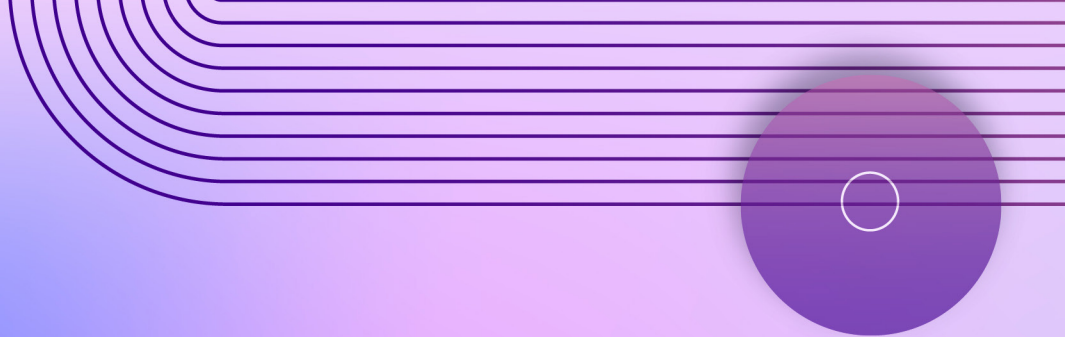




Building the Trusted Internet of Product Data for Digital Product Passport Ecosystems

The Role of Data Spaces,
Asset Administration Shells,
and European Business Wallets

Contributing Projects & Initiatives



Authors

Jesús Alonso, BAIDATA
Katia Lavín, INNOVALIA ASSOCIATION
Cristina Urizar, BAIDATA
Juan Manuel Losada, CBT MULTIMEDIA
Sergio Gusmeroli, POLITECNICO DI MILANO
Arnab Sinha, CEA
Óscar Lázaro, INNOVALIA ASSOCIATION
Carmen Polcaro, INNOVALIA ASSOCIATION
E. Alessandro Canepa, FRATELLI PIACENZA
Juilee Tikekar, IDTA
Haris Avgoustinos, KIWA
Carla Fité Galan, REVERSE RESOURCES
Traci Kinden, STITCHING TEXROAD
Claire Fioretti, MICHELIN FRANCE
Riccardo Giovannotti, GDSO
Kamila Kocia, AVERY DENNISON
Jelte Bootsma, TNO
Andreas Schneider, GTS
Nikolaos Saklamanakis, FUJITSU TECHNOLOGY SOLUTIONS
Carsten Stöcker, SPHERITY

Digital Object Identifier

<https://doi.org/10.5281/zenodo.23417461>

Abstract

The Digital Product Passport (DPP) is emerging as a cornerstone of Europe's transition towards a circular, transparent and data-driven economy. However, scaling DPP ecosystems across global supply chains requires an architecture that can scale across industries and borders while preserving interoperability, trust and data sovereignty. This paper establishes Data Spaces as a key unifying B2B backbone and enabler for a trusted Internet of Product Data (IoPD).

Data spaces natively address the three structural dimensions of DPP execution: sovereign usage control, federated semantic interoperability, and centralized or federated counterparty trust. Within this sovereign transport layer, technological components operate as flexible, interoperable building blocks adapted to sectoral requirements: (1) Semantic Data Modelling, where payloads accommodate the DSSC Blueprint four-level semantic architecture (vocabularies, ontologies, application profiles and schemas) serialized in W3C/JSON-LD, or leverage specialized industrial digital twin models such as the Asset Administration Shell (AAS, IEC63278) for multi-level asset aggregation; and (2) Trust and Identity Anchoring, in which counterparty authentication and non-repudiation can integrate eIDAS 2.0 European Business Wallets (EBWs) and Verifiable Credentials (VC), or leverage established PKI frameworks and X.509 certificates, based on domain maturity.

By evaluating cross-sectorial practical implementations across the tyre, textile, furniture, automotive, and semiconductor sectors, this paper demonstrates how a data-space-centric architecture enables multi-stakeholder value creation beyond regulatory compliance, driving European industrial competitiveness through data-driven circularity.

Keywords

Digital Product Passport, Data Spaces, Asset Administration Shell, Data Sovereignty, Circular Economy

Acknowledgments

This work was supported by the Digital Europe Programme (DIGITAL) under Grant Agreements No 101158775 (CIRPASS2), 101123490 (SM4RTENANCE), and 101195471 (SAGE) and under the Horizon Europe Programme (HORIZON) under Grant Agreement No 101182081 (CIR4FUN).

