PACE-DPP
Digital Product Passport

REPORT ON DATA-ECOSYSTEM SPECIFICATION, DEVELOPMENT AND OPERATION 2025

DOCUMENT TYPE:	**DELIVERABLE**
DELIVERABLE N^0:	**D4.1**
DISTRIBUTION LEVEL:	**PUBLIC**
DATE:	**14/08/2025**
VERSION:	**FINAL**

AUTHOR(S):	**CHRISTOPH KLIKOVITS (FORSCHUNG BURGENLAND GMBH)** **CHRISTOPH FABIANEK (OWNYOURDATA)** **MARTIN KJÄER (TU WIEN)**
REVIEWED:	**STEFAN KASER (INFINEON)**
FORMAL REVIEWED:	**YASMIN LICHTENWAGNER (VIRTUAL VEHICLE)**
APPROVED:	**MARTIN BENEDIKT (VIRTUAL VEHICLE)**

PROJECT ACRONYM:	**PACE-DPP**
PROJECT TITLE:	**PROMOTE & ACCELERATE CIRCULAR ECONOMY BY DIGITAL PRODUCT PASSPORTS**
FFG PROJECT N^0:	**917177**
CHALLENGE:	**CIRCULAR ECONOMY, DATA-SERVICE ECOSYSTEMS**
PROJECT DURATION:	**01/01/2025 - 31/12/2027**
PROJECT WEBSITE:	**WWW.DPP-AUSTRIA.AT**
COORDINATION:	**VIRTUAL VEHICLE RESEARCH GMBH**

DOCUMENT HISTORY

REVISION	DATE	AUTHOR	DESCRIPTION
0.1	26/05/2025	Christoph Fabianek	initial document structure and content
0.2	30/06/2025	Christoph Klikovits	initial document structure and content, task assignment
1.3	10/11/2025	Christoph Klikovits	Update Data Ecosystem, Results
1.4	10/11/2025	Christoph Fabianek	Use-Case Scenarios content
1.5	19/11/2025	Christoph Klikovits	Review and Reference Revision
1.6	16/02/2025	Stefan Kaser	Review

Executive summary

As part of Work Package 4 of the PACE-DPP project, the foundation has been laid for a conceptual and technical framework to support a digital data ecosystem centered around the Digital Product Passport (DPP). The goal is to create a robust basis for the effective use of DPP data, aligned with current and emerging regulatory requirements, and to foster the development of trustworthy and interoperable data spaces.

In the initial phase, key issues in the areas of metadata, data access, identity management, and data intermediation were systematically explored. The focus was placed on identifying and structuring fundamental requirements as well as developing preliminary architectural and semantic building blocks for scalable implementation.

As a practical starting point, exemplary use case scenarios in the timber industry were defined in order to concretely analyze the data flows and information models along a product's lifecycle. Based on these scenarios, initial insights were gained regarding necessary metadata structures and specific challenges related to data compatibility, system interoperability, and regulatory compliance.

In parallel, an initial analysis of existing frameworks for decentralized identity and access management was conducted. The long-term objective is to develop a well-tuned, flexible system that enables differentiated access rights across various stakeholder groups within the ecosystem. In this context, the role of data intermediaries - particularly in accordance with the requirements of the Data Governance Act - was also examined. Initial conceptual considerations regarding their integration into a future trustworthy data environment were formulated.

These initial activities serve as a foundation for further developments within the project. They contribute to the targeted preparation of future technical implementations and help establish a shared understanding of the requirements, opportunities, and challenges in building a Digital Product Passport. Future work will focus increasingly on validating and implementing the developed concepts, as well as integrating feedback from real-world use cases and project partners.

Contents

Introduction 6
Objectives of the Deliverable 7
Intended Audience 8
1 Technology research & State of the Art 9
1.1 Methodology 9
1.1.1 TOGAF as a Methodological Framework 9
1.1.2 Sitra Rulebook as a Governance and Ecosystem Building Block 11
1.1.3 Combined Approach (TOGAF & Sitra Rulebook) 12
1.2 Technology Stack - Research 13
1.2.1 Infrastructure and Technical Approaches 13
1.2.2 Quality Attribute Scenarios (QAS) 17
1.3 A textbook example 18
1.3.1 The six components of a Quality Attribute Scenario 18
1.3.2 Standards-compliant gateway for DPP 18
1.3.3 Federated onboarding with Decentralized Identifiers (DIDs) 19
1.3.4 Wood Use Case Scenario considerations (text book example): 19
1.4 Approaches and Outputs from other works 20
1.4.1 CIRPASS – Ontology and System Architecture for the Digital Product Passport (DPP) 20
1.4.2 CIRPASS-2 – Specification of the DPP Core Ontology 21
1.4.3 The DPP Vocabulary Hub 22
1.4.4 Implications for PACE-DPP 22
1.5 Regulatory Requirements and Standards 23
1.5.1 ESPR 23
1.5.2 EUDR 24
1.5.3 Substantive Requirements for Compliance 24
1.5.4 Obligations of Authorities and Enforcement 25
1.5.5 Relevant International Standards 25
1.5.6 Wood Use Case Scenario specific regulatory requirements: 25
2 Data-Ecosystem Specification 27
2.1 Meta-Data Specification 27
2.2 Decentralised Identity and Access Management 27
2.3 Data Intermediary and Governance 27
2.4 Initial linkage to rapid prototypes (Use-Case-scenarios) 27
2.4.1 Use Case Scenario Summary: Local DPP with did:peer 28
2.4.2 Use Case Scenario Summary: Luminant 28
2.4.3 Use Case Scenario Summary: Improve Forest Owner Data Sharing 28
2.4.4 Use Case Scenario Summary: Client-Managed Secret Mode (CMSM) 28
3 Development of the Data-Ecosystem 30
3.1 Scalable Architecture 30

3.2 Implementation Methodology 30
3.3 Tools, Platforms and Integration Concepts 30
4 Results from 2025 and Outlook 31
4.1 Use Case Scenario "Local DPP with did:peer" 31
4.2 Use Case Scenario "Luminant" 32
4.3 Use Case Scenario "Improve Forest Owner Data Sharing" 34
4.4 Use Case Scenario "Client-Managed Secret Mode" 36
4.5 Key Findings of the Annual Report 2025 38
4.6 Planned Development in 2026/2027 38
Figures & Tables 40
References 41

Introduction

This deliverable provides an initial overview of the conceptual and technical foundations being developed within Work Package 4 (WP4) of the PACE-DPP project. The focus lies on establishing a comprehensive data ecosystem that enables secure, interoperable, and regulation-compliant data exchange for the Digital Product Passport (DPP). The work documented in this report marks the beginning of a longer-term effort to translate the high-level goals of the DPP initiative into a structured, scalable, and stakeholder-oriented technical architecture. It builds on existing research, policy frameworks, and industry needs, and incorporates early practical insights derived from initial use case scenarios in the timber industry.

The structure of this deliverable follows a logical progression that reflects the methodological and content-based work phases of the project:

1. **Technology and State-of-the-Art Research**
   The first phase involves a broad exploration of existing technologies, frameworks, and digital infrastructures relevant to the realization of data ecosystems and DPP-related services. The focus lies on identifying key architectural patterns, best practices, and available open-source components that can serve as a foundation for the technical design.

2. **Analysis of Regulatory Requirements and Standards**
   Building on this technological groundwork, the second step concentrates on identifying and analyzing regulatory frameworks and industrial standards. These include, among others, the Data Governance Act, the Ecodesign for Sustainable Products Regulation, and upcoming EU-level specifications on data exchange, access control, and digital identities. This ensures that the emerging ecosystem aligns with legal obligations and promotes market adoption.

3. **Data Ecosystem Specification: What needs to be implemented**
   The next section addresses the conceptual foundation of the data ecosystem, answering the question: ***what*** needs to be developed. It outlines the key functional areas and capabilities required to realize a compliant and interoperable DPP infrastructure, with a particular focus on metadata specifications, identity and access management, and the role of data intermediaries. The section introduces early implementation plans and possible design approaches for building a scalable and trustworthy environment.

4. **Development of the Data Ecosystem: How to implement it**
   In a subsequent step, the deliverable transitions from conceptual considerations to practical implementation planning. This section focuses on the *how*, outlining a roadmap for technical realization. It describes development strategies, system architectures (e.g., the DISP architecture), and agile methods used to prototype and validate components. The objective is to gradually move from research to structured development and integration.

5. **Operation and Operating Concepts**
   To ensure long-term usability and sustainability, the deliverable also includes a conceptual framework for operating the data ecosystem.
   - **Organisation and Roles**
     This subsection outlines the governance structure, operational responsibilities, and coordination mechanisms between involved actors, such as data holders, intermediaries, and end users.
   - **Monitoring, Maintenance and Support**
     It describes planned mechanisms for system monitoring, error handling, lifecycle management, and user support throughout the operation of the DPP infrastructure.
   - **Security, Compliance and Auditing**
     Security and compliance are central to ecosystem integrity. This part discusses security measures, audit mechanisms, and compliance verification strategies aligned with legal and ethical principles.
   - **Scalability and Performance Optimisation**
     As the DPP ecosystem is expected to grow, this section covers strategies to ensure scalability, system performance, and efficient resource use, including modular design

principles and distributed architecture patterns.

6. **Results from 2025 and Outlook**
   Finally, the deliverable reflects on the progress made during the year 2025 and provides an outlook for the next phases of the project.
   - **Key Findings of the Annual Report 2025**
     This section summarizes the most important insights gained from research and development activities in 2025, including lessons learned, validation results, and emerging challenges.

   - **Planned Development in 2026/2027**
     The report concludes with a preview of the planned technical and conceptual work in the years 2026 and 2027, including piloting, testing, partner onboarding, and operationalization of the developed ecosystem components.

Objectives of the Deliverable

The primary objective of this deliverable is to document the early conceptual groundwork for the design and implementation of the DPP data ecosystem. It captures the results of preliminary investigations into key components such as metadata structures, decentralized identity and access management, the role of data intermediaries, and the requirements for scalable technical architectures. Furthermore, it lays the foundation for aligning future developments with applicable standards and regulatory frameworks, such as the Data Governance Act and emerging ecodesign legislation. This report serves as both a reference point and a strategic orientation document for subsequent work within WP4 and the broader PACE-DPP project.

Intended Audience

This deliverable is intended for a broad and diverse audience that plays a role in the further development and implementation of the Digital Product Passport (DPP) and its supporting data ecosystem. Key target groups include technical experts and developers engaged in the design of interoperable digital infrastructures, as well as project partners and contributors who are actively shaping the conceptual and technical direction of Work Package 4.

Policy stakeholders - particularly those involved in regulatory development and standardization at national and European levels - form another central audience. The deliverable aims to support ongoing alignment with legal frameworks such as the Data Governance Act and the Ecodesign for Sustainable Products Regulation, and to offer insights that may feed into policy refinement and implementation strategies.

Industry representatives and research institutions, especially those exploring sustainable value chains and digital innovation in product lifecycle management, will also find relevant input and orientation in the findings presented. Special attention is given to the needs of small and medium-sized enterprises (SMEs), which are expected to benefit from scalable, standards-based data solutions.

Finally, this deliverable addresses the funding authority, providing transparency regarding the progress of the project and the strategic direction of WP4. It documents early achievements, conceptual considerations, and methodological foundations, thereby ensuring that the development trajectory remains visible and aligned with the broader program goals.

1 Technology research & State of the Art

According to the project proposal, following Tasks are planned in WP4 - DPP Data Ecosystem

- **Metadata Specification**
  Define how metadata should be structured, described, and standardized across the ecosystem
- **Decentralized Identity and Access Management**
  Introduce a secure and user-centric approach for authentication and authorization
- **Data Intermediaries**
  Explore and implement roles that enable secure, transparent, and compliant data exchange
- **Scalable Architecture**
  Develop a technical architecture that is robust, modular, and able to scale with adoption

Overall Goal:
WP4 aims to establish a **methodology** by applying different standardized frameworks, always in close cooperation with the other project partners.

1.1 Methodology

Frameworks Under Consideration

- TOGAF (The Open Group Architecture Framework) as the main methodological backbone [1]
- Sitra Rulebook as a guiding set of principles for data sharing and governance [2]

1.1.1 TOGAF as a Methodological Framework

TOGAF provides the Architecture Development Method (ADM) – an iterative cycle that can be adapted to project needs. The following phases outline the roadmap for the DPP Data Ecosystem:

Preliminary Phase

- Define scope and stakeholders
- Establish architecture principles (e.g. openness, federation, data sovereignty)

In this phase, the project team needs to **set the foundation** for WP4. The scope of the ecosystem must be clearly defined:

- Which domains are included?
- Which partners participate?

At the same time, key stakeholders have to be identified and mapped to their interests. This is also the moment to agree on **architecture principles** such as openness, sovereignty, federation, and interoperability. These principles will guide all later decisions and prevent conflicts between partners.

Architecture Vision

- Develop a vision for the DPP Ecosystem
- Describe stakeholder benefits
- Define high-level use cases

Here, the task is to **formulate a clear vision of the DPP Data Ecosystem**. This includes describing the future state of the ecosystem and highlighting tangible benefits for stakeholders such as trust, efficiency, and new business opportunities. High-level use cases should be outlined to make the vision concrete (e.g. sharing energy consumption data, enabling intermediary services, monetizing data access). The vision must be compelling enough to align all partners behind a common goal.

The goal is to create a clear picture of the future ecosystem and communicate why it matters. The vision should highlight added value (e.g., transparency, interoperability) and show practical use cases to keep partners engaged.

