the material fingerprint credential, issued by a laboratory with a probability score regarding the

material origin. Domain models for DPP attributes, such as composition data, origin metadata, and laboratory information, are defined using JSON-LD contexts to ensure semantic interoperability. Figure 2 provides an overview of the end-to-end origin-claim workflow, from analysis and reference matching to credential issuance and integration into the DPP evidence layer.

Figure 2 - Workflow to Support Origin Claims with MFP Credentials in Raw Material DPP

Building on this foundation, the material fingerprinting use case is integrated into the Raw Material DPP as a dedicated evidence layer that supports origin claims with scientifically grounded, machine-verifiable proof. The workflow begins with material fingerprinting analysis, which is evaluated against a reference dataset to determine coherence between the measured sample and known baselines for specific origin locations. Instead of producing a binary outcome, the result is expressed as origin probabilities, enabling downstream decision-making based on confidence levels and risk thresholds. It needs to be mentioned that the material fingerprinting credential in the PoC does not provide any accept or reject decision. It is the responsibility of downstream actors to determine whether the indicated origin are acceptable based on their own supply strategy, risk thresholds, and compliance requirements.

The outcome of the analysis is issued as a verifiable credential specifically designed for material fingerprinting, and the DPP resolves and validates this credential as part of its verification pipeline. In the prototype displayed in Figure 3, this is reflected in the “Origin Probabilities” view, where candidate origin locations (e.g., mines or regions) are presented with a probability score and supporting quality indicators such as false positive risk and sample representativity. This makes origin assessment both transparent and actionable in digital traceability scenarios, because verifiers can interpret the confidence and limitations associated with the underlying evidence.

Funded by the European Union

Origin Probabilities

COUNTRY	MINE	PROBABILITY (0-1)	FALSE POSITIVE RISK	SAMPLE REPRESENTATIVI
Australia	Mine 1	0,95	0,02	0,89
Australia	Mine 2	0,05	0,02	0,64

Figure 3 - Raw Material DPP frontend view of Material Fingerprinting Origin Probabilities

To ensure the credential is meaningful and auditable beyond the probability score alone, the Raw Material DPP also captures methodological and provenance metadata that explains how the evidence was produced. As shown in Figure 4, the material fingerprint credential includes structured fields such as the methodology name (e.g., “minor and trace elements”), the reference database used for matching (e.g., BRGM-MaDiTraCe database), and the laboratory identifier responsible for the assessment (e.g., BRGM), and the laboratory accreditation (e.g., ISO/IEC 17025 for elemental analyses). This information is displayed in the DPP frontend and is also available in the underlying machine-readable credential payload, allowing verifiers to evaluate the credibility of the issuer, the applicability of the method, and the context of the origin claim.

Finally, the Raw Material DPP is made accessible through a product identifier that can be distributed across the supply chain in a simple and interoperable form. The did:web-based identifier is exposed as a DID link that resolves to the DPP, and it can be embedded into a QR code so that internal users and external verifiers can retrieve the passport and its linked credentials through a web-based frontend. This creates a practical bridge between physical material handling and digital verification. The batch identifier provides access to the DPP, and the DPP provides verified origin evidence through the linked material fingerprint credential.

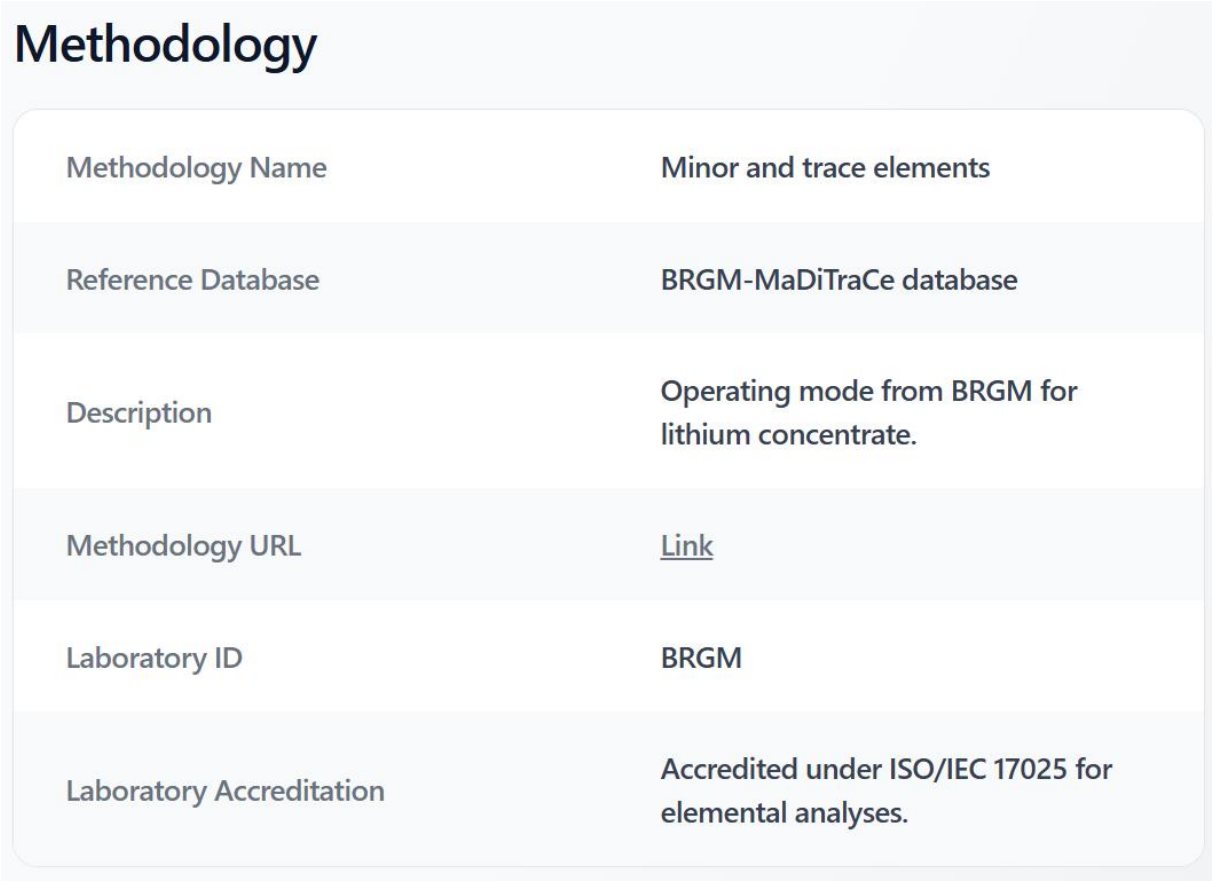

Figure 4 - Raw Material DPP frontend view of the Material Fingerprinting Certificate

Digital Traceability Architecture Components Used in UC1

- **DPP Identifier and Resolution:** Provides the identifier for the raw material batch and enables verifiers to resolve the DPP and retrieve linked evidence such as the material fingerprint credential through DID resolution.
- **Verifiable Data:** Represents the material fingerprint result as a cryptographically signed Verifiable Credential, ensuring the origin assessment is tamper-evident and independently verifiable across organizations.
- **Organization Identity Wallet:** Stores and manages credentials for issuers and participants and supports issuance, presentation, and verification workflows for the material fingerprint credential in a standardized SSI model.
- **Trust Chain (Root Credential):** Validates issuer legitimacy and credential authenticity by checking whether the fingerprint credential was issued by a trusted authority and whether it remains valid and not revoked.

Funded by the European Union

- **Credential Proof:** Ensures credential integrity and verifiability through standardized proof formats (e.g., JSON Web Signatures).
- **Semantics Layer:** Defines semantic interoperability for DPP attributes and material fingerprint evidence by modeling origin metadata, composition information, laboratory identifiers, and methodology using JSON-LD contexts.
- **Raw Material DPP Data Model:** Structures the representation of material batch information and its linked evidence, including laboratory-related details required for verification.