The CIRPASS-2 consortium extends its grateful thanks to Coen JANSSEN and Gabriel CARLIN from DGCONNECT (European Commission) for the hours of patient discussion and open collaboration that were necessary for the creation of this document.

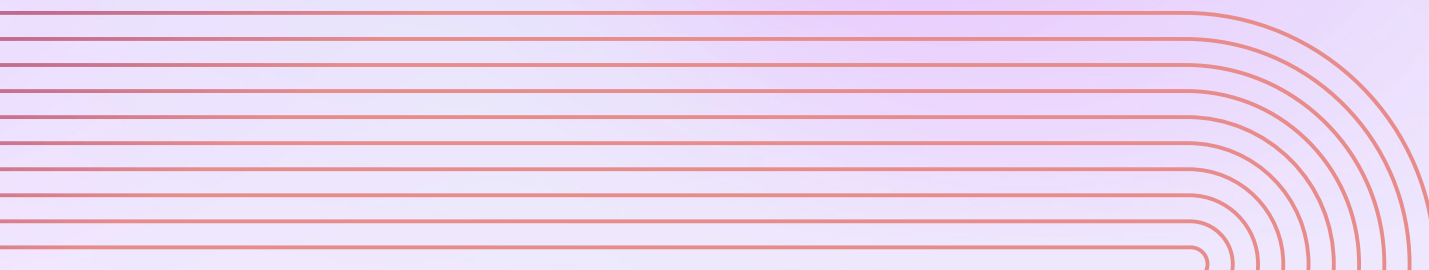


Table of Contents

1.	Introduction: The New Era of Product Transparency	5
2.	From Internet of Things (IoT) to Internet of Product Data (IoPD)	6
2.1.	Internet of Things (IoT)	6
2.2.	Internet of Products (IoP)	6
2.3.	Internet of Product Data (IoPD)	6
3.	DPP System: Practical Implementation Challenges	8
3.1.	Scalable Data Governance and Sovereignty Risks	8
3.2.	Semantic Interoperability and Seamless Global Data Integration	8
3.3.	Institutional Trust, Data Provenance, and Compliance Liabilities	9
4.	The Internet of Product Data: Digital Product Passports powered by Data Spaces	9
4.1.	Data Spaces as the B2B backbone for a trusted internet of product data	10
4.2.	Data Modelling Paradigms: Structuring Semantic Payloads from DSSC Artifacts to the Asset Administration Shell (AAS)	14
4.3.	Trust and Identity Frameworks: From Hierarchical PKI to Decentralized Verifiable Credentials	19
4.4.	Semantic Governance: Artifact Lifecycle and Structural Maintenance	20
4.5.	Exploiting Data with DPP Applications: The Value Creation Layer	21
4.6.	Reference implementation: The IMX Council Battery DPP Showcase	23
5.	DPP Practical implementations with Data Spaces	26
5.1.	The Tyre Industry Use Case: Lifecycle Data Sharing	26
5.2.	Textile Industry Use Cases	30
5.3.	Furniture Industry Use Cases	37
5.4.	Semiconductor Industry: Semiconductor-X	42
5.5.	Energy Data and BESS: Market-Role Governance and Controlled Battery-Passport Access	51
5.6.	DPPs, Data Spaces and EBWs: WE BUILD Practical Implementations	53
6.	Conclusions and Recommendations	57
6.1.	Conclusions: From Regulatory Compliance to Unprecedented Data Exploitation	57
6.2.	Strategic Recommendations for Economic Operators	58
6.3.	Strategic Recommendations for Policy Makers & Regulators	58
	Annex A: Alignment Matrix with CIRPASS D4.1 Reference Architecture	59

1. INTRODUCTION: THE NEW ERA OF PRODUCT TRANSPARENCY

Europe is entering a new era of product transparency in which information must become persistent, structured, accessible and trustworthy across the entire cradle-to-cradle lifecycle, from ideation and manufacturing to end-of-life and re-manufacturing or recycling. In this context, the **Digital Product Passport (DPP)**, initially conceived for cross-border market surveillance, is emerging as a structured collection of dynamic product-related data, linked to a unique identifier and governed by explicit access rights, to support sustainability, circularity, value retention and regulatory compliance. This marks a shift away from static documentation, fragmented declarations and one-off audits toward continuously available, machine-readable product intelligence, interoperable across manufacturers, suppliers, market authorities and, where relevant, consumers.