Business Architecture

- Model ecosystem business processes (e.g. data provision, intermediary services, monetization)
- Define roles and responsibilities

At this stage, the focus lies on **describing the operational logic of the ecosystem**. All relevant business processes, such as data provision, intermediary brokering, and monetization, have to be modeled. For each process, the roles and responsibilities of the different actors need to be clearly defined. This step also requires drafting governance structures:

- Who decides on rules?
- Who enforces compliance?

By clarifying these aspects early, the ecosystem avoids misunderstandings and ensures transparent cooperation.

Information Systems & Data Architecture

- Define data flows, interfaces, semantic standards
- Evaluates the usage of IDS / GAIA-X connectors

The TODO here is to **design the data layer of the ecosystem**. This means defining how data flows between actors, what interfaces are needed, and which semantic standards should be applied to ensure interoperability. A central question is how to integrate with existing European initiatives such as IDS (International Data Spaces) or GAIA-X. Data models, APIs, and metadata standards must be specified so that datasets can be exchanged seamlessly and understood across organizational boundaries.

- Select infrastructure components (e.g. cloud stacks, connectors, security mechanisms)
- Define interoperability requirements

This phase addresses the **technical backbone of the ecosystem**. The team must decide which infrastructure to use (e.g. cloud stacks, sovereign cloud solutions), how connectors are built, and which security mechanisms are implemented. It also involves identifying interoperability requirements to guarantee that all components can interact in a standardized way. Security-by-design and modularity are critical here, as the architecture must remain adaptable to future technologies and standards.

Opportunities & Solutions / Migration Planning

- Develop a stepwise roadmap
- MVP (Minimum Viable Product)
- Pilot phase
- Scaling

Now the focus shifts to **roadmapping and implementation planning**. A stepwise approach is required: first build a Minimum Viable Product (MVP) to demonstrate the core concept, then extend to pilot deployments with real users, and finally scale up the ecosystem. Each step should be carefully planned with milestones, resource allocation, and risk assessment. This ensures that progress is measurable and that stakeholders stay committed.

Implementation Governance

The ecosystem's implementation must be **monitored and controlled** to ensure compliance with the defined architecture. This requires setting up governance structures, monitoring KPIs, and defining processes for decision-making during implementation. The team must also ensure that partners follow agreed standards and that deviations are documented and addressed. Without strong governance, the ecosystem risks fragmentation or non-compliance.

Architecture Change Management

- Adapt to new requirements and standards

Finally, the ecosystem must be able to **adapt to new requirements**. This includes updating architecture elements in response to changing standards, regulations (e.g. EU Data Governance Act), or stakeholder needs. A feedback loop should be established to continuously collect input from users and partners and to translate it into architectural adjustments. This guarantees long-term sustainability and relevance of the ecosystem.

TOGAF ensures a structured and traceable path from Vision → Architecture → Implementation → Operations. It provides a governance model and clear phases that reduce risks and ensure alignment with partners and standards. [1]

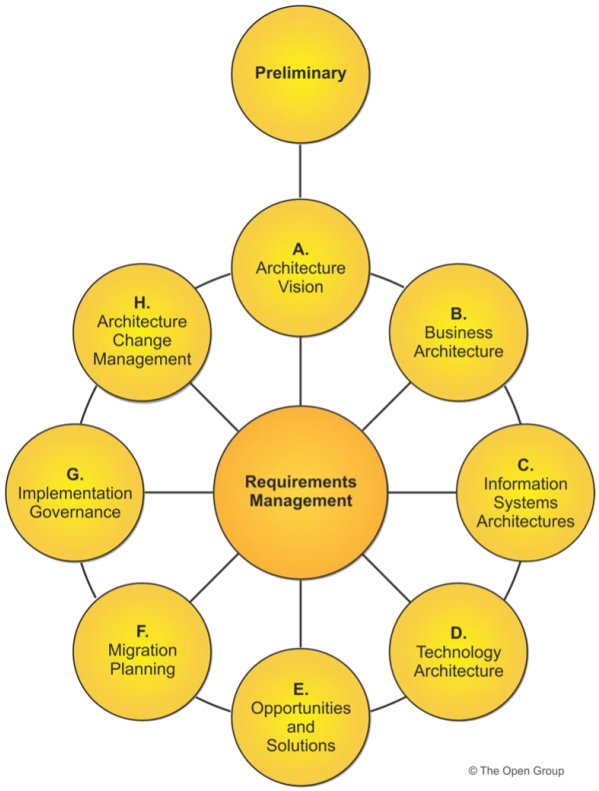

Figure 1: TOGAF Framework

1.1.2 Sitra Rulebook as a Governance and Ecosystem Building Block

The Sitra Rulebook is less about methodology and more about providing concrete content and governance rules that can be "fed into" the TOGAF phases. It acts as a catalog of content and guidelines to ensure that the architecture is not just technically sound but also fair, transparent, and legally compliant.

Governance Layer

- Guiding principles: Transparency, fairness, data sovereignty

Technology Architecture

- Decision-making mechanisms for the ecosystem

At this layer, one needs to establish the foundational rules of governance. The project team should define a clear set of principles that underpin the ecosystem - such as openness, fairness in data use, and respect for data sovereignty. In addition, transparent decision-making mechanisms must be agreed upon. This involves clarifying who has the authority to make ecosystem-wide decisions, how disputes will be resolved, and how accountability is ensured.

These governance rules will later feed directly into the **Preliminary Phase and Architecture Vision** of TOGAF.

Roles & Actors

- Core ecosystem roles: Data holders, data users, intermediaries, orchestrators
- Rights and obligations assigned to each role

Here, the focus is on defining the ecosystem's human and organizational roles. Each role must be clearly described, along with its responsibilities, rights, and obligations. For example, data holders need clear guidelines on how they must supply data and under what conditions. Data users should understand their usage rights and restrictions. Intermediaries should know their obligations regarding neutrality and transparency, while orchestrators must manage trust and compliance. This clarity will become part of the **Business Architecture phase in TOGAF**, ensuring that business processes are mapped to well-defined roles.

Legal & Contracts

- Templates for contracts between participants (e.g. data provision agreements, data use agreements)
- Reference to the EU Data Governance Act

The legal dimension requires the preparation of contract templates and legal frameworks that participants can use as the basis of collaboration. These templates should cover aspects like liability, data usage rights, responsibilities, and dispute resolution. Importantly, they must be aligned with European legislation such as the EU Data Governance Act to ensure compliance. This step gives the ecosystem legal certainty and builds trust among participants. These contents directly support the Implementation **Governance and Change Management phases** in TOGAF.

Business Layer

- Value creation models and incentive systems
- KPIs for impact measurement

In this layer, the team must define how value is generated and shared within the ecosystem. Possible models include pay-per-use data access, subscription models, or cooperative sharing agreements. Incentives must be designed to encourage active participation by both providers and users - for example, financial rewards, reputation benefits, or access to premium services. Furthermore, measurable KPIs must be set up to track the ecosystem's effectiveness, such as user growth, data transactions, or sustainability impacts. These elements feed directly into the **Business Architecture and Opportunities & Solutions** phases of TOGAF.

Operational Layer

- Processes for onboarding, data release, and security
- Technical requirements (e.g. connectors, authentication mechanisms)

At the operational level, concrete processes and workflows must be designed to keep the ecosystem functional. This includes creating onboarding procedures for new participants, defining the steps for data release and approval, and ensuring that robust security measures (authentication, encryption, monitoring) are in place. Additionally, the Rulebook requires defining the technical enablers of interoperability, such as standardized connectors and APIs. These aspects align closely with the **Information Systems, Technology Architecture, and Implementation Governance phases** of TOGAF.

The Sitra Rulebook acts as a content library for building a data ecosystem. While TOGAF provides the process methodology, the Rulebook supplies the substantive content: principles, roles, legal frameworks, business incentives, and operational processes. Together, they ensure that the DPP Data Ecosystem is not only technically structured but also governed fairly, legally compliant, and operationally sustainable. [2]

1.1.3 Combined Approach (TOGAF & Sitra Rulebook)

The project leverages a hybrid methodology by combining the strengths of TOGAF (as a structured, iterative framework for architecture development) with the Sitra Rulebook (as a repository of governance, contractual, and operational content). This combined approach supports that the ecosystem is developed in a methodical, transparent, and governance-compliant way.

Architecture Vision
Integrate the Sitra principles (transparency, fairness, data sovereignty) to shape the ecosystem vision and its governance model. This ensures that the long-term vision is not only technically sound but also anchored in trust and fairness.

Business Architecture
Adopt the roles and business models defined in the Sitra Rulebook as the foundation for mapping processes and value creation. This allows the ecosystem to build on tested role definitions (providers, users, intermediaries, orchestrators) and to establish clear incentive structures.

Data Architecture
Enhance the design with Sitra's contractual templates and usage rules. By embedding legal agreements and usage conditions directly into the data architecture, compliance and trustworthiness are ensured from the start.

Technology Architecture
Integrate Sitra's interoperability and security requirements into the technical blueprint. This guarantees that technical implementations are aligned with governance expectations and meet international standards.

Implementation
Apply the Rulebook as the operational toolkit for policies, contracts, and compliance. During implementation, the Rulebook provides ready-made content that accelerates rollout and ensures legal robustness.

The combined approach ensures that the methodological rigor of TOGAF is complemented by the practical governance content of Sitra. Together, they provide both the process and the substance needed to design and implement a robust, transparent, and scalable Data Ecosystem.

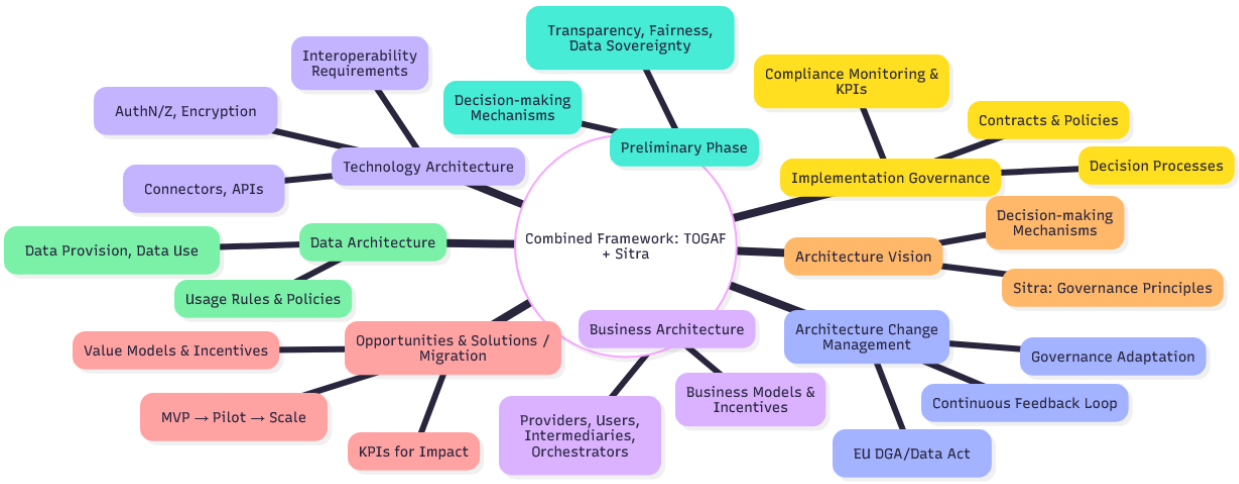

Figure 2: Combined approach TOGAF & Sitra

1.2 Technology Stack - Research

The following chapter discusses individual technology categories. Research was conducted on the topic of technology stacks that are considered state-of-the-art technologies in the context of the digital product passport.

1.2.1 Infrastructure and Technical Approaches

A fundamental architectural principle is the decentralization of identity and trust management based on W3C standards.

Decentralized Identifiers (DIDs) provide persistent, cryptographically verifiable, and interoperable identification of products, actors, and assets. They enable decentralized trust relationships and reduce dependence on central registries or authorities [3].

Verifiable Credentials (VCs) serve as standardized, portable, and trustworthy containers for claims and attestations. In Digital Product Passport (DPP) use cases, VCs can represent conformity declarations, sustainability indicators, or product-origin information. Their selective disclosure capabilities enable privacy-preserving and verifiable data sharing across organizational boundaries [3].

While the decentralized W3C approach forms the core, alternative infrastructures remain relevant for interoperability and legacy integration.

X.509-based Public Key Infrastructure (PKI) continues to play a crucial role in authenticating organizations, services, or devices through certificates and trusted certificate authorities [4].

GS1 Identifiers and EPCIS (Electronic Product Code Information Services) are well-established in industry, providing globally unique product and actor identifiers (e.g., GTIN, GLN, SSCC) and supporting event-based traceability along supply chains [5].

Cryptographic Primitives and Key Management
Trust and integrity in the DPP ecosystem are ensured through well-defined cryptographic primitives. Core design decisions involve the choice between symmetric and asymmetric cryptography, depending on use cases such as signing, encryption, or secure channel establishment. Supported key types and curves - for example, P-256, secp256k1, and Ed25519 - are selected based on interoperability requirements, performance characteristics, and regulatory alignment. Private key management mechanisms, including secure elements, hardware security modules (HSMs), and delegation frameworks, ensure secure handling of cryptographic material. Compatibility with signature and proof formats such as JWS, Linked Data Proofs, or COSE guarantees seamless integration into both web-native and IoT contexts [6].

IEC Standards as the Basis for the Digital Product Passport (DPP) 4.0
The Digital Product Passport (DPP) is gaining momentum, with initiatives like DPP for Machinery highlighting its importance. To ensure success and widespread adoption, internationally recognized standards are essential. These standards guarantee uniformity in data models and data provision.