Use Case 2: Creation of UNTP Traceability Events

UNTP (UN/CEFACT, 2024) provides a voluntary, globally applicable B2B traceability framework, enabling downstream actors to verify provenance and chain-of-custody continuity. MaDiTraCe integrates UNTP traceability into the Raw Material DPP using the same architectural mechanism as for material fingerprinting evidence. Traceability events are encapsulated as verifiable, cryptographically protected data objects and then linked to the raw material's DID-based identifier. This makes supply chain information such as chain-of-custody (CoC) discoverable and verifiable across organizations without relying on a single central database.

In UNTP terms (UN Transparency Protocol, 2025), these digital traceability events (e.g., transaction, transformation, aggregation, and association) form a Transparency Graph that links input materials to output products through verifiable lineage relationships. In MaDiTraCe, this event evidence is attached to Raw Material DPPs so verifiers can reconstruct material flows and validate provenance relationships across supply chain tiers.

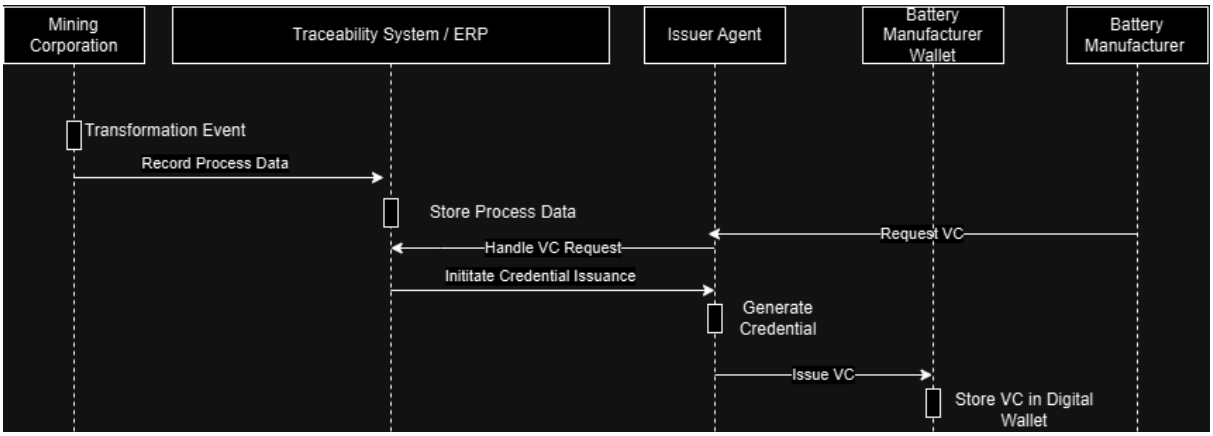

Figure 5 - Sequence Workflow for Recording a Traceability Event

The interaction flow for creating and attaching UNTP traceability event evidence follows the same credential-based pattern used for Material Fingerprinting but is triggered by operational lifecycle activity rather than laboratory assessment. As soon as a lifecycle step occurs, the initiating party records the corresponding process information as a traceability event in the traceability system or ERP environment. A credential request is then initiated toward an issuer agent, which evaluates the request context and generates a verifiable credential representing the traceability event in a machine-verifiable form. Once issued, the credential is transferred to and stored in the receiving wallet, where it becomes available for subsequent verification and can be linked to the Raw Material DPP through the DID-based identifier. The sequence in Figure 5 illustrates how dynamic CoC data can be transformed into trusted evidence that is discoverable through the DPP and verifiable across organizational boundaries. The system defines four distinct actor roles with specific operational requirements:

- **Upstream Manufacturer (Issuer):** Records custody and processing steps by issuing UNTP-aligned traceability event objects for received inputs and produced outputs to create machine-verifiable CoC evidence.
- **Raw Material Supplier (Holder):** Provides the incoming batch identifiers and associated evidence in form of transaction or transformation events.
- **Downstream Manufacturer (Verifier):** Retrieves the Raw Material DPP and linked traceability events to validate continuity of custody, mass-balance consistency, and the integrity of provenance claims before accepting the material into production.
- **Auditor (Independent Verifier):** Uses the event history to confirm that CoC requirements are met via evidence-based verification of compliance and ESG claims.

Digital Traceability Architecture Components Used in UC2

- **DPP Identifier and Resolution:** Provides the persistent identifier used to link UNTP traceability events to the raw material batch and enables downstream actors to retrieve the event evidence through the Raw Material DPP entry point.
- **Verifiable Data:** Encapsulates traceability events as cryptographically signed VCs, making chain-of-custody evidence tamper-evident and verifiable.
- **Organization Identity Wallet:** Stores and manages credentials used to issue, present, and verify traceability event credentials for event evidence presentations across the supply chain.

Funded by the European Union

- **Trust Chain:** Validates issuer legitimacy and credential authenticity so that traceability event credentials can be trusted as evidence created by verified economic operators.
- **Semantics Layer:** Ensures semantic interoperability for traceability event payloads and references by expressing event attributes, identifiers, and relationships in JSON-LD contexts and structured schemas.
- **Raw Material DPP Data Model:** Provides the structural mechanism to attach UNTP traceability event evidence to the Raw Material DPP, enabling verifiers to resolve a single DPP to access the required evidence.

Use Case 3: Linked DPP Data Sharing

This use case establishes the concept of linked Raw Material DPPs, where the passport of a downstream batch (Tier-n+1) explicitly references the identifier of its upstream input batch (Tier-n). From a raw material supply chain traceability perspective, this linkage is essential to create a traversable and auditable supply chain graph, allowing downstream economic operators to trace sustainability and provenance evidence back to upstream sources without relying on unstructured document exchange. In MaDiTraCe, the link is implemented directly inside the Tier-n+1 passport payload by including the upstream Raw Material DPP identifier (DID) as a structured reference within the downstream product record. This use case does not address mass-balance or infer missing provenance in mixed-material scenarios; it only links and shares available DPP evidence.

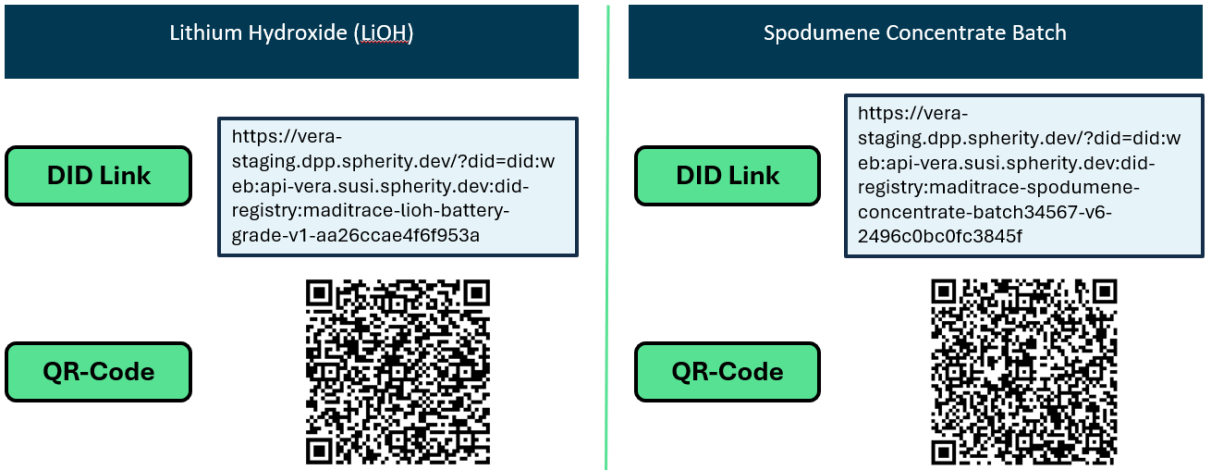

Figure 6 - Linked Raw Material DPP Identifiers across Tiers

The workflow begins when a Tier-n+1 processor produces a new batch and generates its Raw Material DPP. As part of the DPP creation step, the processor records the upstream inputs used in production by explicitly embedding one or more upstream batch identifiers. For example, a battery chemical intermediate passport can include a dedicated "Raw Material Sources" section that lists the DID of the upstream material passport (such as the Spodumene concentrate batch) and provides minimal relationship metadata. This makes the link between upstream and downstream passports enables verifiers to traverse the chain upstream by resolving the referenced identifiers in a machine-readable way.