As the DPP transition demands all the 5Vs characteristics¹ of a product data, a novel, secure and trusted architecture for product data sharing is needed. In this architecture, **DPPs** provide the policy and consumer-side driver by defining mandatory product information, while **Data Spaces** supply the foundational, payload-agnostic business-to-business infrastructure backbone enabling cross-organizational data exchange while preserving confidentiality and data sovereignty. Within this sovereign data space envelope, technical components operate as adaptable building blocks:

- **Semantic Data Modelling:** Payloads leverage domain ontologies and application profiles serialized in W3C/JSON-LD or specialized industrial digital twin metamodels like the Asset Administration Shell (AAS, IEC63278) for complex industrial assets, aligned across the DSSC four-level semantic stack.
- **Trust and Identity Anchoring:** Counterparty authentication and payload non-repudiation can integrate eIDAS 2.0 European Business Wallets (EBWs) and Verifiable Credentials (VCs), or leverage established PKI frameworks and X.509 cryptographic signatures depending on value chain maturity

Integrated within a unified data space governance models, these building blocks architect a trusted **Internet of Product Data (IoPD)**: a variegated business-consumer-government ecosystem where product information is dynamically discovered, verified, and securely exchanged across borders and value chains.

While the DPP ecosystem provides the product-centric network to operationalize passport data for Green Eco-Design and Sustainability, the Data Space ecosystem deploys the broader governed Digital infrastructure for secure, interoperable data exchange across multiple use cases. Consequently, this integrated framework becomes a foundational capability for **Europe's Twin Transition** (Digital and Green). It enables economic operators to migrate from compliance-by-document to compliance-by-data, transitioning from isolated databases to interoperable information flows, and from unverifiable claims to traceable, identity-linked evidence. For industry, this establishes the baseline for more efficient reporting, circular business models and cross-sector interoperability; for regulators, it optimizes requirement verification; and for markets, it scales trustworthy product transparency.

¹ Volume, Velocity, Variety, Veracity, Value

2. FROM INTERNET OF THINGS (IOT) TO INTERNET OF PRODUCT DATA (IOPD)

The evolution from IoT to IoPD reflects a fundamental paradigm shift in how product information is structured, governed and exchanged across industrial value networks. Moving beyond isolated telemetry and centralized repositories, the ESPR framework² demands a transition towards a layered, federated lifecycle-wide product intelligence.

2.1. Internet of Things (IoT)

IoT architectures prioritize physical connectivity, telemetry and operational control (e.g., fault detection, remote maintenance) within closed, vertical systems. The generated data is device-centric, platform-siloed, and decoupled from standardized product models, severely limiting its reuse for cross-organizational transparency, circularity, and regulatory reporting.

2.2. Internet of Products (IoP)

IoP elevates the IoT paradigm by anchoring connectivity to product identities, enabling servitization (e.g., predictive maintenance, pay-per-use models, performance-based contracts). This gave rise to first-generation DPPs – monolithic SaaS platforms focus primarily on consumer-facing (B2C) presentation and static compliance declarations. While effective as presentation interfaces and immediate responsiveness, these centralized systems face severe limitations when attempting to aggregate complex, multi-tier supply chain data. Upstream suppliers remain reluctant to deposit proprietary know-how into third-party, closed databases, creating critical data gaps in primary Product Carbon Footprints (PCF), material provenance and supply-chain environmental impacts.

2.3. Internet of Product Data (IoPD)

IoPD resolves this bottleneck by decoupling the **underlying B2B data infrastructure** from the **top-tier application interfaces**. IoPD treats structured product data as a primary, governable asset distributed across federated networks, serving all levels of identification granularity under the ESPR mandate:

- **Model-level & Batch-level DPPs:** Leverage IoPD as a federated B2B aggregation engine. It allows economic operators to securely collect upstream supply chain data—such as raw material provenance, chemical compliance, and transport/distribution carbon footprints—from Tier-N suppliers without forcing them to expose proprietary business relationships.
- **Item-level (Instance) DPPs:** Extend this B2B backbone into the post-sale operational lifecycle. As illustrated in Figure 1, the Internet of Product Data (IoPD) reference architecture enforces a structural decoupling between top-tier application and value-creation interfaces (B2C/B2B) and the underlying federated B2B infrastructure layer. Within this sovereign transport layer, Data Spaces act as the payload-agnostic usage-control backbone (DSP/ODRL), orchestrating modular building blocks for semantic data modelling—incorporating W3C/JSON-LD domain ontologies and Asset Administration Shells—and decentralized trust anchoring (eIDAS 2.0 European Business Wallets, Verifiable Credentials, and PKI frameworks).