Role of IEC Standards
The International Electrotechnical Commission (IEC) provides the technical foundation for the DPP through two key standards:

IEC 63278 – Asset Administration Shell (AAS)
- Defines the structure, metamodel, and interfaces for the digital representation of physical assets. (in detail in part 2 of the IEC)
- Provides a standardized, extensible data structure
- Ensures secure, interoperable information exchange across companies
- Covers the entire product lifecycle
- Enables seamless integration with IT and OT systems

IEC 61406 – Digital Nameplate (DNP 4.0)
- Establishes a unique Identification Link for assets, ensuring reliable access to product information.
- Identification via QR, NFC, or RFID
- Direct access to documentation, certificates, and sustainability data
- Connection to the AAS for a complete digital representation
- Real-time data availability for manufacturers, integrators, and users

Benefits of IEC Standards for the DPP
Together, IEC 63278 and IEC 61406 ensure a standardized, globally applicable approach to product data management. Key advantages include:

- Regulatory compliance – supports EU sustainability regulations (ESPR)
- Standardized, machine-readable product information – drives efficiency
- Interoperability – product data usable across manufacturers
- Global applicability – supports international supply chains
- Digital transformation – reduces paper documentation and enables automation

IEC 61406 - Digital Nameplate / Identification Link (IL) covers:

- Part 1 (IEC 61406-1:2022): Minimum requirements for a globally unique identification of a physical object that also acts as a link to related digital information - the Identification Link (IL). The encoded data is an "IL string" with the data-format of a URL; it is carried on the product via a 2D symbol (e.g., QR/Data Matrix) or NFC tag. Applies to individually delivered objects that already have a unique identity assigned by the manufacturer.
- Part 2 (IEC 61406-2:2024): Adds structured IL strings (standardized syntax & semantics) and clarifies uniqueness at type/model, lot/batch, and individual item levels [7].

Draft Implementation checklist for DPP:

Table 1: Draft implementation checklist digital nameplate

Area	What to implement for DPP	Form / Constraints (from IEC)
Identifier on the product	Place an IL carrier on each DPP-relevant product	2D code or NFC tag on the physical object; must be machine-readable.
IL string format	Encode the product's IL string in the carrier	URL-formatted IL string (typically https); global uniqueness required.
Space-saving & comparison rule	Optimize IL string for small codes and consistent matching	Public registry mirrors the spec: you may omit https:// in the code; when comparing IL strings, strip any leading https://. *(The normative rules are in IEC 61406-2 Annex F; the public IANA text reflects them.)*
Link target (resolver)	Make the IL resolve to current digital information	The standard's purpose is that the IL links to digital info (docs, certificates, sustainability data, etc.). Ensure resolver uptime and appropriate audience views.
Structured IL (optional but recommended)	If you need to encode type/lot/item inside the IL string	Follow IEC 61406-2 structured IL syntax & semantics; pick the correct granularity (type / lot / item).
Scope boundaries	Don't over-constrain your physical nameplate	IEC 61406-1 does not dictate layout/text of traditional nameplates; focus on the identification link itself.

IEC 63278-1 - Asset Administration Shell (AAS) structure covers:

IEC 63278-1:2023 / EN IEC 63278-1:2024 defines the structure of a standardized digital representation of an asset, called the Asset Administration Shell (AAS), providing uniform access to information and services across the asset lifecycle. Part 1 establishes the general structure requirements every AAS must comply with; later parts of the IEC series will add the information metamodel, interfaces/APIs, mappings (e.g., OPC UA, AutomationML), and security details [8].

Draft Implementation checklist for DPP:

Table 2: Draft implementation AAS

Area	What to implement for DPP	Form / Constraints (from IEC 63278-1 and companion IDTA specs)
AAS presence	Provide an AAS for each DPP-covered asset (product, component, system)	Part 1 mandates a standard AAS structure with uniform access to information/services (cross-enterprise use).
AAS structure (high-level)	Structure the digital representation into AAS Submodels → SubmodelElements with semantic anchoring	Part 1 sets general structure requirements; for concrete classes/attributes/constraints use I DAT-1001(Metamodel) (AAS, Submodel, Property, Operation, File, Blob, RelationshipElement, ConceptDescription, etc.) and its normative JSON/XML/RDF schemas.
Semantic identifiers	Attach semantic IDs to properties/elements	Use ConceptDescriptions and (where relevant) IEC 61360 data specs (IDTA Part 3a) to ensure machine-interpretable meaning.
Interfaces / APIs	Expose AAS & Submodels via standard APIs	IEC series plans interface parts; implement IDTA-01002: HTTP/REST API with service specifications, profiles, and normative OpenAPI documents (Registry, Repository, Submodel, Discovery, ConceptDescription).
Discovery & registries	Support finding AASs & Submodels across a landscape	Implement AAS Registry and Submodel Registry/Repository endpoints per IDTA profiles to enable cross-party discovery and lookup.
Serialization	Choose JSON/XML/RDF representations	Use the normative schemas from IDTA-01001 for interoperability; they are derived from the metamodel.
Mappings to other stacks	Plan for OPC UA companion mapping where needed	There is an official OPC UA companion mapping for AAS; align if your OT/SCADA layer is OPC UA-centric.
Security	Align AAS services with industrial security	IEC Part 1 is structural; security mechanisms are specified in IDTA-01004 (Security) - apply when exposing AAS over networks.

Trust Identity and Data Governance:

Self-Sovereign and Federated Identity Models:
A Self-Sovereign Identity (SSI) approach enables entities to manage their authentication and authorization processes without relying on centralized identity providers. SSI aligns with the principles of data sovereignty, transparency, and user control. Alternatively, government-backed identities, such as ID Austria (provided by A-Trust), offer legally recognized credentials that can be integrated for trust assurance in regulated environments. Comparable mechanisms exist across Europe (e.g., eIDAS 2.0 wallets in Germany and other Member States) [9].

Authentication and Authorization Mechanisms:
Authentication mechanisms may rely on public-key infrastructures (PKI) or decentralized protocols such as OpenID for Verifiable Credentials (OID4VC). Access control policies can be implemented through various paradigms, including Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and Credential-Based Access Control (CBAC). Dynamic delegation and revocation capabilities are essential for managing trust relationships and ensuring adaptive access in federated ecosystems [10].

Data Governance and Usage Control:
Data governance within the DPP ecosystem is based on explicit consent and enforceable usage policies. Standards such as ODRL (Open Digital Rights Language), DPV (Data Privacy Vocabulary), and ALC (Access and License Control) provide mechanisms to express, exchange, and enforce usage constraints. Auditability and provenance tracking ensure full transparency across the data lifecycle, enabling stakeholders to verify when and how data was accessed or modified. This supports accountability, trust, and regulatory compliance [11].

Data Model and Semantics:
The core DPP data model builds upon European Commission initiatives such as CIRPASS and ESPR, ensuring alignment with regulatory and interoperability requirements. Extensible model design allows integration of sector-specific and cross-sectoral attributes relevant to sustainability, circularity, and compliance. Semantic interoperability is achieved through established ontologies and Linked Data vocabularies - such as Schema.org, ECLASS, and Product Ontology - enabling machine-readable and harmonized data exchange. Versioning and lifecycle management mechanisms track product information across updates, ownership changes, and multi-stakeholder collaboration over time [12].

Interoperability and Data Exchange:
Interoperability is facilitated through standardized APIs and protocols, including NGSI-LD, DCAT-AP, EPCIS 2.0, W3C DIDComm, and Gaia-X interfaces. Data is represented in JSON-LD, ensuring both structural and semantic clarity while maintaining compatibility with linked data ecosystems. Semantic Containers or similar encapsulation mechanisms are used for packaging DPP data together with policies, metadata, and provenance information, supporting portability and controlled sharing [13].

Trust Infrastructure:
Trust assurance mechanisms include digital signatures and integrity proofs to guarantee authenticity and tamper-evidence. Cryptographic timestamping and anchoring in distributed ledgers (e.g., blockchain) enhance traceability and verifiability of DPP-related transactions and attestations across organizational boundaries.

Deployment and Scalability Requirements:
Deployment strategies must balance edge and cloud capabilities. Lightweight components are required for constrained edge devices such as IoT sensors and smart meters, while scalable cloud services support validation, aggregation, and registry functions. The architecture emphasizes resilience, redundancy, and fault tolerance, ensuring continuous operation in multi-stakeholder, distributed ecosystems.

Compliance and Legal Alignment:
Compliance with European frameworks, particularly the GDPR and Data Governance Act (DGA), is a foundational requirement. The infrastructure must provide clear mechanisms for lawful data processing, data subject consent management, and cross-border data sharing in compliance with EU data sovereignty principles [14].

Furthermore, interfaces with notified bodies and market surveillance authorities enable automated reporting, certification, and policy updates, ensuring continuous regulatory alignment.

1.2.2 Quality Attribute Scenarios (QAS)

Quality Attribute Scenarios offer a rigorously structured way of expressing non-functional requirements. Instead of stating that a product "must be scalable" or that a gateway "should be interoperable", a scenario pinpoints who or what triggers an event, under which circumstances the event occurs, which part of the system is stressed, how the system is expected to react and how success will be measured. The idea originated at the Carnegie Mellon Software Engineering Institute in the late 90s and was quickly embedded in the Architecture Trade-off Analysis Method (ATAM) and the Quality Attribute Workshop (QAW). Since then, the technique has become widely used in industry: defence programmes have used scenario-driven evaluations in several major U.S. Government procurements, while ATAM itself has been applied to more than twenty industrial systems ranging from avionics to banking platforms.

Large-scale commercial players follow the same recipe. Netflix, for example, subjects its micro-service mesh to an internal variant of QAW whenever a new reliability or latency target is debated, while European telcos employ scenario templates to decide whether a 5G core upgrade can be rolled out without breaking existing integrations. What makes the approach attractive in such disparate settings is its diplomacy: by requiring relevant stakeholders such as architects, operations staff, domain experts and business owners to sit together in a moderated workshop, hidden assumptions come up early and the associated costs can be calculated before any code is written. The QAW guidance prescribes that participants first brainstorm dozens of scenarios, then consolidate, vote and finally refine the top candidates into "test-ready" descriptions. This disciplined elicitation step has proven valuable whenever a project must reconcile competing quality drivers like performance versus security, integrability versus time-to-market, etc.
Once agreed, scenarios drive the whole life-cycle. Architects select tactics that can demonstrably satisfy the specified response measure, developers turn the same measure into automated acceptance tests and operations teams convert it into dashboards and alarms. Auditors later verify compliance against the identical yard-stick. Because each scenario is written in technology-agnostic language, the contract remains stable even when a subsystem is replaced, migrated to the cloud or handed over to a different vendor [15].

1.3 A textbook example

To illustrate the quality attribute scenario format, consider a performance scenario that appears verbatim in training material of the Carnegie Mellon university:

> *A remote user requests a database report via the web interface during the system's peak-hour load. The report is delivered within five seconds.* (insights.sei.cmu.edu)

Even in a single sentence the essential ingredients are visible: the source (remote user), the stimulus (report request), the environment (peak load), the affected artifact (web interface - report generator path), the expected response (report returned) and the quantitative response measure (≤ 5 s). Because every element is explicit, architects can immediately ask whether caching, additional hardware or query optimisation is the right tactic - and testers can build a load-test that issues exactly this request profile.

1.3.1 The six components of a Quality Attribute Scenario

- **Source of stimulus:** Identifies the actor: a human, a system or natural phenomenon. Important to describe so that trust boundaries, contractual obligations and legal constraints become clear. When the source is an external partner organisation, e.g., interface versioning and liability clauses frequently shape the architectural response.
- **Stimulus:** Defines precisely what happens. Precise wording avoids the trap of designing for the wrong event class. For instance, distinguishing between *adding* a module, *upgrading* it, or *wiring two existing modules together* leads to very different integration mechanisms.
- **Environment:** Describes the operational state at the moment the stimulus arrives: e.g., normal service, degraded mode, maintenance window, cyber attack, etc. The same failure at midnight may have a very different tolerance than during a Black-Friday rush.
- **Artifact:** Names the part of the system directly affected. Granularity matters: if only a message broker is touched, encapsulation tactics differ from those used when the entire data-pipeline is at stake.
- **Response:** States the desired behaviour without dictating implementation. This frees designers to choose, say, a pub-sub backbone or an API gateway, as long as the behaviour, e.g. continued message routing without loss, is achieved.
- **Response measure:** Provides the quantitative pass / fail criterion: time, throughput, effort, cost, defect rate, percentage compliance with a standard, and similar metrics. This is the most important aspect of a quality attribute scenario when it comes to the evaluation of a chosen architecture as it quantifies, if its implementation has been successful [16].

1.3.2 Standards-compliant gateway for DPP

The Digital Product Passport (DPP) ecosystem involves dozens of stakeholders scattered across large supply chains. Efficient, low-friction data exchange is therefore necessary, and we expect that future participants as well as regulatory bodies insist on compliance with the forthcoming standards, which are defined by CEN/CENELEC. The following scenario captures this integrability challenge:

- **Source of stimulus:** A new SME supplier in the electronics sector joins the DPP ecosystem and requests to connect its existing ERP system.

- **Stimulus:** The supplier submits a formal onboarding ticket that includes its endpoint URL and a valid CEN/CENELEC draft-compliant schema declaration.
- **Environment:** The platform is in normal operation, processing ≤ 10 000 document exchanges per hour.
- **Artifact:** The DPP integration gateway (API and partner registry)
- **Response:** The gateway generates an adapter configuration, validates sample payloads, registers the partner and enables bi-directional data exchange without manual code changes.
- **Response measure:** End-to-end onboarding is completed within 10 calendar days and consumes no more than one person-week of engineering effort. Payloads must pass syntactic and semantic validation against the standards as defined by CEN/CENELEC.