Once the Tier-n+1 passport is published, the discovery process begins when a downstream economic operator retrieves the Tier-n+1 DPP (e.g., by resolving its DID from a QR code). The verifier can then follow the upstream reference embedded in the Tier-n+1 DPP and resolve the Tier-n passport to retrieve upstream evidence, such as origin proofs, sustainability indicators, certifications, and fingerprinting credentials. This enables practical inheritance workflows where downstream actors can validate upstream values (e.g., carbon footprint, origin assessment confidence) and use them as verified primary data inputs.

In addition to direct resolution via identifiers, the same linkage model can be implemented as part of governed cross-company data exchange through the dataspace. In this variant, the Tier-n+1 processor embeds the upstream DPP identifier in its passport, but access to the upstream passport content and evidence is retrieved using dataspace-controlled asset exchange via Eclipse Dataspace Connectors (EDC), as defined in Use Case 5.

In practice, this means the Tier-n+1 passport provides the upstream DID reference, while the upstream supplier exposes the corresponding upstream DPP payload and linked credentials as a dataspace asset. Downstream verifiers can then request this upstream asset through the EDC, ensuring that traceability remains possible even when upstream data is access-restricted. This explicit linking model provides a foundation for traceability at scale, because the relationship is expressed directly in the downstream DPP record. As a result, downstream actors can traverse and verify upstream evidence in a consistent manner, while suppliers retain control over sensitive data sharing through dataspace policy enforcement.

Actors

- **Tier-n Raw Material Supplier:** Publishes the upstream raw material DPP and exposes it either directly via its DID endpoint or as a governed dataspace asset.

Funded by the European Union

- **Tier-n+1 Manufacturer:** Creates the Tier-n+1 DPP and explicitly embeds upstream DPP identifiers as structured references to establish the traceability linkage.
- **Downstream Economic Operator (Verifier):** Resolves the Tier-n+1 DPP, follows upstream identifier references, and retrieves upstream passport evidence either directly or via EDC connector exchange (UC5) for compliance and reporting.
- **Auditor (Independent Verifier):** Verifies that upstream references are valid, that the linkage is consistent, and that inherited claims are supported by verifiable evidence across tiers.

Digital Traceability Architecture Components Used in UC3

- **DPP Identifier and Resolution:** Enables explicit referencing of Tier-n passports from within Tier-n+1 DPPs and supports traversal by resolving upstream identifiers.
- **Raw Material DPP Data Model:** Provides the structured mechanism (e.g., "Raw Material Sources") to store upstream DPP identifiers inside the Tier-n+1 passport payload.
- **Semantics Layer:** Ensures upstream reference semantics are machine-readable and interoperable across organizations and IT systems via standardized JSON-LD contexts and schemas.
- **Verifiable Data:** Ensures that upstream evidence (e.g., certificates or fingerprint results) is verifiable when retrieved through linked passports.
- **Trust Chain:** Allows verifiers to confirm issuer trust and authenticity for both upstream and downstream passports and linked credentials.
- **Data Exchange Protocol (EDC + DCP/DSP stack):** Enables retrieval of upstream passport data as a data asset over the DCP/DSP stack using connector-based exchange and contract enforcement.
- **SSI Authorization & Access Control:** Enforces policies for upstream data access when upstream passport content is shared through the dataspace.

3.2. Governance, Trust, & Interoperability Use Cases

This subchapter presents the governance, trust, and interoperability use cases that enable scalable ecosystem participation and controlled data exchange, including automated

dataspace onboarding, sovereign evidence sharing via connector-based protocols, and risk-based red-flag governance mechanisms for enhanced due diligence.

Use Case 4: Automated Dataspace Onboarding via Wallets

For raw material supply chain traceability, participation in a dataspace provides significant benefits as it enables secure B2B exchange of DPP data, provenance evidence, and chain-of-custody information between upstream suppliers and downstream economic operators (e.g., battery manufacturers, refiners, or OEMs in Catena-X). However, scaling such participation requires onboarding mechanisms that do not rely on manual checks by dataspace administrators. This use case therefore introduces an automated onboarding approach where the Organization Identity Wallet (OID) becomes the authorization instrument for joining the dataspace.

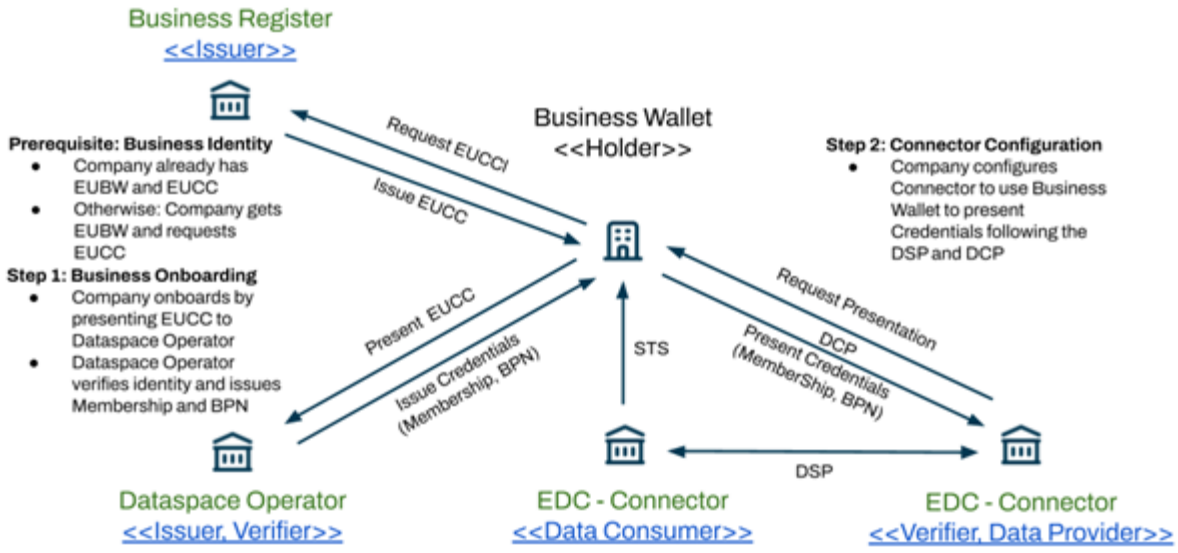

Figure 7 - Automated dataspace onboarding via OIDs

The onboarding process assumes that the organization already holds an enterprise credential (e.g., Legal Person Identifier (LPID) or EU Company Certificate (EUCC)) in its OID wallet. In this concept, a national business registry acts as the trusted issuer of such credentials. This credential acts as the foundational proof that the company is the correct legal entity and can be authenticated within the dataspace onboarding flow.

When the raw material supply chain provider connects to the dataspace, it presents the enterprise credential in its wallet to the dataspace operator. The dataspace operator verifies the credential cryptographically by validating its assertion proof, checking its status against revocation information, and confirming the issuer's authority via trust lists. In addition, the

Funded by the European Union

presenter is authenticated through the provided proof. Depending on dataspace-specific onboarding policies, this verification scope can be extended with additional credentials (e.g., ESG or ISO-related proofs).