²<https://green-forum.ec.europa.eu/implementing-ecodesign-sustainable-products-regulation>

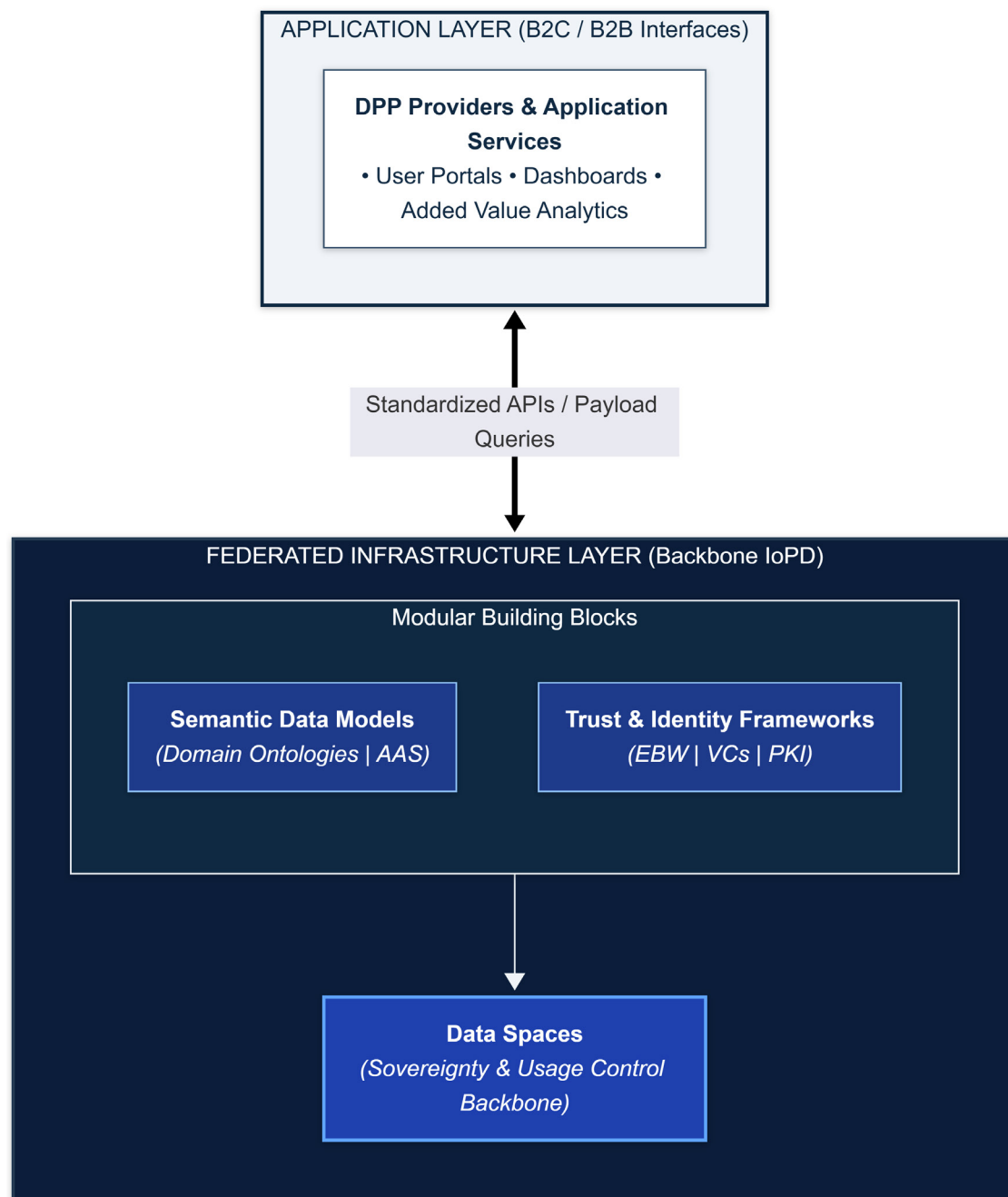


Figure 1. Layered Internet of Product Data (IoPD) Reference Architecture

In this architecture, DPP Providers and Economic Operators are able to transition from isolated static data silos into high-value dynamic application enablers. Rather than attempting to own or centralize the data layer, the DPP Ecosystem consumes sovereign, standardized data payloads – delivered over Data Space connectors using domain ontologies or digital twin models like AAS – to power intuitive user interfaces, regulatory reporting tools, and advanced value-added services for consumers, manufacturers, and market authorities.