1.3.3 Federated onboarding with Decentralized Identifiers (DIDs)

In a federated, open ecosystem, new stakeholders should be able to join quickly without bespoke integration work, while preserving high assurance about who they are and what roles they hold. Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) enable self-managed identities and role attestations that can be verified across organizational boundaries. The following scenario focuses on fast, low-touch onboarding with robust verification and auditable outcomes.

- **Source of stimulus:** A prospective participant (e.g., an SME supplier) that has established a DID for its legal entity.
- **Stimulus:** The participant initiates onboarding by registering its DID before requesting access to publish and consume DPP-related data.
- **Environment:** Normal platform operations with identity services online (DID resolution, issuer trust list, revocation/status), including periods of increased demand (onboarding waves).
- **Artifact:** The identity and access layer: trust framework (issuer registry, policies), VC verifier and status checking, onboarding workflow, partner registry.
- **Response:** The platform resolves the DID document, verifies it, evaluates policy for the requested roles/scopes, provisions access (client credentials, policies), registers the participant, and produces an immutable audit trail.
- **Response measure:** End-to-end onboarding completed within 2 business days with ≤ 1 person-day of effort; ≥ 90% of cases fully automated (no human intervention). 100% of onboarding events are auditable (tamper-evident log with participant DID, issuer DIDs, timestamps).

1.3.4 Wood Use Case Scenario considerations (text book example):

EUDR due-diligence data intake and validation (Compliance & Integrability)
For wood products, the EUDR requires plot-level geolocation, an electronic due-diligence statement (DDS) reference, and risk assessment/mitigation before placing products on the EU market. Our platform must be able to accept, validate, and link these data to the DPP efficiently and at scale, while providing clear feedback for remediation.

- **Source of stimulus:** A manufacturer submits EUDR due-diligence data (including geolocation and DDS reference) which has been used in a wood product that requires a DPP for placement on the EU market.
- **Stimulus:** A payload containing plot-level coordinates, harvest dates, risk assessment artefacts, and the DDS reference number is uploaded for validation and linkage to the product's DPP.
- **Environment:** Normal operations, mixed data quality from multiple upstream systems.
- **Artifact:** EUDR intake and validation service (schema/semantic/geospatial validators), DDS reference resolver, mapping engine to DPP, error reporting subsystem.
- **Response:** The system validates schema and semantics (including coordinate precision and polygon geometry rules), checks DDS reference availability, evaluates the presence of required risk assessment fields, and either accepts and links the record to the DPP or rejects with precise diagnostics (field-level error locations, codes, suggested fixes). Accepted records become queryable and auditable.
- **Response measure:** Validation decision (accept/reject with full diagnostics) returned within 1 minute. Error messages pinpoint the offending field/segment in 100% of rejections. The system sustains ≥ 5 000 submissions/hour during peak windows with no loss or duplication.

1.4 Approaches and Outputs from other works

1.4.1 CIRPASS – Ontology and System Architecture for the Digital Product Passport (DPP)

The EU-funded project CIRPASS (Digital Product Passport Architecture) aims to define the conceptual and technical foundations for the future Digital Product Passport (DPP). One of the key outcomes is the design of a two-layer ontology model that addresses both the cross-sectoral requirements of European legislation and the domain-specific needs of individual product categories.

The first layer is a generic "DPP system ontology", serving as a common foundation for all product groups. It includes basic classes such as Product, Material, Certificate, or Economic Operator.

The second layer consists of domain-specific ontologies, tailored to the concrete requirements of sectors such as textiles, electronics, batteries, or construction materials. These ontologies are derived from delegated acts under the ESPR Regulation (Ecodesign for Sustainable Products Regulation).

Mappings and transformations are foreseen between these two layers, allowing existing data models to be aligned with the DPP. This results in a flexible and extensible architecture, enabling interoperability between different industries, systems, and data sources.

Access Architectures: HTTP-URI and Decentralized Identifiers (DID)

A core feature of the CIRPASS architecture is the support for two parallel access mechanisms for retrieving DPP data:

- **HTTP-URIs**, based for example on the GS1 Digital Link standard. This approach is easy to implement and compatible with existing technologies such as QR codes or DataMatrix codes already used in retail and logistics
- **Decentralized Identifiers (DIDs)**, a modern, self-sovereign identity approach. DIDs enable trustworthy, interoperable links to product-related data and support decentralized, controlled access to sensitive information

Both mechanisms ultimately resolve a unique product identifier (UID), which is linked - via a so-called resolver - to the corresponding DPP Data Repository (DDR). This data repository is managed by the Responsible Economic Operator (REO), i.e. the manufacturer or entity placing the product on the market.

Technical Architecture – Overview of Components

The implementation of a DPP according to CIRPASS follows a standardized workflow, typically consisting of five technical steps:

1. **Assembling & Issuing**
   Product-related data is extracted from internal systems such as ERP, LCA tools, or PLM solutions, transformed (e.g., into JSON-LD), and stored as a knowledge graph in the REO's own data repository.

2. **Data Quality & Compliance**
   The resulting DPP data is validated using SHACL shapes, which are rule-based mechanisms to check structure and completeness. This ensures that all mandatory fields are correctly populated.

3. **Access Control**
   Controlled data publishing is handled through ODRL policies (Open Digital Rights Language). A Policy Decision Point (PDP) decides whether an external request (e.g., from a repair service) has a legitimate interest to access specific data.

4. **Registry Linkage**
   To enable regulatory oversight, a minimum set of metadata - such as product ID, REO ID, or production site - is reported to a central EU registry.

5. **Resolver & Typed Links**
   The resolver supports typed links (e.g., type=DPP, type=Certificate, type=RepairInstructions) to enable different stakeholders - such as consumers, authorities, or service providers - to access context-specific views of the same product instance.

Compass usage of Ontologies

Choosing an ontology-based architecture instead of static data models offers multiple advantages:

- **Modularity & Reusability**
  Ontologies can be extended, reused, or combined more easily than rigid schemas. They offer flexibility for future updates and allow mappings to legacy systems
- **Interoperability & Machine Readability**
  Ontologies provide the foundation for automated data linking, querying, and reasoning. This transforms DPPs from mere data containers into active digital resources – usable in dashboards, lifecycle assessments, or data marketplaces
- **Governance & Scalability**
  Standardized validation rules (e.g. SHACL) and a clean separation between core and domain ontologies allow for scalable governance models and centralized quality control [17]

1.4.2 CIRPASS-2 – Specification of the DPP Core Ontology

In the successor project CIRPASS-2, a first version of the Ontology Requirements Specification (ORS) was published in 2025. This document defines:

- the scope and purpose of a future EU-wide DPP core ontology
- supported representation languages (e.g., RDF/OWL, SHACL)
- prioritized use cases
- a set of competency questions - i.e. example questions the ontology must be able to answer
- and validation criteria for implementation

The ORS acts as a design foundation for a harmonized EU DPP core model, which can later be extended by sectoral or national initiatives.

Another important output from CIRPASS-2 is the collection and analysis of existing ontologies and classifications across relevant domains such as electronics, textiles, tires, and construction, which can serve as building blocks for the domain layer [18].

1.4.3 The DPP Vocabulary Hub

To support implementation, the DPP Vocabulary was created as an open, collaborative platform. It allows developers and projects to publish, browse, and reuse ontologies and data models for DPP applications.

Key features include:

- access to the initial DPP core ontology modules (e.g. *Product & DPP*, *Actors & Roles*, *Substances of Concern*)
- integration of controlled vocabularies and code lists (e.g. for material types or recycling categories)
- export of validation artifacts (e.g. SHACL shapes)
- and a search function for discovering existing assets

The hub enables projects to avoid duplicating efforts, accelerate development, and contribute their own extensions back to the community [19].

1.4.4 Implications for PACE-DPP

For the PACE-DPP project, other project results provide a clear technical orientation framework that can be directly applied to guide system design and implementation.

Define the Model Architecture

It is recommended to adopt the layered model structure (e.g. proposed by CIRPASS):

- **Upper Layer**: The EU DPP core ontology, as defined in the Ontology Requirements Specification (ORS) and published through the DPP Vocabulary Hub
- Lower Layer: Domain-specific ontologies tailored to the relevant product groups and derived from delegated acts or established sectoral vocabularies

Set Up the Technology Stack & Data Pipeline

- **Ingest product data** from internal sources such as ERP or LCA tools
- **Transform** the data into **Linked Data** (preferably using **JSON-LD**)
- **Validate** the data using **SHACL shapes** to ensure structure and completeness
- **Store** the resulting knowledge graph in a **DPP Data Repository**
- **Integrate** the system with a **resolver infrastructure** (e.g., HTTP-URI or DID-based)

Define the Access Control Model

- Establish **ODRL policy templates** to control access to specific data elements
- Use **role- and attribute-based access control** (e.g., for repair shops, regulatory authorities)
- Plan for **future integration** with **eIDAS 2.0** and **SSI-based** credential management

Prepare for EU Registry Integration

- Develop a **metadata export concept** to submit mandatory references (e.g., UID, REO-ID) to a future **EU-wide registry** for regulatory discoverability

Promote Reuse and Interoperability

- Actively **reuse assets** from the **DPP Vocabulary Hub** to avoid duplication and ensure alignment with the European DPP ecosystem

- **Publish project-specific extensions** (e.g., domain ontologies or shapes developed within PACE-DPP) back to the community to contribute to the evolving standard landscape

1.5 Regulatory Requirements and Standards

For the full legal analysis, datasets and methodological details, please consult Deliverable 2.2, Work Package 2. The following is a high-level overview:

1.5.1 ESPR

The ESPR provides the overarching legal foundation for the DPP as a digital mechanism for ensuring transparency, traceability, and sustainability across product life cycles.

Key Requirements Derived from the Regulation

The ESPR requires comprehensive data collection through the DPP. The passport must digitally record a complete and structured dataset encompassing basic product and corporate information, technical performance metrics, real-use data, and end-of-life parameters. This integrated data infrastructure enables full lifecycle transparency and supports scientifically grounded sustainability assessments.

In addition, product data must be organized according to a granular and hierarchical information structure, capturing information at the model, batch, and individual item levels. Such a tiered system allows for precise traceability, monitoring, and targeted design improvements, while enabling data-driven circularity and resource efficiency strategies.

The Regulation further prescribes differentiated access rights, requiring that the DPP system ensures stakeholder-specific access. Regulators, consumers, and repair operators must receive only the information relevant to their respective functions. This tiered access system promotes transparency while safeguarding data confidentiality and market competitiveness.

Finally, the ESPR underscores transparency and continuous improvement as guiding principles. Standardized data acquisition and harmonized reporting procedures across the DPP infrastructure enhance accountability and comparability of sustainability performance. These provisions directly support the objectives of the EU Green Deal and the transition towards a circular economy by fostering ongoing environmental impact reduction throughout product lifecycles.

Obligations of Economic Operators

Under Articles 27 to 35 of the ESPR, specific obligations apply to different economic actors within the value chain.

Manufacturers must ensure that all products are designed and produced in compliance with the relevant ecodesign requirements. Products must be accompanied by the appropriate documentation and, where applicable, a DPP and CE marking. Manufacturers are required to conduct conformity assessments, maintain technical documentation and EU Declarations of Conformity for at least ten years, and guarantee continued compliance after design modifications. They must also ensure product identification, provide digital user instructions and safety information in the relevant national language (offering paper copies upon request), and implement corrective measures such as product withdrawal or recall in cases of non-compliance. Cooperation with authorities is mandatory, including the submission of documentation within fifteen days of a substantiated request.

Authorised Representatives may be appointed through a written mandate but cannot assume responsibility for design or production compliance. Their core obligations include retaining the EU Declaration of Conformity and technical documentation for ten years, cooperating with authorities during corrective measures, and terminating their mandate if the manufacturer violates ESPR requirements.

Importers may only place products on the EU market that fully comply with delegated ecodesign acts. Prior to market entry, they must verify that the manufacturer has conducted the conformity assessment, affixed the CE marking, and provided the required information, including the DPP and its backup copy. Importers must

provide contact details, ensure appropriate storage conditions, and refrain from distributing non-compliant products until conformity is re-established. They must maintain documentation for ten years, supply it to authorities within fifteen days upon request, and actively cooperate on corrective actions.

Distributors are obligated to exercise due diligence when making products available on the market. They must ensure that each product bears the required conformity markings, includes the necessary documentation, and is linked to a DPP where required. Distributor responsibilities include verifying manufacturer and importer details, refraining from distributing products suspected of non-compliance, and supporting corrective measures such as product withdrawal or recall. Furthermore, distributors must ensure that all DPPs, labels, and product information are accurate and easily accessible, including in online and distance-selling environments.

Fulfilment Service Providers must ensure that logistical processes - such as storage, packaging, and shipping - do not compromise product compliance with ecodesign requirements.

Providers of Online Marketplaces and Search Engines, as regulated under the Digital Services Act (Regulation (EU) 2022/2065), are required to cooperate with market surveillance authorities to prevent the online sale of non-compliant products. They must promptly remove or disable access to such content upon official request and establish a single point of contact for direct communication with authorities.

1.5.2 EUDR

The EU Deforestation Regulation (EUDR) establishes obligations for operators and traders placing relevant commodities - such as cattle, cocoa, coffee, palm oil, rubber, soy, and timber - on the EU market or exporting them. The regulation introduces binding due diligence, traceability, and reporting mechanisms to prevent deforestation and forest degradation associated with EU trade flows.

Core Obligations of Market Participants

Operators must perform comprehensive due diligence to ensure that all commodities are deforestation-free (i.e., not linked to deforestation occurring after 31 December 2020), legally produced under the laws of the country of origin, and accompanied by a due diligence statement prior to market placement.