Once successful verification is completed, the dataspace operator issues a dataspace membership credential to the organization. From a traceability perspective, this is the key step that turns a raw material supplier into a recognized participant who can publish and consume traceability-relevant information—such as Raw Material DPP references, conformity evidence, or UNTP-aligned events—under governed access control rules.

After onboarding, the connector-side access configuration is established so that the organization's EDC connector can use the wallet during data exchange to present the required credentials. In practical raw material DPP scenarios, this allows an upstream supplier to expose selected passport attributes and traceability evidence through their EDC connector to authorized downstream actors. For example, a battery manufacturer or OEM can request specific datasets (composition, origin evidence, certification credentials, chain-of-custody events), and the dataspace authorization layer can evaluate whether the requesting party is permitted to access them based on membership and verifiable claims presented via its wallet.

Actors

- **Business Registry (Issuer):** Issues the enterprise credential (LPID or EUCC) as a trusted digital identity credential for the organization to store and later present in onboarding and B2B interactions.
- **Organization (Holder):** Stores the enterprise and dataspace membership credentials in its wallet and presents them with authentication proof during onboarding and connector-based data exchange.
- **Dataspace Operator (Verifier + Issuer):** Verifies enterprise credential validity, and status, and issues the dataspace membership credential.

Digital Traceability Architecture Components Used in UC4

- **Enterprise Credential:** Foundational business identity credential used to prove that the actor (e.g., mine, refiner, processor) is a legitimate legal entity. In UC4, the enterprise credential acts as the trust basis before any dataspace participation is allowed.

- **Organization Identity Wallet:** Operational agent of the organization during onboarding. It stores the enterprise credential and presents it to the dataspace onboarding service provider.
- **Trust Chain:** Enables the dataspace to verify who issued the enterprise credential and whether the issuer is trusted (e.g., business register).
- **Verifiable Data:** The onboarding process is executed via VCs, starting with the enterprise identity credential and ending with issuance of a dataspace Membership Credential. Verifiable Credential check is the standardized mechanism that enables trust automation in onboarding.
- **EDC Connector:** Enforces credential-based access control for traceability data exchange and integrates wallet-based presentation during DCP interactions.

Use Case 5: Verifiable Data Exchange over Dataspace Protocols

Following automated dataspace onboarding (UC4), the raw material supply chain provider becomes a verified dataspace participant and can exchange traceability-relevant evidence with downstream economic operators under governed and sovereign conditions. This use case defines how a supplier shares DPP data and linked verifiable evidence in form of VCs. The exchange in the dataspace is performed peer-to-peer and controlled by machine-enforceable usage policies, ensuring that the supplier remains in control of its data.

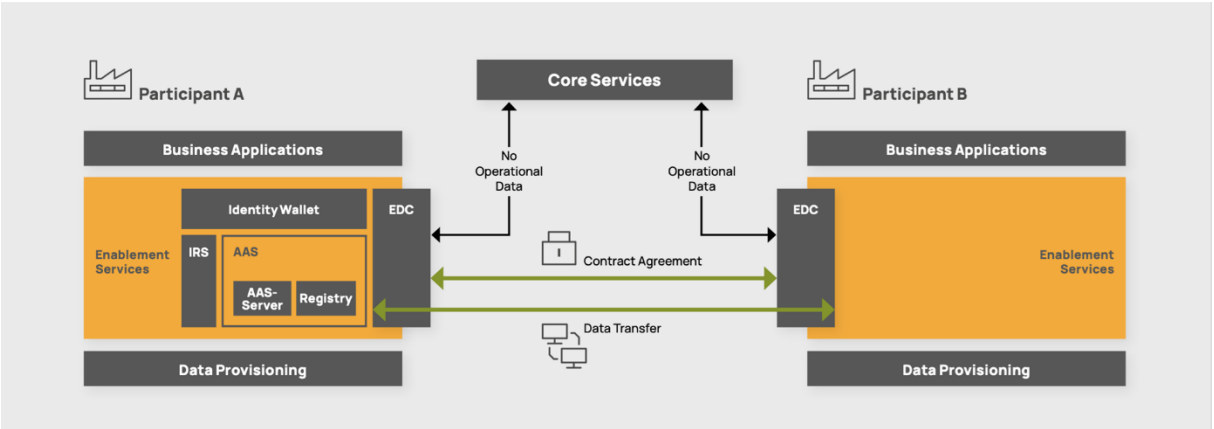

Figure 8 - Catena-X Data Exchange Framework with Eclipse Dataspace Connector and Asset Administration Shell (Catena-X, 2023)

The exchange workflow begins when the supplier makes selected assets available through its dataspace interface, typically via its EDC. These assets can include DPP payloads, linked VCs, or traceability records that downstream operators require for due diligence and chain-

Funded by the European Union

of-custody verification. Rather than exposing everything openly, the supplier attaches access rules to the offer so that only authorized participants can retrieve the evidence. This policy-driven interaction model is the key step that makes dataspace membership an essential feature for traceability. The connector-based architecture that enables contract-governed exchange is illustrated in Figure 8.

Before any data transfer is permitted, the architecture establishes trust and authorization using the credential mechanisms introduced during onboarding. In this step, the requesting economic operator proves that they are a valid dataspace participant by presenting the required credentials from their organizational identity wallet. After contract agreement, the actual data exchange takes place through the dataspace transfer protocol under the conditions defined in the negotiated contract.

The economic operator retrieves the requested evidence directly from the supplier endpoint through the connector-mediated transfer process, which preserves the integrity and origin of the payload. In a raw material traceability scenario, this enables downstream actors to receive verified upstream evidence (e.g., company certificates or fingerprinting VCs) and integrate it into their own compliance validation workflows, while the supplier remains in control of access and distribution.

Actors

- **Raw Material Supplier (Data Provider):** Publishes Raw Material DPP assets and linked verifiable evidence through the dataspace connector, defines usage policies and access rules, and provides the requested payloads through governed connector-to-connector exchange.
- **Downstream Economic Operator (Data Consumer):** Requests traceability evidence (e.g., DPP payloads, certificates, compliance attributes), presents membership credentials for authorization, and retrieves the evidence via the dataspace protocols.
- **Dataspace Governance:** Provides the policy and contract framework that ensures participants apply consistent trust rules and that data exchange follows the network governance model.

Digital Traceability Architecture Components Used in UC5

- **Data Exchange Protocol:** Enables connector-to-connector data exchange over EDC via dataspace protocol stack (DCP + DSP), ensuring that traceability evidence is exchanged under governed contract terms.
- **SSI Authorization & Access Control:** Evaluates whether the data consumer fulfills the access policy requirements before traceability data can be released.
- **Organization Identity Wallet:** Stores the organization's credentials and enables the presentation of verifiable proofs required to access restricted evidence.
- **Verifiable Data:** Represents the exchanged evidence in tamper-evident, cryptographically verifiable form, enabling downstream verification after transfer.
- **Digital Twin:** Supports discovery and structured referencing of DPP assets and traceability evidence made available for exchange within the dataspace ecosystem.
- **Semantics Layer:** Ensures that exchanged DPP payloads and evidence remain interpretable across organizations and systems, enabling semantic interoperability across the value chain.
- **Asset Administration Shell (AAS):** Provide industrial-grade structuring and referencing of exchanged assets, supporting standardized access to DPP-linked information in digital twin contexts.

Use Case 6: Decentralized Red Flag Governance

Moving beyond static certification models, this use case introduces a red flag governance mechanism that enables dynamic trust management across multi-actor raw material supply chains. Instead of relying only on periodic audits, MaDiTraCe allows verified supply chain actors to issue machine-verifiable non-conformity signals when potential issues are detected during verification. This supports responsible sourcing and due diligence expectations, e.g., OECD-aligned workflows (OECD, 2016), including scenarios where risk indicators such as CAHRA-related sourcing signals require additional scrutiny.

Figure 9 illustrates the red flag workflow and certification governance logic. The workflow is triggered when a downstream actor (e.g., refiner, auditor, or manufacturer) identifies a discrepancy related to a material batch—for example, inconsistencies between observed properties and the claims linked in the DPP. Instead of escalating through informal

Funded by the European Union

communication channels, the detecting party issues a Red Flag Verifiable Credential. This red flag credential is cryptographically signed and linked to the batch DPP identifier, ensuring the signal remains tamper-evident and attributable to the issuing organization.

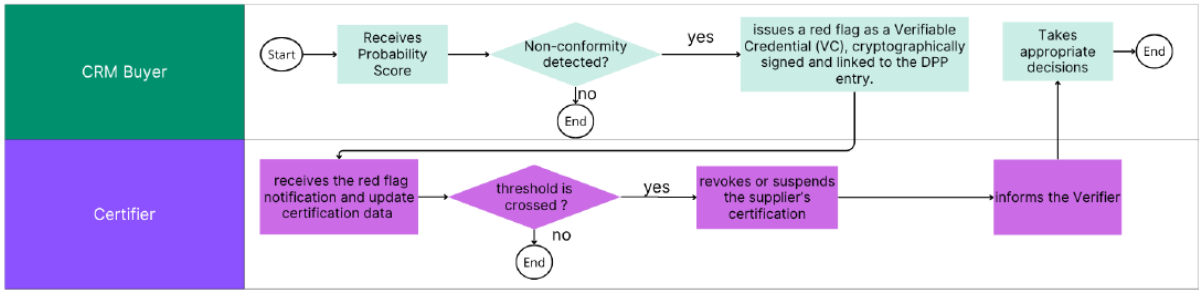

Figure 9 - Sequence workflow for issuing a traceability event as a Verifiable Credential

Importantly, issuing a red flag does not automatically invalidate the material record or revoke certifications by default. Instead, the red flag acts as a governance trigger that requires additional verification steps and stronger evidence before the material can continue to be treated as "verified" in downstream claims. Governance authority remains with the certification body, which defines escalation thresholds, aggregates red flags, and decides whether the relevant certification should remain valid, be suspended, or be revoked. Any party verifying the batch or supplier status acts as a verifier by checking the current certification state held by the certification body, ensuring decisions rely on up-to-date certification information rather than outdated documents.

To ensure that this mechanism has practical effect in digital traceability workflows, the governance authority platform may limit the issuance or publication of compliance-relevant credentials and assertions in the DPP. This allows the material to remain traceable and visible in the system, while clearly signaling that certain claims are under additional scrutiny.

Actors

- **Upstream Supplier (Subject of Assessment):** Provides the material batch and associated DPP evidence that may be flagged during verification.
- **Downstream Economic Operator (Red Flag Issuer):** Detects a potential non-conformity or risk indicator and issues a Red Flag VC linked to the batch DPP.
- **Certification Body (Governance Authority):** Aggregates red flag signals, evaluates them against predefined governance criteria, applies escalation thresholds, and maintains the authoritative certification status.

- **Downstream Buyer or Auditor (Verifier):** Checks the current certification status via the certification body and evaluates the batch based on the latest trust state.

Digital Traceability Architecture Components Used in UC6

- **Organization Identity Wallet:** Stores and manages credentials for supply chain actors and enables issuing and presenting Red Flag VCs.
- **Verifiable Data:** Represents red flags and supporting due diligence documentation as cryptographically signed evidence objects that remain tamper-evident and independently verifiable.
- **Enterprise Credential:** Ensures red flag issuers and governance authorities act under verified legal-entity identity.
- **Trust Chain:** Validates issuer legitimacy, credential authenticity, and status information so that red flag issuers, certification bodies, and evidence providers can be trusted within the governance workflow.
- **Semantics Layer:** Ensures that red flag credentials, due diligence evidence, and related DPP attributes are expressed in interoperable structures such as JSON-LD contexts and schemas so that different participants can interpret risk signals consistently.

4. PoC Architecture Evaluation

This section presents the final MaDiTraCe PoC architecture by reviewing how the architecture defined in the intermediate report (D3.4) is realized through the implemented and validated PoC use cases. Instead of restating the architecture purely as a conceptual model, this chapter evaluates the practical adoption of the D3.4 principles and building blocks in UC1–UC6, showing how traceability, evidence issuance, verification, linking across tiers, dataspace onboarding, and governed data exchange are supported by the implemented components.

4.1 Alignment of the PoC with Architecture Principles

The MaDiTraCe PoC architecture implements the design principles defined in D3.4 by translating them into concrete operational workflows across UC1–UC6. The architecture is implemented as a set of interoperable, verifiable, and modular building blocks that can be adopted incrementally by supply chain stakeholders. The resulting PoC demonstrates how

Funded by the European Union

raw material traceability can be realized using open standards, verifiable credentials, DID-based identifiers, and controlled data exchange mechanisms.

Accessibility is addressed by keeping core passport access lightweight and non-proprietary. The Raw Material DPP frontend provides simple entry points through DID links and QR codes, supports verification through a browser-based interface, and enables download of passport content in both human-readable and machine-readable formats. This lowers barriers for stakeholders with limited IT capabilities while maintaining the ability to integrate with enterprise systems where available.

Data accuracy is ensured by binding each traceability-relevant claim to an accountable issuer through verifiable credentials. This is demonstrated in UC1, where material fingerprinting results are issued by an authoritative body as probability-based evidence, and in UC2, where CoC events are recorded as structured credentials in the form of UNTP traceability events. The PoC enforces provenance by making issuer identity, signature validity, and credential integrity verifiable across organizational boundaries.

Interoperability is achieved by using open and widely recognized standards across all layers of the PoC. Identity and authenticity rely on W3C DID Core and Verifiable Credentials; semantic interoperability is supported through JSON-LD contexts and structured data categories; and cross-company exchange is aligned with dataspace practices using connector-based protocols. This ensures the architecture can interoperate with external ecosystems.

Modularity is implemented through a component-based architecture where each building block supports a distinct responsibility and can be deployed independently. The DPP is modeled as a bundle of verifiable credentials instead of a single monolithic payload, enabling separate issuance of product information, sustainability metrics, compliance status, and evidence such as material fingerprinting.

Verifiability is the core technical guarantee across the PoC. All evidence is signed, issuer-linked, and verifiable through standardized proof mechanisms. DIDs provide persistent identifiers for batches and organizations; VC integrity is validated cryptographically; and verification workflows support third-party validation of claims.

4.2 PoC Building Blocks and Their Utilization Across Use Cases

This section reviews the PoC architecture building blocks defined in D3.4 and explains how they are exercised across UC1–UC6. The building blocks form a layered traceability stack,

where the DPP and its evidence can be issued and verified locally, linked across tiers, and exchanged in governed data ecosystems. The architecture components as traceability-enabling layers are illustrated in Figure 10.