This digital due diligence statement must be submitted through the EU information system and include identification of the operator, product description and HS code, country of production, geolocation data of the production plots, and a declaration confirming that the risk of non-compliance is negligible. Operators are required to retain these statements for at least five years and assume full legal responsibility for their accuracy. Commodities may only enter or leave the EU market once all three conditions - deforestation-free status, legal compliance, and a valid due diligence statement - are met.

1.5.3 Substantive Requirements for Compliance

Operators must conduct risk assessment and mitigation procedures, evaluating non-compliance risks based on geographic, environmental, and socio-legal criteria. These include the verification of land legality, forest governance, indigenous and community rights (including Free, Prior, and Informed Consent – FPIC), human rights, labor standards, and environmental safeguards. Where non-negligible risks are identified, operators are obligated to implement risk mitigation measures before marketing products.

The regulation also establishes strict traceability requirements, mandating the submission of geolocation data (latitude/longitude or polygons for areas exceeding 4 hectares) for all production sites. This ensures verifiable traceability across global supply chains.

All due diligence documentation must be maintained for regulatory audits and shared electronically through an interoperable EU customs – authority interface, facilitating consistent and efficient compliance verification across member states.

1.5.4 Obligations of Authorities and Enforcement

Member State authorities are responsible for implementing a risk-based control system to monitor compliance. This includes verifying due diligence statements, inspecting operators and traders, and enforcing corrective or preventive measures. Authorities are empowered to suspend market access, seize or withdraw products, and impose proportionate, dissuasive penalties for violations. Moreover, final enforcement actions must be made publicly available through the European Commission's transparency platform.

1.5.5 Relevant International Standards

The effective implementation of the DPP frameworks is underpinned by international standards that ensure methodological rigor, transparency, and comparability in sustainability data.

ISO 14040:2006 defines the fundamental framework for Life Cycle Assessment (LCA), encompassing goal and scope definition, inventory analysis, impact assessment, interpretation, and reporting. It ensures methodological consistency and transparency across environmental evaluations.

ISO 14044:2006 complements ISO 14040 by specifying detailed methodological and data quality criteria for conducting LCA, including temporal, geographical, and technological representativeness, precision, completeness, and reproducibility.

ISO 14067:2018 establishes standardized methodologies for quantifying and reporting product carbon footprints, enabling accurate and comparable greenhouse gas accounting across supply chains.

ISO 14025:2006 defines principles for Environmental Product Declarations (EPDs, Type III), ensuring the reliability and verifiability of life cycle-based environmental information for business-to-business and business-to-consumer communication.

Finally, the ISO 59000 family provides an emerging framework for circular economy implementation, setting shared principles and metrics for circularity assessment, business model innovation, and sustainable supply chain management.

1.5.6 Wood Use Case Scenario specific regulatory requirements:

Regulation (EU) 2023/1115 on Deforestation-Free Products (EUDR)

The EUDR entered into force on 29 June 2023 to ensure that wood and six other high-risk commodities placed on, or exported from, the EU market are both deforestation-free (no clearing after 31 December 2020) and legally produced.

Scope, Deadlines and Transitional Rules:

- Application dates – Large and medium operators/traders must comply from 30 December 2025; micro- and small-enterprises from 30 June 2026, following a one-year postponement adopted in December 2024
- Legacy timber – Wood harvested before 29 June 2023 remains subject to the outgoing EU Timber Regulation until 31 December 2027.

Core Operator Obligations for Wood Products:

- Geolocation at plot level – Six-decimal-place coordinates are mandatory; plots > 4 ha must be reported as polygons rather than single points
- Electronic due-diligence statement (DDS) – Before customs clearance, operators upload a DDS to the EUDR Information System and receive a reference number that must appear in the import/export declaration
- Risk assessment & mitigation – Operators evaluate 14 risk factors and implement mitigation where risk is not negligible. A Commission implementing act classifies supplier countries or regions as high, standard or low risk, enabling lighter checks for low-risk origins.

Ecodesign for Sustainable Products Regulation (ESPR)

Effective 18 July 2024, the ESPR is the horizontal framework for setting sustainability and information requirements for nearly all physical goods sold in the EU, replacing the 2009 Ecodesign Directive.

Key Regulatory Instruments:

- Ecodesign performance requirements – Future delegated acts may impose minimum thresholds for durability, energy and resource efficiency, recycled content, carbon footprint and the presence of substances hindering circularity
- Digital Product Passport (DPP) – Each regulated product will carry a unique, machine-readable passport containing composition, origin, repair and end-of-life data; customs authorities will be able to verify DPPs automatically at the border
- Ban on destroying unsold consumer goods – The ESPR outright prohibits the destruction of unsold textiles and footwear from 19 July 2026 for large enterprises, with potential extension to additional sectors (including furniture) via delegated acts
- Green Public Procurement leverage – Mandatory GPP criteria may be issued so public buyers favour the highest-performing products

Product Road-Map Relevant to Wood: The first ESPR & Energy-Labelling Working Plan (2025-2030), adopted on 16 April 2025, lists furniture among 11 priority groups - positioning wood-based articles as early candidates for DPP and ecodesign rules, with preparatory studies starting in 2025 and draft delegated acts expected before 2028.

Regulatory Convergence for the "Use Case Scenario Wood"

- Single source of provenance – Plot-level coordinates, harvest dates and DDS reference numbers collected under the EUDR can be embedded verbatim in the ESPR Digital Product Passport, eliminating duplicate data capture.
- Streamlined market surveillance – A customs officer scanning the DPP QR code will simultaneously see ESPR sustainability metrics and a live link to the EUDR DDS, allowing one-stop compliance checks.
- End-to-end circularity – EUDR tackles upstream forest impacts, while ESPR drives downstream product design, durability and recyclability; together they create a closed regulatory loop for responsibly sourced, circular wood products.

2 Data-Ecosystem Specification

The specification of a functional and trustworthy data ecosystem requires a systematic understanding of the technical, organizational, and governance components that enable secure, interoperable, and value-creating data exchange across the product life cycle. This chapter outlines the foundational work necessary to define such an ecosystem in the context of Digital Product Passports (DPPs) and circular-economy data spaces. It identifies the core specification domains - **Meta-Data Definition**, **Decentralised Identity and Access Management**, and **Data Intermediary & Governance Frameworks** - and articulates the steps needed to transform them into a coherent, operational architecture.

Furthermore, this chapter establishes an initial linkage to the rapid prototypes developed in 2025, situating them within these specification domains to illustrate how early practical implementations can inform, validate, and refine the conceptual foundations of the emerging data ecosystem.

Collectively, these components form the blueprint for a robust data-ecosystem specification. They provide the conceptual and technical foundations required to move from isolated prototypes toward an integrated, scalable, and future-proof ecosystem capable of supporting DPP implementation across industries. The following sections outline the necessary design principles, responsibilities, and mechanisms that will guide this transition.

2.1 Meta-Data Specification

This section outlines the key metadata elements and specification tasks required to describe products across their life cycle and to enable data-driven circular-economy applications.

- Define required metadata categories across the product life cycle (e.g. origin of materials, manufacturing data, maintenance instructions, recycling guidance)
- Specification of minimum and optional data attributes per product group as foreseen in delegated acts under the ESPR
- Outline metadata provenance and responsibilities (e.g. raw material producers vs. manufacturers vs. recyclers)
- Mechanisms for ensuring data quality, update cycles, and data validation
- Interoperability of metadata using standards and common vocabularies (e.g. URI-based product identifiers, BOM, LCA references)
- Metadata structuring principles to support circular economy metrics and durability indicators [20]

2.2 Decentralised Identity and Access Management

This section specifies the key identity, authentication, and access-control requirements needed to enable secure and trustworthy interactions within decentralised DPP infrastructures

- Link product identifiers to identity-based access rules (QR, RFID, NFC)
- Define access roles for public, business, and regulatory users
- Use decentralised identifiers (DIDs) and verifiable credentials to manage trust
- Manage lifecycle transitions: ownership changes, maintenance, recycling
- Ensure secure and privacy-preserving data access throughout the value chain

2.3 Data Intermediary and Governance

This section defines the governance requirements and intermediary functions necessary to facilitate fair, secure, and efficient data sharing within a DPP ecosystem

- Define the role of data intermediaries in coordinating actors and managing consent
- Apply principles from Sitra's Rulebook for a Fair Data Economy
- Ensure equitable distribution of responsibilities, rights, and benefits
- Align with data spaces and emerging EU infrastructures (e.g. DSSC)
- Include provisions for dispute resolution, contract templates, and compliance monitoring

2.4 Initial linkage to rapid prototypes (Use-Case-scenarios)

This section provides a concise overview of the rapid prototypes developed in 2025, with each use case scenario briefly summarised below; detailed descriptions and technical results are presented in the Results chapter.

2.4.1 Use Case Scenario Summary: Local DPP with did:peer

The Local DPP with did:peer use case scenario demonstrates a fully offline Digital Product Passport that uses a did:peer identifier embedded in a QR code to provide verified product information without requiring any external connectivity. A simple product - such as a light source - is equipped with a QR code encoding a unique, cryptographically verifiable identifier. When scanned, users can locally access essential information (manufacturer, production data, CO_2 footprint, compliance facts) directly on the device, even in the absence of a network connection. The prototype highlights the feasibility of compact, self-contained DIDs and shows how decentralized identifiers can serve as a stable reference mechanism for low-infrastructure DPP scenarios. This approach is particularly relevant for minimal-tech environments, long-lived products, and early-stage DPP deployments where offline accessibility and privacy-preserving verification are key.

2.4.2 Use Case Scenario Summary: Luminant

The Luminant use case scenario showcases an interoperable Digital Product Passport for a light source that integrates Asset Administration Shell (AAS) data, decentralized identifiers, and intermediary-hosted product information. A unique DPP identifier is linked to a DID and stored alongside structured AAS submodels, enabling verifiable and machine-readable product data across the value chain. The DID is bound to the physical device via an NFC chip, allowing role-based access through verification relationships: consumers access public product information, service technicians retrieve authenticated maintenance data, and regulators verify compliance and recycling evidence. The prototype demonstrates how industrial data models (AAS) and SSI concepts (DID, VC) can be combined to achieve transparent, trustworthy, and privacy-preserving DPP interactions throughout the product life cycle.

2.4.3 Use Case Scenario Summary: Improve Forest Owner Data Sharing

This use case scenario addresses the challenge of enabling small and decentralized forest owners to securely share verified sustainability and supply data with the wood industry. Through ID Austria authentication, Verifiable Credentials, and a neutral data intermediary, forest owners can digitally confirm their identity and submit structured operational data such as harvesting details or delivery information. All shared data is cryptographically verifiable and linked to authenticated sources, improving reliability for sustainability reporting, planning, and regulatory compliance. The data intermediary coordinates consent, ensures secure storage, and manages controlled access, following principles from Sitra's Fair Data Economy Rulebook. This prototype demonstrates how decentralised identity and VC-based trust can replace manual, error-prone data exchange processes within the Austrian forestry value chain.

2.4.4 Use Case Scenario Summary: Client-Managed Secret Mode (CMSM)

The Client-Managed Secret Mode use case scenario demonstrates a hardware-anchored Digital Product Passport in which the product itself generates and securely stores its private key inside an Infineon Secure Edge Node. All cryptographic operations - such as signing DID updates, issuing verifiable statements, or decrypting messages - are executed on-device, ensuring that the private key never leaves the hardware. The DID Document associated with the device exposes verification methods and role-based access policies, while Verifiable Credentials attest the identities of the manufacturer, component suppliers, and other trusted actors. This architecture enables secure provenance checks, authenticated messaging, and fine-grained access control across the value chain. The prototype shows how on-device keys, DIDs, and VCs form a tamper-resistant trust anchor for DPPs, supporting high-assurance scenarios and regulatory compliance.

		Local DPP with did:peer	Luminant	Improve Forest Owner Data Sharing	Client-Managed Secret Mode (CMSM)
Meta-Data Specification	minimum and optional data attributes per product group	⏳	⏳	✓	⏳
	required metadata categories across the product life cycle	⏳	⏳	⏳	⏳
	metadata provenance and responsibilities	⏳	⏳	✓	✓
	mechanisms for data quality, update cycles, and validation	⏳	✓	⏳	✓
	interoperability for metadata standards and vocabularies	✓	✓	⏳	⏳
	circular economy metrics and durability indicators	⏳	✓	⏳	⏳
Decentralised Identity & Access Management	link product identifiers to identity-based access rules	✓	✓	⏳	✓
	define access roles for public, business, and regulatory users	⏳	✓	⏳	✓
	decentralised identifiers and verifiable credentials	✓	✓	✓	✓
	lifecycle transitions: ownership changes, maintenance, recycling	⏳	✓	⏳	✓
	secure and privacy-preserving data access throughout the value chain	⏳	⏳	✓	✓
Data Intermediary and Governance	role of data intermediaries in coordinating actors and managing consent	⏳	✓	✓	✓
	principles from Sitra's Rulebook for a Fair Data Economy	⏳	⏳	⏳	⏳
	equitable distribution of responsibilities, rights, and benefits	⏳	⏳	⏳	✓
	align with data spaces and emerging EU infrastructures	⏳	⏳	⏳	⏳
	provisions for dispute resolution, contract templates, and compliance monitoring	⏳	⏳	⏳	⏳

Figure 3: Overview status use case scenarios

3 Development of the Data-Ecosystem

This chapter outlines the key activities required to design, build, and operationalise a comprehensive data ecosystem capable of supporting Digital Product Passports (DPPs) at scale. It brings together the architectural, methodological, and technological elements that organisations and stakeholders must consider when transitioning from isolated implementations toward coordinated, interoperable, and value-creating data infrastructures. By defining the necessary system layers, organisational processes, and integration frameworks, this chapter provides a blueprint for how a robust DPP-enabled data ecosystem can emerge across industries and value chains. The following sections elaborate the architectural principles, implementation pathways, and tool landscapes that collectively form the foundation for such an ecosystem.