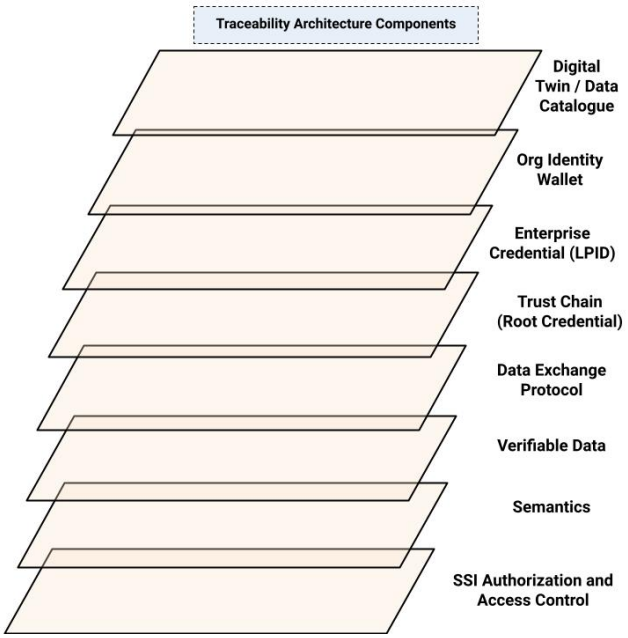

Figure 10 - MaDiTraCe Traceability Architecture Components

4.2.1 Digital Twin / Data Catalogue

The Digital Twin / Data Catalogue provides the discovery layer for DPP assets and linked evidence. It allows stakeholders to locate material batches, retrieve associated credentials, and navigate supply chain relationships. It is primarily relevant once multiple DPPs exist in the ecosystem, supporting UC3 (linked DPPs) and UC5 (dataspace data exchange) where discovery of relevant upstream assets is required.

4.2.2 Organization Identity Wallet

The Organizational Identity Wallet acts as the operational identity agent of an economic operator. It stores enterprise identity credentials, receives membership credentials during onboarding, and enables issuance and presentation workflows for verifiable data. It is central in UC4 (automated onboarding) and becomes an enabler for UC5 (policy-bound exchange) and UC6 (governance signals and evidence).

4.2.3 Enterprise Credential

Enterprise credentials provide the proof that an actor is a legitimate legal entity. These credentials support trusted onboarding and ensure that evidence exchange is attributable

Funded by the European Union

to verified organizations. This building block is critical to UC4 and indirectly supports UC5 and UC6 by ensuring that governance actions are issued by accountable entities.

4.2.4 Trust Chain

The Trust Chain establishes which issuers are trusted and ensures that credentials can be validated against appropriate trust anchors. It enables verification of issuer authenticity, credential integrity, and trust delegation. The trust chain is required in all use cases that require verifiable evidence (UC1, UC2, UC5, UC6) and is foundational for UC4 onboarding.

4.2.5 Data Exchange Protocol (Dataspace Protocol Stack and EDC)

The Data Exchange Protocol enables cross-company exchange under governance and usage policies. Within MaDiTraCe, this is the key mechanism for post-onboarding interactions where sensitive data cannot simply be published openly. It becomes the central enabler for UC5 and is configured as a downstream capability after UC4.

4.2.6 Verifiable Data (VCs)

Verifiable Data represents the common evidence format across the PoC. Instead of exchanging PDFs or informal claims, evidence is represented as cryptographically signed credentials that can be validated programmatically. This is the main output of UC1 (fingerprint evidence), UC2 (traceability events), UC5 (shared certifications and DPP attributes), and UC6 (red flags and enhanced due diligence evidence).

4.2.7 Semantics Layer

The semantics layer ensures that exchanged data remains interoperable and machine-interpretable. By structuring DPP attributes into consistent categories and using JSON-LD contexts, MaDiTraCe supports semantic alignment across different organizations and systems. This component is essential for UC1–UC3 (passport content and linking) and remains relevant for UC5 exchange scenarios where data is consumed across organizational boundaries.

4.2.8 SSI Authorization & Access Control

SSI-based authorization enforces who can access which evidence and under which rules. This ensures that membership credentials and governance rules translate into runtime access decisions in dataspace exchange scenarios. This component is central to UC5 and supports UC6 through “evidence gating” mechanisms, ensuring that compliance claims are restricted until additional due diligence evidence is supplied.

4.3 Summary Matrix: Use Case vs. Component Utilization

Overall, the PoC validates the D3.4 architectural approach by demonstrating that the traceability model can be realized through verifiable data primitives and modular components. UC1–UC3 show how raw material batch evidence is structured, linked, and made verifiable, while UC4–UC6 demonstrate how governance, onboarding, and controlled exchange mechanisms operationalize traceability at ecosystem scale. Table 1 provides the consolidated view that shows how each component is exercised across UC1–UC6.

Table 1 - Use case to Architecture Component Mapping

Architecture Component	UC1 Material Fingerprinting	UC2 UNTP Traceability Events	UC3 Linked DPPs	UC4 Automated Dataspace Onboarding	UC5 Verifiable Data Exchange	UC6 Red Flag Governance
Digital Twin	S	S	**C**	O	S	S
Org Identity Wallet	S	S	S	**C**	**C**	**C**
Enterprise Credential	O	O	O	**C**	S	S
Trust Chain	**C**	**C**	S	**C**	**C**	**C**
Data Exchange Protocol	O	O	S	S	**C**	O
Verifiable Data (VCs)	**C**	**C**	S	**C**	**C**	**C**
Semantics Layer	**C**	**C**	**C**	S	**C**	**C**
SSI Auth & Access Control	O	O	O	S	**C**	**C**

Legend: C = Core, S = Supporting, O = Optional

Funded by the European Union

5. Raw Material DPP Data Model

This section specifies the Raw Material DPP data model as implemented in the MaDiTraCe PoC and explains how raw material batch information is structured as verifiable, interoperable, and machine-readable data. The model builds on DID-based identifiers and JSON-LD semantics to ensure that passport content can be resolved and interpreted consistently across organizations and systems. To reflect practical implementation, the section derives the data model structure, categories, and attribute groups from the PoC Raw Material DPP examples (Spodumene Concentrate and Lithium Hydroxide).

5.1 Data Model Structure and Semantics

The MaDiTraCe Raw Material DPP data model is designed to represent a raw material batch as a verifiable digital asset that can be accessed, validated, and re-used across supply chain tiers. Each batch is assigned a W3C-compliant DID that acts as the unique and persistent batch identifier, enabling resolution through standard web infrastructure and avoiding reliance on proprietary platforms. This DID-based approach allows downstream economic operators to reference and retrieve DPP content in a consistent manner, supporting interoperability across multiple organizations and systems.

In the MaDiTraCe prototype implementation, the DPP is made available through a web-based frontend that exposes both human-readable views and machine-readable payloads. The frontend provides access to the DPP identifier, supports verification of associated credentials, and enables downloads in formats suitable for different stakeholders. This is illustrated in Figure 11, which shows how identifiers, verification, and download capabilities are combined to ensure that the DPP content is accessible in a verifiable manner for both operational use and audit contexts.

Beyond static data representation, the Raw Material DPP is structured to support verifiable evidence attachment, where third-party credentials can be linked to the passport and validated through a consistent verification pipeline. In the MaDiTraCe examples, this includes material fingerprinting evidence with probability-based origin attribution, as introduced in UC1.

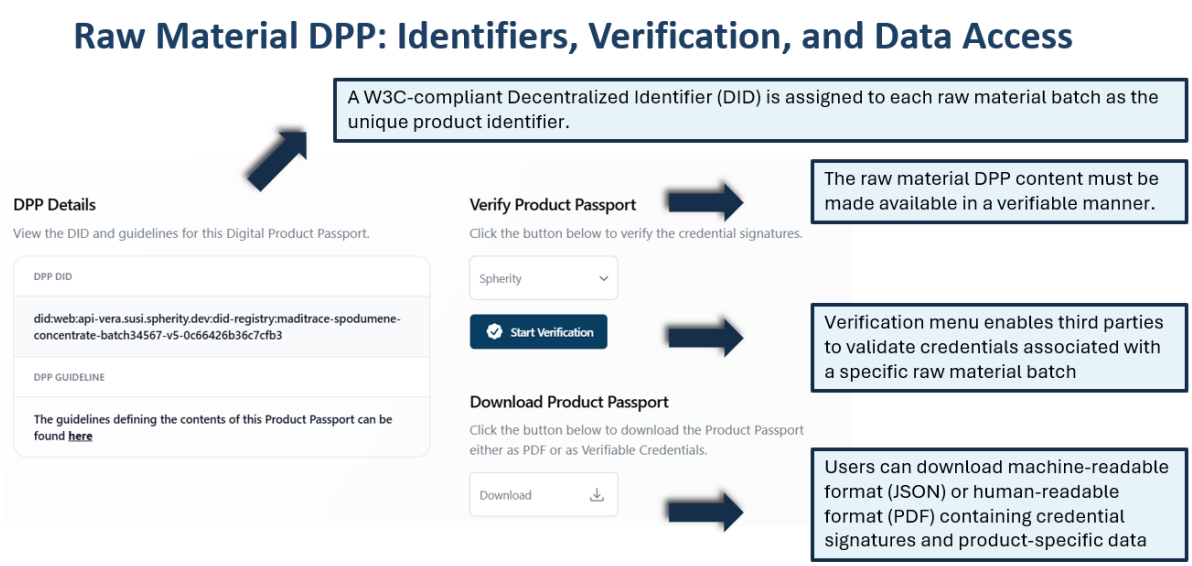

Figure 11 - Raw Material DPP Frontend with did:web-based identifiers, credential verification, and data access options for a raw material batch

5.2. Data Categories and Attributes

The Raw Material DPP content is organized into consistent data categories that reflect the needs of regulatory compliance, sustainability reporting, and supply chain traceability. This structure is based on the initial requirements and core attribute set consolidated in Deliverable D3.8 "Supply Chain Mapping, Requirements, Elicitation, Classification" (data attributes, requirements, and accessibility) and the practical DPP implementation guidance in Deliverable D3.3 "Guidelines for Methodology Implementation". The two Raw Material DPP examples–Spodumene Concentrate Batch and Lithium Hydroxide Battery Grade Batch –follow the same structural logic, combining product identity and classification attributes with sustainability indicators, compliance information, and evidence metadata.

The core category *Product Overview* captures the batch snapshot required for identification and contextual interpretation. This includes product name, batch number, category, and chemical formula, alongside manufacturing context such as manufacturer name, location, contact, production date, and expiry date. These attributes provide the minimal baseline required to uniquely describe the material and support downstream referencing in procurement, due diligence, and audit workflows.

A second foundational category is I*dentifiers and Trade Classification*, which ensures cross-system compatibility with widely adopted identification schemes. Both DPP examples include structured fields for GTIN, HS Code (including description), and CAS Number,

Funded by the European Union

enabling alignment with customs classification, chemical registries, and existing ERP master data. This category ensures that DPP data remains usable beyond the DPP environment itself and can be mapped to operational systems.

Sustainability-related information is captured under *Energy & Carbon Footprint* and *Water & Land Use*, supporting ESG reporting and downstream footprint aggregation. The Spodumene DPP provides metrics such as electricity consumption, fuel energy consumption, and a total carbon footprint, alongside water withdrawal, discharge, reuse/recycle rate, and land use indicators. The Lithium Hydroxide DPP mirrors the same structure, with values adapted to its processing context. These structured indicators allow downstream economic operators to incorporate upstream verified sustainability values into their own calculations and reporting workflows. The indicators are selected in alignment with the project's LCI approach (i.e., use of Life Cycle Inventory datasets and consistent impact assessment choices), as documented in Deliverable 4.7 "LCAs of selected materials and products".

A dedicated area of the DPP supports *Traceability and Origin Evidence*, where scientifically grounded proofs can be attached as structured evidence. In both examples, the DPP contains material fingerprinting metadata including methodology name, reference database, laboratory ID, and accreditation information, as well as a probability-based origin result. This evidence model directly corresponds to the fingerprinting workflow described in UC1 (Chapter 3.1).

The DPP also includes a *Regulatory Status* category that captures compliance-relevant declarations and hazard classification attributes. The example DPPs contain a REACH registration status, EU Battery Regulation compliance status, UN transport reference, and hazard classification. This category supports automated checks and provides a standardized compliance overview for downstream processors, auditors, and regulators. Finally, both DPPs include operational information under *Logistics & Processing* as well as *Safety & Handling*, supporting real-world transport, storage, and handling workflows. This includes transport mode, processing location, and safety instructions.

The overall data category structure is illustrated in Figure 12, which shows how the Raw Material DPP frontend organizes the passport into product overview, sustainability, and traceability and compliance sections, enabling users to navigate both static batch information and linked evidence.

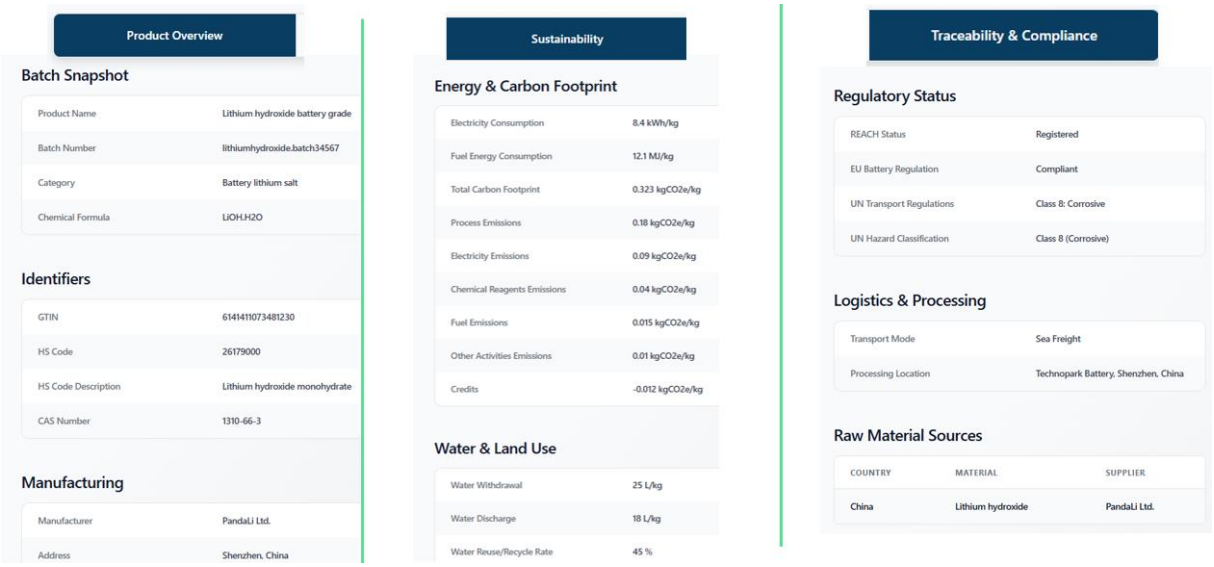

Figure 12 - Raw Material DPP Core Data Elements

5.3. Example Payload: Spodumene Concentrate Batch

The compressed JSON-LD payload in Appendix represents the main structure of the verifiable Raw Material DPP data as implemented in the PoC for a specific batch of high-grade spodumene concentrate. In the MaDiTraCe implementation, the DPP is modeled as a bundle of Verifiable Credentials, where each credential covers a specific data domain. All credentials share the same batch DID, enabling verifiable evidence to be resolved and validated over a single structure.

6. Conclusions

This deliverable presents the final architecture and Proof of Concept (PoC) implementation for the MaDiTraCe project, demonstrating the successful transition from the intermediate architecture definition in D3.4 to an operational, standards-aligned traceability stack for critical raw materials. The implemented PoC validates that a modular architecture based on Self-Sovereign Identity, DIDs, and VCs can support trustworthy, multi-tier traceability without introducing centralized data silos. Through the defined use cases (UC1–UC6), MaDiTraCe shows how evidence can be issued, linked, verified, and exchanged across organizations in a way that remains interoperable and auditable.