3.1 Scalable Architecture

This section outlines the technical foundations and architectural principles required to build a scalable and interoperable Digital Product Passport (DPP) infrastructure. It identifies the key system layers, modular components, and integration patterns that enable DPP services to operate reliably across diverse product groups, organisational contexts, and technical environments. The focus is on establishing an architecture that ensures data protection and traceability, supports compliance with emerging regulations, and facilitates cross-stakeholder interoperability throughout the value chain:

- Describe layered architecture: data sources, transformation, access, and interfaces
- Support product-specific extensions via modular components
- Integrate various data carriers based on use cases and environments
- Ensure data protection, traceability, and standard compliance (e.g. ESPR)
- Foster interoperability across stakeholders and platforms

3.2 Implementation Methodology

This section presents a structured methodology to guide organisations in developing, operationalising, and scaling their DPP capabilities. It introduces maturity stages, assessment approaches, and organisational roles that help companies align internal processes, build competencies, and engage their value chain partners effectively. By combining methodological steps with iterative pilot activities, the section provides a pathway for organisations to transition from initial compliance-driven adoption toward strategic, data-driven value creation:

- Identify maturity levels: compliance, value chain integration, data-driven services
- Assess internal readiness and value chain engagement
- Define roles (e.g. DPP owner, data stewards) and align responsibilities
- Use pilots and experimentation to validate approaches and build capacity
- Plan long-term investments aligned with business opportunities

3.3 Tools, Platforms and Integration Concepts

This section introduces the technological tools, platforms, and integration concepts that support the creation, management, and exchange of DPP data across heterogeneous systems. It highlights how enterprise applications, data space technologies, semantic interfaces, and automation mechanisms can be combined to form an interoperable ecosystem for trusted product data flows. The focus lies on enabling reliable data provisioning, legal and semantic alignment, and integration with sustainability and reporting tools to support end-to-end DPP processes:

- Use enterprise systems (PLM, ERP, AAS, PIM, logistics) as data sources
- Implement APIs, semantic interfaces, and conversion services
- Leverage data space tools (DSSC) and legal frameworks (Rulebook)
- Enable automation via smart contracts and contract templates
- Integrate sustainability tools for reporting, verification, and optimisation

4 Results from 2025 and Outlook

In 2025, the research activities surrounding Digital Product Passports (DPPs) yielded a series of substantive advances, most notably the development of several rapid prototypes that provide initial empirical evidence for the feasibility and design of key technological components. These prototypes address three foundational domains that are widely recognized as prerequisites for interoperable, scalable, and trustworthy DPP infrastructures:

- **Meta-Data Specification**, examining how product-related information can be modelled, encoded, and exposed in a standardized, machine-readable manner suitable for both local retrieval and integration into data space architectures
- **Decentralised Identity and Access Management**, investigating the role of Decentralized Identifiers (DIDs), DID documents, and Verifiable Credentials in establishing secure, tamper-evident identities for products and actors, and in enabling verifiable interactions across distributed ecosystems
- **Data Intermediary and Governance**, exploring how neutral intermediaries can operationalize consent management, role definition, and policy enforcement in alignment with frameworks such as Sitra's Fair Data Economy Rulebook and emerging EU data governance requirements

The use case scenarios presented in the following sections - *Local DPP with did:peer*, *Luminant*, *Improve Forest Owner Data Sharing*, and *Client-Managed Secret Mode* - operationalize these research strands within distinct, practice-oriented contexts. Each prototype embodies a complementary perspective on how decentralized identity mechanisms, structured meta-data models, and governance functions may be implemented in a real-world DPP environment. Collectively, they offer an integrative, evidence-based foundation for understanding the technical, organisational, and regulatory considerations required for the emergence of robust and future-proof DPP ecosystems.

4.1 Use Case Scenario "Local DPP with did:peer"

Description:
The "Local DPP with did:peer" use case scenario demonstrates a fully local and offline implementation of a Digital Product Passport (DPP) using decentralized identifiers to ensure product authenticity and integrity without relying on external connectivity. In this first proof of concept, a simple physical product - such as a light source - is equipped with a QR code that encodes a unique, verifiable did:peer identifier. By scanning this QR code, users can locally access essential product information such as manufacturer details, production date, CO_2 footprint, or compliance data, even in the absence of an internet connection. No operational or dynamic data (e.g., usage hours or switching cycles) are yet included. This initial version serves as a foundational step toward a verifiable, privacy-preserving DPP architecture, focusing on minimal technical prerequisites, offline accessibility, and the use of decentralized identifiers as a robust and independent reference mechanism for future, more advanced DPP services.

Addressed topics and relevance:
- use decentralised identifiers (DIDs) and verifiable credentials to manage trust
  aspect: shows how did:peer enables local and verifiable product identification without any online dependencies
- link product identifiers to identity-based access rules (QR, RFID, NFC)
  aspect: did:peer identifier is represented as a QR code on the product

Sequence Diagram:
The sequence diagram below illustrates the interactions between the manufacturer, the light source, and the buyer in the Local DPP with did:peer Use Case Scenario. It shows how a decentralized identifier (DID) is created, linked to the product via a QR code, and later used by the buyer to locally access verified product information offline.

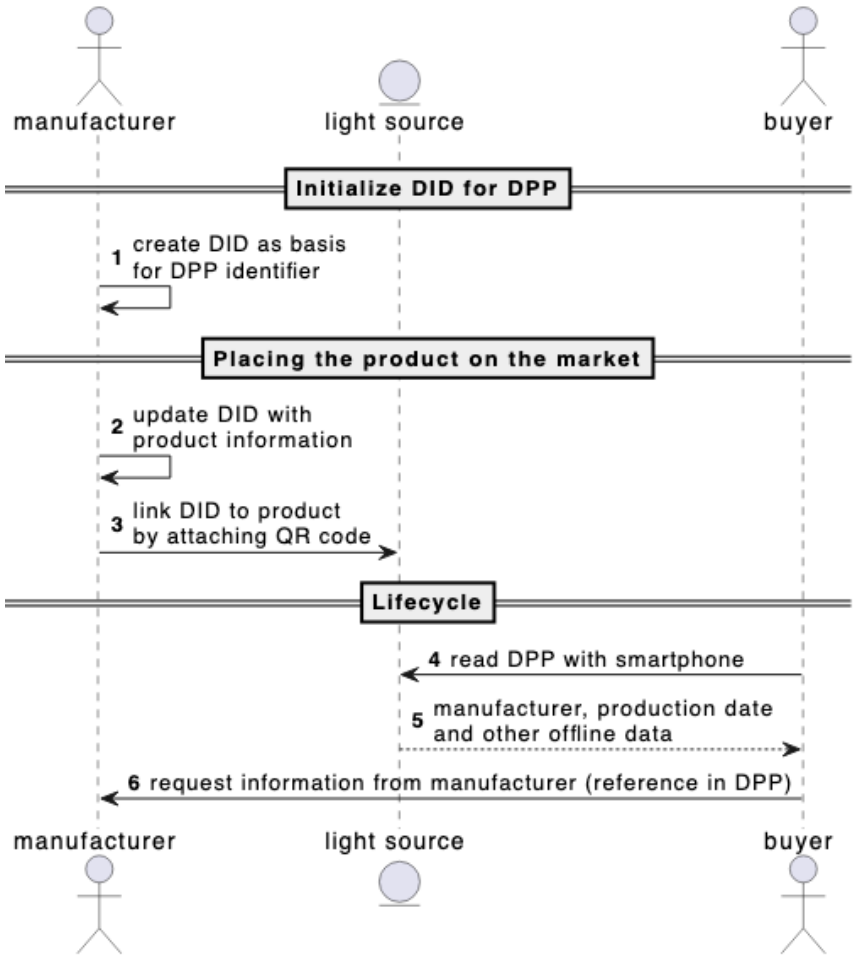

Figure 4: Sequence Diagram Local DPP with did:peer

The prototype demonstrates how the did:peer identifier can be directly embedded into a QR code, as shown at https://my-dpp.data-container.net/. Since most smartphones currently do not include a native DID resolver, it is more practical to encode a URL in the QR code that redirects to the corresponding DID resource - as demonstrated at https://my-dpp.data-container.net/link. This demo also illustrates that it is technically feasible to store up to approximately 800 bytes of information directly within the identifier itself, enabling compact, self-contained DIDs that can include references to additional resources such as an Asset Administration Shell (AAS) or related metadata.

4.2 Use Case Scenario "Luminant"

Description

The Luminant Use Case Scenario demonstrates how a Digital Product Passport (DPP) can be created for a light source by combining verified product data from an Asset Administration Shell (AAS) with publicly accessible information referenced in a Decentralized Identifier (DID) document and stored within a data intermediary. The prototype illustrates the integration of standardized, machine-readable product data with verifiable identity and access mechanisms, ensuring both transparency and data sovereignty. A central focus of this Use Case Scenario is the implementation of verification relationships within the DID document to define and manage access rights for different stakeholders - for example, enabling service technicians to retrieve authenticated operational or maintenance data while maintaining strict control over data visibility and provenance. Through this setup, the Luminant prototype showcases a trusted, interoperable framework for DPPs that bridges industrial data models (AAS) with self-sovereign identity principles (DID, VC) to support secure and role-based data access across the product lifecycle.

Addressed topics and relevance:

- link product identifiers to identity-based access rules (QR, RFID, NFC)
  aspect: an NFC chip attached to the light source links the product's unique identifier to identity-based access rules, enabling secure, role-specific data retrieval
- define access roles for public, business, and regulatory users
  aspect: demonstrated by defining distinct verification relationships in the DID document that grant tailored access to specific users
- use decentralised identifiers (DIDs) and verifiable credentials to manage trust
  aspect: using DIDs to uniquely represent the product and its stakeholders, while Verifiable Credentials (VCs) are used to authenticate product data and issuer identities
- ensure secure and privacy-preserving data access throughout the value chain
  aspect: demonstrated through using verification relationships within the DID to enforce role-based access control

Sequence Diagram

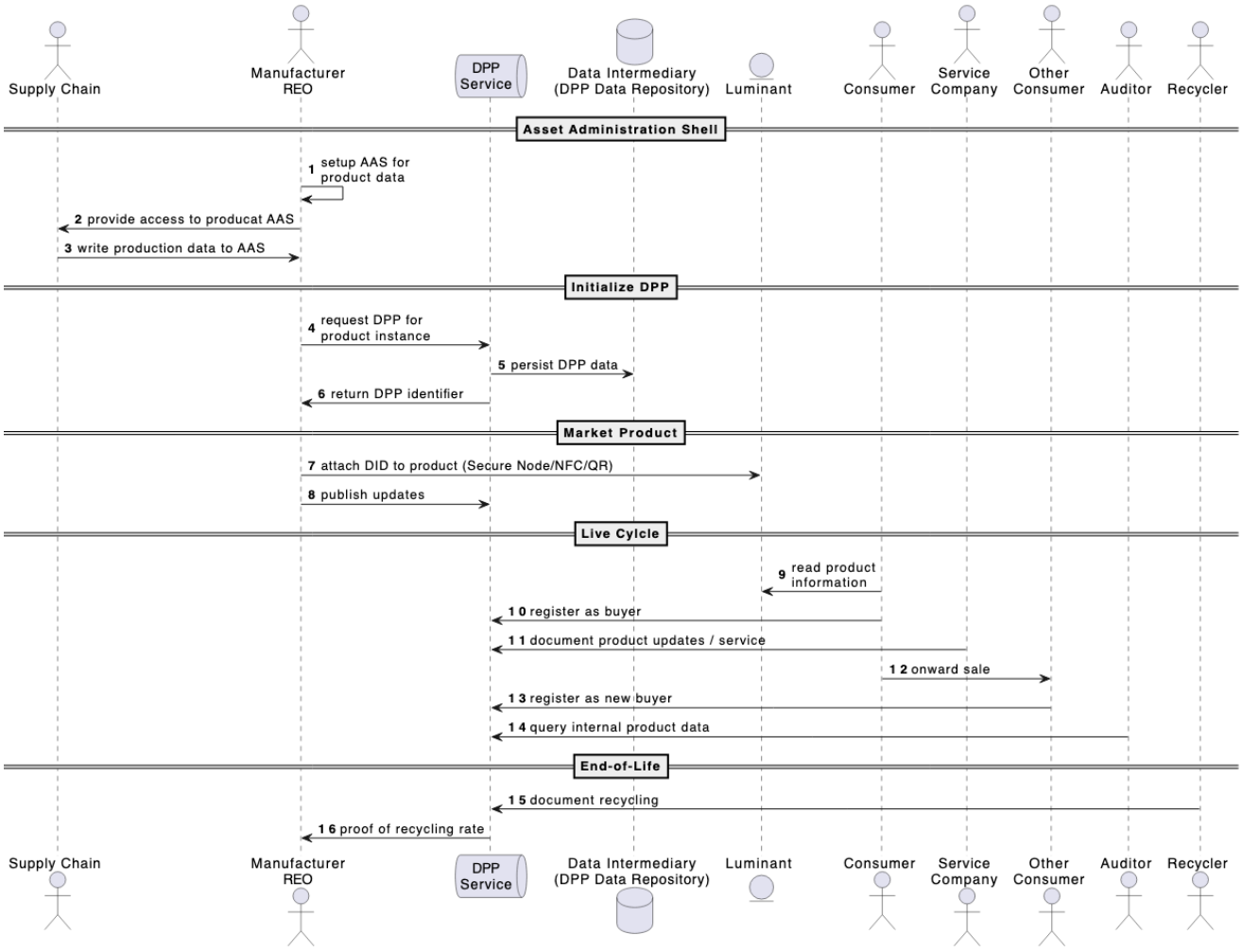

Figure 5: Sequence diagram Luminant

The sequence shows how the Luminant prototype creates and governs a Digital Product Passport (DPP) for a light source across all actors. The manufacturer/REO (Responsible Economic Operator) first sets up the product's Asset Administration Shell (AAS) and writes standardized submodels (e.g., technical specifications, environmental and compliance data). Additionally, supply chain actors can provide relevant data upon receiving write access.

- AAS hosted as BaSyx instance: https://basyx.data-container.net/ (deployment instructions: https://github.com/OwnYourData/basyx-k8s-demo)

A DPP service then issues a unique DPP identifier, links it to a Decentralized Identifier (DID), and registers resolvable references to public information as well as to protected AAS endpoints hosted by the data intermediary. The DID is bound to the physical device - the luminant - via an attached NFC chip, so that interaction with the product starts from its on-device identifier.

- DPP Service: https://dpp-service.ownyourdata.eu
  (source code available on https://github.com/OwnYourData/dpp-service)
- DID Trust Registry: https://oydid.ownyourdata.eu
- Data Intermediary: https://my.go-data.at

Downstream, the DID document becomes the hub for access and trust: it exposes minimal public facts (e.g., product type, manufacturer, CO_2 footprint) while also providing references for richer, role-restricted data originating in the AAS:

- Consumers can tap the NFC to read transparent product information and provenance;
- Service companies authenticate and, through DID verification relationships, are authorized to retrieve maintenance or operational data needed for diagnostics and repair;
- Auditors/regulators resolve the DID to verify compliance claims and recycling evidence; and
- An other consumer in a resale scenario can check authenticity and selected lifecycle records without accessing business-confidential details.

Throughout these interactions, DIDs provide globally unique, portable identifiers for the product and stakeholders, while Verifiable Credentials (VCs) attest to issuer identity and the integrity of shared data. By enforcing the verification relationships defined in the DID, the system links the product identifier (via NFC) to identity-based access rules, cleanly separates public, business, and regulatory views, and ensures secure, privacy-preserving data access along the entire value chain.

4.3 Use Case Scenario "Improve Forest Owner Data Sharing"

Description
This Use Case Scenario addresses the challenge of improving data exchange and transparency between forest owners and the wood industry. The goal is to enable forest owners - often small, decentralized actors with limited IT infrastructure - to provide verified, high-quality sustainability and supply data in a standardized, privacy-preserving way. Using digital identities (DIDs), verifiable credentials (VCs), and a data intermediary, the Use Case Scenario establishes a trusted data-sharing process where forest owners can digitally confirm their identity and securely transmit structured information (e.g., harvesting and delivery data) to PHA. This approach strengthens data reliability for sustainability reporting and enhances planning, traceability, and regulatory compliance within the Austrian forestry value chain.

Addressed topics and relevance:
- define the role of data intermediaries in coordinating actors and managing consent
  aspect: data intermediary ensures trusted coordination between forest owners and PHA by managing data sharing and consent in a neutral and compliant way
- apply principles from Sitra's Rulebook for a Fair Data Economy
  aspect: addresses principles to ensure transparency, user control, and equitable value sharing in data exchange

Sequence Diagram

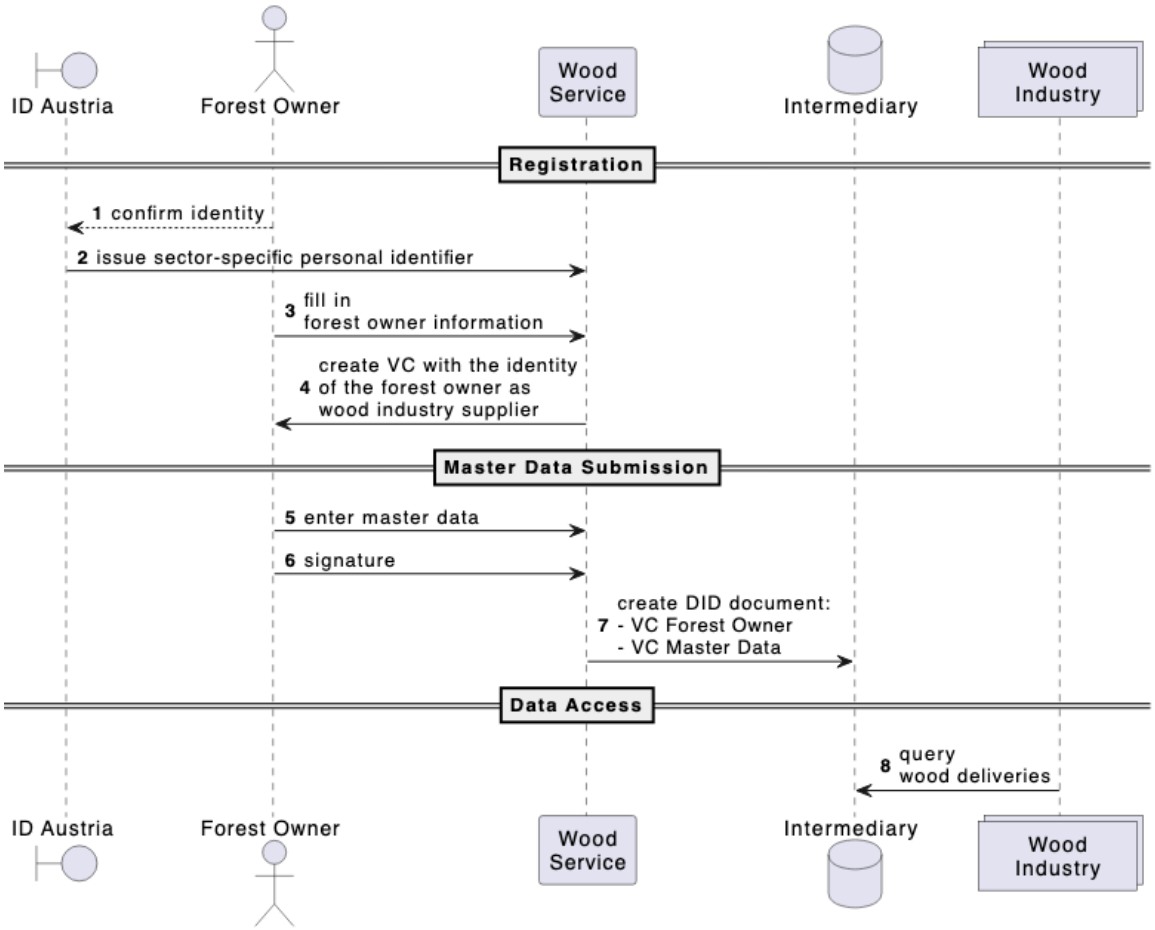

Figure 6: Sequence diagram: improve forest owner data sharing

The sequence diagram illustrates the complete data exchange flow between the forest owner, ID Austria, a wood service, the data intermediary, and the wood industry. The main objective of this Use Case Scenario is to demonstrate how Verifiable Credentials (VCs) and the ID Austria digital identity can be used to establish trust and data authenticity within the forestry data ecosystem.

During the registration phase, the forest owner confirms their identity via ID Austria (steps 1–2), which issues a sector-specific personal identifier. This step ensures that the subsequent data exchange is based on a legally verified identity, meeting national and EU-level eIDAS and Data Governance Act requirements. The forest owner then provides basic identity and supplier information through the wood service (step 3), which creates a Verifiable Credential (step 4) certifying the forest owner as a verified supplier for the wood industry.

In the master data submission phase, the forest owner records additional operational information such as forest plot details, harvest data, or delivery information (step 5) and digitally signs the submission (step 6). The service then creates a DID document that references both the forest owner's VC and the newly issued master data VC (step 7). This linkage ensures that all data remain cryptographically verifiable and traceable to an authenticated source.

Finally, during the data access phase, the wood industry retrieves the verified master data from the intermediary (step 8). The intermediary acts as a neutral, trusted party responsible for secure data storage and consent management, ensuring that only authorized actors can access the shared information.

Overall, this implementation demonstrates how sovereign digital identities and Verifiable Credentials can replace manual data exchange processes in the forestry sector, improving trust, transparency, and compliance while maintaining data sovereignty for forest owners.

Video with walk-through: PACE-DPP_PHAv01.mp4 (publication on YouTube planned after PHA approval)

4.4 Use Case Scenario "Client-Managed Secret Mode"

Description
This Use Case Scenario demonstrates a DPP in which the private key is generated and kept inside the product - specifically, in an Infineon Secure Edge Node - and all signing operations are executed on-device. In CMSM (Client-Managed Secret Mode), external services submit payloads (for DID creation, VC issuance, VP publication, or DID updates) to the secure node, which returns the signature while the key never leaves the hardware. The device thus becomes the cryptographic trust anchor for the product DID and for subsequent verifiable statements across the passport lifecycle.

Equally, the prototype documents the identities and credentials of other actors to complete the chain of trust: e.g., the manufacturer as VC issuer and the secure-element supplier as a referenced, verifiable party. These actor credentials are linked to the product's DID (e.g., via service endpoints and verification relationships), enabling provenance checks, authenticated messaging, and role-based access without exporting secrets from the device. The result is a standards-aligned, hardware-anchored DPP that combines device-held keys, DIDs, and Verifiable Credentials to provide end-to-end, auditably secure product trust.

Addressed topics and relevance:

- link product identifiers to identity-based access rules (QR, RFID, NFC) *aspect: an NFC interface exposes the product's DID, which uses verification relationships to enforce identity-based access to device-signed operations on the Secure Edge Node*
- define access roles for public, business, and regulatory users *aspect: access roles for specific users are defined as DID verification relationships and enforced via credential-based policies at the device and intermediary*
- use decentralised identifiers (DIDs) and verifiable credentials to manage trust *aspect: trust is managed via a device-anchored DID (CMSM) and Verifiable Credentials that cryptographically attest identities and claims*
- ensure secure and privacy-preserving data access throughout the value chain *aspect: access is enforced via on-device keys, DID-based role control, and selective disclosure of VCs so each actor sees only the minimum required data*

Sequence Diagram

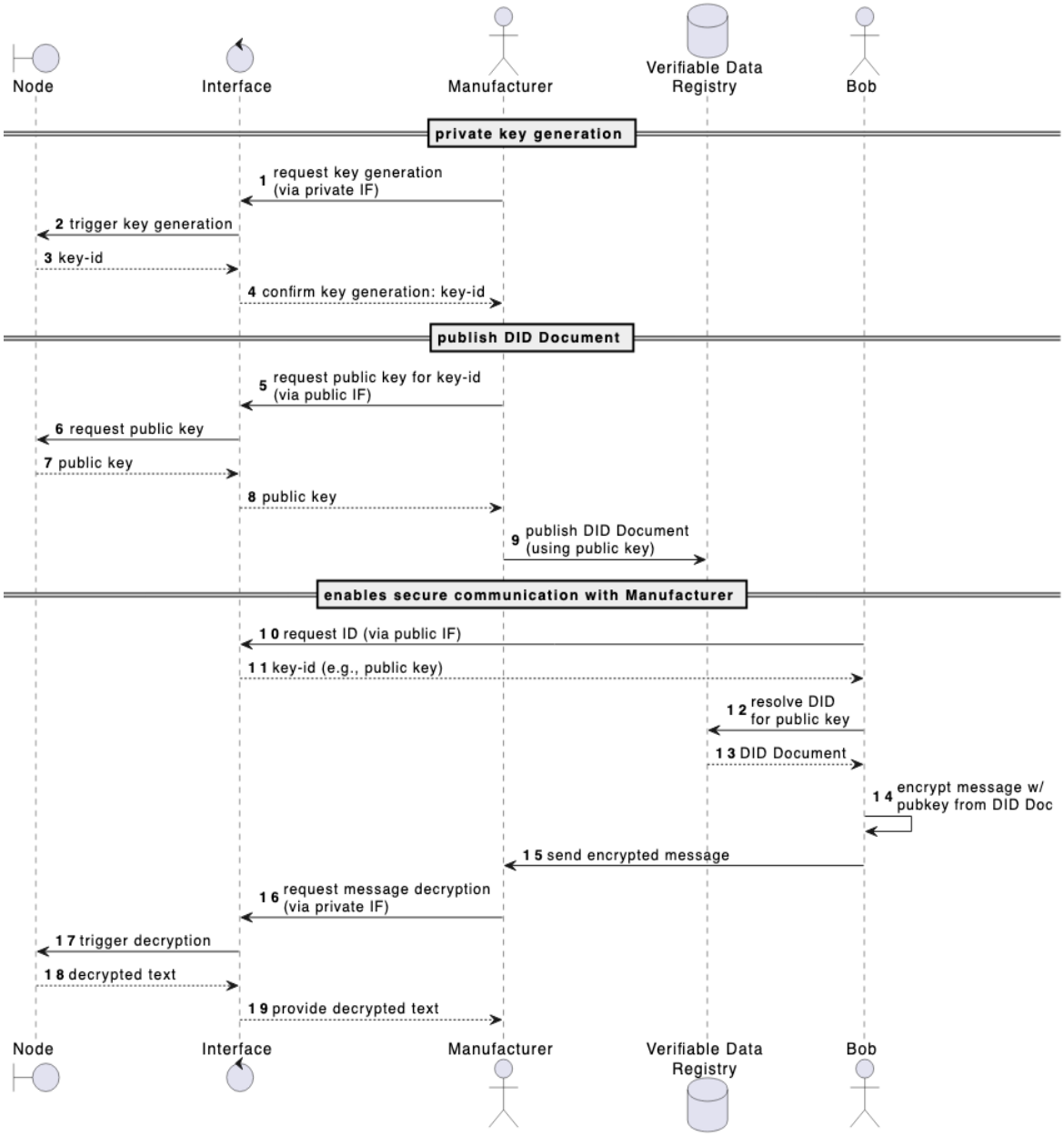

Figure 7: Sequence diagram - Client managed secret mode

Below, each group of interactions in the sequence diagram is explained in terms of what happens and why it is useful for the Client-Managed Secret Mode (CMSM) DPP Use Case Scenario.