A central innovation demonstrated in the PoC is the integration of Material Fingerprinting as verifiable origin evidence. By encapsulating probability-based analytical results into cryptographically signed Verifiable Credentials and linking them to Raw Material DPPs, the

Funded by the European Union

architecture strengthens the physical–digital connection and reduces traceability risks such as material substitution and decoupling attacks. In parallel, the PoC validates how traceability evidence can evolve beyond static product snapshots by supporting UNTP-aligned traceability events. This PoC of a DPP connected to material fingerprint is one of the main achievements of MaDiTraCe project. However, the generalisation of Material Fingerprinting for a substance (e.g., lithium) would require the development and consolidation of a reference database.

Beyond the DPP data model itself, MaDiTraCe demonstrates that scalable traceability requires governance and interoperability mechanisms at ecosystem level. The PoC therefore includes an architecture path from automated dataspace onboarding using enterprise identity credentials and organizational wallets to controlled, policy-bound data exchange using connector-based protocols. Together with the red-flag governance concept, which enables risk-based escalation and enhanced due diligence evidence requirements, the PoC illustrates how trust can be maintained through verifiable, role-based evidence workflows rather than relying solely on periodic audits or document-based checks.

Funded by
the European Union

7. References

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

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

BRGM. (2026). *BRGM: French geological survey.* Retrieved from https://www.brgm.fr/en

Catena-X. (n.d.). Why: Understanding the Catena-X Data Space. Retrieved from https://catenax-ev.github.io/docs/operating-model/why-understanding-the-catena-x-data-space

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

CEN/CENELEC JTC 24. (2025a). prEN 18216: Digital product passport – Data exchange protocols. CEN-CENELEC Management Centre.

CEN/CENELEC JTC 24. (2025b). prEN 18219: Digital product passport – Unique identifiers. CEN-CENELEC Management Centre.

CEN/CENELEC JTC 24. (2025c). prEN 18220: Digital product passport – Data carriers. CEN-CENELEC Management Centre.

CEN/CENELEC JTC 24. (2025d). prEN 18221: Digital product passport – Data storage, archiving, and data persistence. CEN-CENELEC Management Centre.

CEN/CENELEC JTC 24. (2025e). prEN 18222: Digital Product Passport – Application Programming Interfaces (APIs) for the product passport lifecycle management and searchability. CEN-CENELEC Management Centre.

CEN/CENELEC JTC 24. (2025f). prEN 18223: Digital Product Passport – System interoperability. CEN-CENELEC Management Centre.

CIRPASS. (2024). CIRPASS: Digital product passport initiative. Available from: cirpassproject.eu/

European Parliament and Council. (2023). Regulation (EU) 2023/1542 of the European Parliament and of the Council of 12 July 2023 concerning batteries and waste batteries, amending Directive 2008/98/EC and Regulation (EU) 2019/1020 and repealing Directive 2006/66/EC (EU Battery Regulation).

European Parliament and Council. (2024a). Regulation (EU) 2024/1252 of the European Parliament and of the Council of 11 April 2024 establishing a framework for ensuring a secure and sustainable

Funded by the European Union

supply of critical raw materials and amending Regulations (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1724 and (EU) 2019/1020 (Critical Raw Materials Act).

European Parliament and Council. (2024b). 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 (Ecodesign for Sustainable Products Regulation).

European Parliament and Council. (2024c). Directive (EU) 2024/1760 of the European Parliament and of the Council of 13 June 2024 on corporate sustainability due diligence and amending Directive (EU) 2019/1937 and Regulation (EU) 2023/2859.

Gäbler, H. E., Schink, W., & Gawronski, T. (2020). Data evaluation for cassiterite and coltan fingerprinting. Minerals, 10(10), 1–15. https://doi.org/10.3390/min10100926

OECD. (2016). OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas (3rd ed.). Retrieved from https://www.oecd.org/content/dam/oecd/en/publications/reports/2016/04/oecd-due-diligence-guidance-for-responsible-supply-chains-of-minerals-from-conflict-affected-and-high-risk-areas_g1g65996/9789264252479-en.pdf

Thania Nowaz, Paulina Fernandez, Lukas Förster, Michael Tost, Daniel Monfort Climent, Samuel Olmos Betin, and Frank Melcher. (2025). Navigating the mining industry challenges: An introduction to the cera 4in1 standards. Berg- und Hüttenmännische Monatshefte, 170(2):108–11

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

UN/CEFACT. (2026). *Trade Facilitation and E-business (UN/CEFACT).* Retrieved from https://unece.org/trade/uncefact

UN Transparency Protocol (UNTP). (2025). Digital Traceability Events. Retrieved from https://untp.unece.org/docs/specification/DigitalTraceabilityEvents

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. (2020). JSON-LD 1.1. Retrieved from https://www.w3.org/TR/json-ld11/

W3C. (2024). JSON Web Signatures for Data Integrity Proofs. Retrieved from https://www.w3.org/TR/vc-jws-2020/

8. Appendix

Appendix provides an example of a compressed JSON-LD payload for the Spodumene Concentrate Batch #34567 Raw Material DPP.

{ "type": ["VerifiableCredential"],

"issuer": "did:web:...:brgm-french-geological-survey",

"issuanceDate": "2025-12-04T06:45:48Z",

"@context": [

"https://www.w3.org/2018/credentials/v1",

"https://.../maditrace-product-information.jsonld"],

"credentialSubject": {

"id": "did:web:...:maditrace-spodumene-concentrate-batch34567",

"type": ["MaditraceProductInformation"],

"productName": "Spodumene concentrate",

"batchNumber": "spodumen.batch34567",

"chemicalFormula": "LiAl(Si2O6)/SiO2"

},

"proof": { "type": "Ed25519Signature2018", "jws": "<truncated>" }

},

{

"type": ["VerifiableCredential"],

"issuer": "did:web:...:brgm-french-geological-survey",

"issuanceDate": "2025-12-04T06:45:48Z",

"@context": [

"https://www.w3.org/2018/credentials/v1",

"https://.../maditrace-sustainability.jsonld"

],

Funded by the European Union

"credentialSubject": {

"id": "did:web:...:maditrace-spodumene-concentrate-batch34567",

"type": ["MaditraceSustainability"],

"totalCarbonFootprint": { "value": 0.323, "unit": "kgCO2e/kg" }

},

"proof": { "type": "Ed25519Signature2018", "jws": "<truncated>" }

},

{

"type": ["VerifiableCredential"],

"issuer": "did:web:...:brgm-french-geological-survey",

"issuanceDate": "2025-12-04T06:45:48Z",

"@context": [

"https://www.w3.org/2018/credentials/v1",

"https://.../maditrace-traceability-compliance.jsonld"

],

"credentialSubject": {

"id": "did:web:...:maditrace-spodumene-concentrate-batch34567",

"type": ["MaditraceTraceabilityCompliance"],

"reachStatus": "Pending registration",

"euBatteryRegulation": "Compliant"

},

"proof": { "type": "Ed25519Signature2018", "jws": "<truncated>" }

},

{

"type": ["VerifiableCredential"],

"issuer": "did:web:...:brgm-french-geological-survey",

"issuanceDate": "2025-12-04T06:45:48Z",

"@context": [

"https://www.w3.org/2018/credentials/v1",

"https://.../maditrace-material-fingerprint.jsonld"

],

"credentialSubject": {

"id": "did:web:...:maditrace-spodumene-concentrate-batch34567",

"type": ["MaditraceMaterialFingerprint"],

"methodology": "Minor and trace elements",

"originProbabilities": [

{ "mine": "Mine 1", "country": "Australia", "probability": 0.95 },

{ "mine": "Mine 2", "country": "Australia", "probability": 0.05 }

]

},

"proof": { "type": "Ed25519Signature2018", "jws": "<truncated>" }

}

Funded by
the European Union