1) Private key generation (device-held root of trust)
   The manufacturer requests key generation through the private interface (1), which instructs the Secure Edge Node in the product to create an asymmetric key pair on device (2). The node returns a key-id (3), and the manufacturer confirms the operation (4).
   Scope: The private key never leaves the hardware, establishing a tamper-resistant cryptographic anchor for the product's DID and any later signatures (e.g., for VCs, VPs, event logs). This prevents key export, simplifies compliance, and makes the product itself the trust root for the DPP.
2) Publish DID Document (discoverability and verification)
   To make the key usable by others, the manufacturer asks - via the public interface - for the public key corresponding to the key-id (5–8). Using that public key, the manufacturer publishes the DID Document to a Verifiable Data Registry (9).
   Scope: The DID Document exposes the product's verification methods and verification relationships (e.g., assertionMethod for signing and keyAgreement for encryption) and can include service endpoints (e.g., links to AAS/DPP data via a data intermediary). Anyone resolving the DID can now

verify device-signed data and discover where to request additional information under the correct access policy.

3) Enables secure communication with the manufacturer (role-aware crypto workflows)
The manufacturer queries the public interface to confirm the identifier used for crypto (10–11) and resolves the DID at the registry to obtain the current DID Document (12–13). A third party - shown as Bob (e.g., a service partner or auditor) - uses the DID Document's public key to encrypt a message destined for the device/manufacturer workflow (14). The manufacturer forwards the ciphertext to the system (15), and - via the private interface - requests the node to decrypt (16–18). The decrypted content is returned to the manufacturer (19).

Scope: This demonstrates how the DID's keyAgreement material enables confidential, end-to-end communication with the product while keeping secrets in hardware. Coupled with verification relationships and credential checks, only authorized actors can trigger sensitive operations (e.g., maintenance commands, attestation challenges, or VC issuance), supporting identity-based access control and privacy-preserving data exchange across the value chain.

Taken together, these phases show how CMSM realizes a hardware-anchored DPP: keys are generated and used inside the product, public keys are published via a DID Document for ecosystem verification and discovery, and subsequent interactions (signing, encryption/decryption, VC issuance) are mediated by role-aware policies derived from DID verification relationships - linking the product identifier (via NFC) to identity-based access rules for public, business, and regulatory users.

4.5 Key Findings of the Annual Report 2025

The activities conducted in 2025 resulted in a consolidated understanding of the technical, organisational, and governance requirements for future Digital Product Passport (DPP) ecosystems. Through the development of four rapid prototypes - *Local DPP with did:peer*, *Luminant*, *Improve Forest Owner Data Sharing*, and *Client-Managed Secret Mode* - the project established a first evidence base for the three core specification domains: Meta-Data Specification, Decentralised Identity & Access Management, and Data Intermediary & Governance. These prototypes demonstrated the feasibility of decentralised identifiers in both offline and online settings, the integration of Asset Administration Shell (AAS) data into verifiable DPP workflows, the use of sovereign digital identities for cross-sector data exchange, and the ability of hardware-based trust anchors to support high-assurance interactions.

A key outcome of 2025 is the consolidation of prototype insights toward an integrated demonstrator. While the prototypes address distinct aspects of the ecosystem, their combined findings clarify where harmonisation is required - particularly regarding metadata alignment, identity binding, consent management, and trust establishment. Furthermore, collaboration with partners enabled an initial refinement of governance and access models, including the differentiation of public, business, and regulatory roles through DID verification relationships and Verifiable Credentials.

Overall, the 2025 results provide a robust conceptual and empirical foundation for the specification work presented in the subsequent chapter. They demonstrate that the defined specification domains are not only theoretically valid but also practically actionable, thereby preparing the ground for broader ecosystem alignment and future pilot deployments.

4.6 Planned Development in 2026/2027

Building on the results and validated concepts from 2025, the work in 2026/2027 focuses on advancing the developed prototypes into a coherent, scalable, and interoperable architecture for real-world DPP ecosystems. A central objective is the development of an integrated architecture within the Data-Ecosystem work package that aligns with international state of the art - including CIRPASS-2, emerging European data-space initiatives, and relevant industry standards. This architecture will define how data models, identity mechanisms, verification relationships, and governance structures interact across heterogeneous systems and product groups.

In parallel, the project will deepen the refinement of governance and access models together with industry, public-sector, and ecosystem partners. This includes evaluating how a data intermediary can assume operational responsibilities - such as consent management, role assignment, policy enforcement, and lifecycle transitions - in practice-relevant use cases. The role of intermediaries will be tested in additional work

packages, but the conceptual and architectural foundation will be designed within the Data-Ecosystem package.

Another major focus is the consolidation of prototype components into a unified demonstrator, enabling end-to-end evaluation of metadata handling, DID-based identity management, on-device trust anchors, and data-space integration. This demonstrator will serve as a basis for initial ecosystem-wide alignment and the preparation of pilot deployments in operational environments.

Through these developments, the project aims to ensure that the resulting architecture is future-proof, interoperable, and capable of supporting real DPP implementations across industries while maintaining technical rigor, regulatory compatibility, and practical relevance.

Figures & Tables

Figure 1: Togaf Framework 11
Figure 2: Combined approach Togaf & Sitra 13
Figure 3: Overview status use case scenarios 29
Figure 4: Sequence Diagram Local DPP with did:peer 32
Figure 5: Sequence diagram Luminant 33
Figure 6: Sequence diagram: improve forest owner data sharing 35
Figure 7: Sequence diagram - Client managed secret mode 37

Table 1: Draft implementation checklist digital nameplate 15
Table 2: Draft implementation AAS 16

References

[1] 'TOGAF | www.opengroup.org'. Accessed: Nov. 19, 2025. [Online]. Available: https://www.opengroup.org/togaf

[2] 'Rulebook model for a fair data economy (version 3.0)', Sitra. Accessed: Nov. 19, 2025. [Online]. Available: https://www.sitra.fi/en/publication/rulebook-for-a-fair-data-economy/

[3] C. Mazzocca, A. Acar, S. Uluagac, R. Montanari, P. Bellavista, and M. Conti, 'A Survey on Decentralized Identifiers and Verifiable Credentials', *IEEE Communications Surveys & Tutorials*, pp. 1–1, 2025, doi: 10.1109/COMST.2025.3543197.

[4] S. Khan *et al.*, 'A Survey on X.509 Public-Key Infrastructure, Certificate Revocation, and Their Modern Implementation on Blockchain and Ledger Technologies', *IEEE Communications Surveys & Tutorials*, vol. 25, no. 4, pp. 2529–2568, 2023, doi: 10.1109/COMST.2023.3323640.

[5] Y. K. Tolcha, G. Park, and D. Kim, 'Building Digital Product Passports: EPCIS 2.0 Meets Knowledge Graphs', in *2025 IEEE International Conference on RFID (RFID)*, Apr. 2025, pp. 1–6. doi: 10.1109/RFID64926.2025.11015538.

[6] M. A. Mehrabi, C. Doche, and A. Jolfaei, 'Elliptic Curve Cryptography Point Multiplication Core for Hardware Security Module', *IEEE Transactions on Computers*, vol. 69, no. 11, pp. 1707–1718, Nov. 2020, doi: 10.1109/TC.2020.3013266.

[7] C. Ducuing and R. H. Reich, 'Data governance: Digital product passports as a case study', *Competition and Regulation in Network Industries*, vol. 24, no. 1, pp. 3–23, Mar. 2023, doi: 10.1177/17835917231152799.

[8] A. L. Våge, 'Industry 4.0 and Asset Administration Shell (AAS): Implementing a Small Scale Demonstrator', Master thesis, NTNU, 2023. Accessed: Nov. 19, 2025. [Online]. Available: https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/3082413

[9] L. Mattei, F. Morpurgo, C. Occhipinti, L. M. Ratto Vaquer, and T. Vasylieva, 'Self-Sovereign Identity Model: Ethics and Legal Principles', *DISO*, vol. 3, no. 2, p. 25, June 2024, doi: 10.1007/s44206-024-00113-2.

[10] V. Sahiti Yellanki and B. Sah, 'A Survey on Various Secure Access Control and Authentication in a Block Chain-Enable Cloud IoT', in *Explainable IoT Applications: A Demystification*, S. N. Mohanty, S. Satpathy, X. Cheng, and S. K. Pani, Eds, Cham: Springer Nature Switzerland, 2025, pp. 295–308. doi: 10.1007/978-3-031-74885-1_19.

[11] H. J. Pandit, B. Esteves, G. P. Krog, P. Ryan, D. Golpayegani, and J. Flake, 'Data Privacy Vocabulary (DPV) -- Version 2', Aug. 27, 2024, *arXiv*: arXiv:2404.13426. doi: 10.48550/arXiv.2404.13426.

[12] 'Ontology Requirements Specification_v1.0.pdf', Google Docs. Accessed: Nov. 19, 2025. [Online]. Available: https://drive.google.com/file/d/193PSjcwGupcLnl7U42sv85tXQVtZwi9K/view?usp=embed_facebook

[13] J. Conde, A. Pozo, A. Munoz-Arcentales, J. Choque, and Á. Alonso, 'Fostering the integration of European Open Data into Data Spaces through High-Quality Metadata', Feb. 08, 2024, *arXiv*: arXiv:2402.06693. doi: 10.48550/arXiv.2402.06693.

[14] M. Pathak, 'Data Governance Redefined: The Evolution of EU Data Regulations from the GDPR to the DMA, DSA, DGA, Data Act and AI Act.', Feb. 06, 2024, *Social Science Research Network, Rochester, NY*: 4718891. doi: 10.2139/ssrn.4718891.

[15] B. P. Gallagher, 'Using the Architecture Tradeoff Analysis MethodSM to Evaluate a Reference Architecture: A Case Study', Art. no. CMUAEI2000TN007, June 2000, Accessed: Nov. 19, 2025. [Online]. Available: https://apps.dtic.mil/sti/html/tr/ADA388852/

[16] R. Kazman, M. Klein, and P. Clements, 'ATAM: Method for Architecture Evaluation':, Defense Technical Information Center, Fort Belvoir, VA, Aug. 2000. doi: 10.21236/ADA382629.

[17] J. Deich, L. Loeb, A. Meins-Becker, T. Meisen, and A. Pomp, 'Towards Connecting General DPP Ontology Frameworks with Domain-specific Information Sources'.

[18] 'Ontology Requirements Specification_v1.0.pdf', Google Docs. Accessed: Nov. 19, 2025. [Online]. Available: https://drive.google.com/file/d/193PSjcwGupcLnl7U42sv85tXQVtZwi9K/view?usp=embed_facebook

[19] 'Specifications · DPP Vocabulary Hub · Semantic Treehouse'. Accessed: Nov. 19, 2025. [Online]. Available: https://dpp.vocabulary-hub.eu/specifications

[20] 'Data Catalog Vocabulary', *Wikipedia*. Sept. 28, 2024. Accessed: Nov. 19, 2025. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Data_Catalog_Vocabulary&oldid=1248213646

Project participants:

Virtual Vehicle Research GmbH (AT)

Fahrzeugwerk Bernard KRONE GmbH & Co. KG (DE)
Forschung Burgenland GmbH (AT)
Infineon Technologies Austria AG (AT)
Papierholz Austria GmbH (AT)
Research Studios Austria Forschungsgesellschaft mbH (AT)
Siemens Aktiengesellschaft Österreich (AT)
Silicon Austria Labs GmbH (AT)
Spath Micro Electronic Design GmbH (AT)
Sustainista GmbH (AT)
Technische Universität Berlin, Institut für Werkzeugmaschinen und Fabrikbetrieb (DE)
Technische Universität Wien, Institute of Computer Engineering (AT)
Verein zur Förderung der selbstständigen Nutzung von Daten, OwnYourData.eu (AT)

Acknowledgment

Funded by
Federal Ministry
Innovation, Mobility
and Infrastructure
Republic of Austria

FFG
Promoting Innovation.

DLR Projektträger

Supported by:
Federal Ministry
for Economic Affairs
and Climate Action
on the basis of a decision
by the German Bundestag

This Lighthouse Project has been made possible by financial contributions from the Austrian Federal Ministry for Innovation, Mobility and Infrastructure (BMIMI), supported by the Austrian Research Promotion Agency (FFG), as well as from the German Federal Ministry for Economic Affairs and Climate Action (BMWK), supported by the German Research Promotion Agency (DLR-PT).

Disclaimer

Every effort has been made to ensure complete and accurate information concerning this document. However, the author(s) and members of the consortium cannot be held legally responsible for any mistake in printing or faulty instructions. The authors and consortium members retrieve the right not to be responsible for the topicality, correctness, completeness or quality of the information provided. Liability claims regarding damage caused using any information provided, including any kind of information that is incomplete or incorrect, will therefore be rejected. The information contained in the document is based on the author's experience and on information received from the project partners – the Publication as provided reflects the authors' views.