By establishing Data Spaces as the sovereign B2B trust engine, complemented by flexible semantic and identity building blocks, IoPD empowers the entire ecosystem: suppliers maintain data sovereignty, manufacturers achieve automated ESPR compliance, and software providers scale innovative digital services on top of a trusted product data foundation.

3. DPP System: Practical Implementation Challenges

Operationalizing an open, multi-tier Internet of Product Data (IoPD) under the Ecodesign for Sustainable Products Regulation (ESPR) is not merely a software deployment exercise; it demands resolving systemic architectural frictions across competitive, cross-border value networks. As mandatory implementation timelines approach for diverse product categories, operational execution faces a severe **sectoral readiness asymmetry**. While highly digitized industrial ecosystems have actively pioneered sovereign data sharing frameworks, less digitally mature value chains exhibit minimal familiarity with data space paradigms and are heavily dominated by micro-SMEs. This acute timeline compression, combined with heterogeneous digital capabilities and cross-border supply chain fragmentation, exposes three primary technical and governance bottlenecks.

3.1. Scalable Data Governance and Sovereignty Risks

Scalable data governance across multi-tier supply chains requires resolving a fundamental paradox: maximizing data usefulness for circularity while enforcing zero-trust data minimization to protect proprietary IP (e.g., bills-of-materials, chemical compositions, and operational margins). Conventional binary access control models collapse in federated networks, where data sensitivity ranges from public compliance declarations to highly confidential trade secrets.

Consequently, the primary governance bottleneck is achieving machine-executable, attribute-level policy enforcement that dynamically restricts data visibility on an essential “need-to-know” basis. This governance framework must operate as an auditable transaction mechanism—providing non-repudiable proof of counterparty identity, access timestamps, and contractual policy compliance—while maintaining the architectural flexibility required to support voluntary, monetized B2B data exchanges that extend well beyond baseline ESPR mandates.

3.2. Semantic Interoperability and Seamless Global Data Integration

Industrial product data remains trapped inside heterogeneous enterprise systems (ERP, PLM, MES, compliance databases) utilizing diverse product identifiers, proprietary structural schemas, and domain-specific vocabularies. This integration friction is severely compounded by 2 structural operational deficits:

- **Upstream Identification Gap (EN 18219 / ISO 15459):** While downstream B2C logistics benefit from established commercial identifier schemes, Tier-N material suppliers and upstream processing facilities frequently lack standardized Product, Operator, and Facility Identifier schemes compliant with EN 18219 and ISO 15459.
- **Voluntary Standard Adoption Paradox (JTC 24 & JRC):** Although the Joint Research Centre (JRC) strongly recommends deploying the eight CEN-CENELEC JTC 24 standards to achieve cross-sectoral interoperability, compliance under baseline ESPR delegated acts remains largely voluntary

for economic operators (in contrast to stricter mandatory mandates emerging in domain-specific frameworks such as the Packaging and Packaging Waste Regulation - PPWR).³

Without **standardized structural representations**, persistent upstream identifiers, and formal domain ontologies, critical compliance and circularity attributes (e.g., recycled content percentages, REACH chemical limits⁴, Scope 3 footprints⁵) lose context during transfer. This triggers severe semantic degradation and prohibitive integration overhead (the “NxN custom interface problem”), rendering automated, machine-to-machine verification operationally unfeasible under tight regulatory deadlines.

3.3. Institutional Trust, Data Provenance, and Compliance Liabilities

In a federated multi-tier network, trust extends beyond inspecting data payloads; it demands mutual, cryptographically verifiable counterparty authentication. Economic operators must verify the legal identity and authorization of both data issuers (who publish lifecycle assertions) and data consumers (who request access to sensitive attributes) without relying on a single, centralized identity provider. Without verifiable organizational identities, decentralized counterparty authentication, and immutable provenance trails, dynamic DPP ecosystems become highly vulnerable to identity spoofing, unauthorized data harvesting, payload tampering, and greenwashing liabilities. If actor identities, source integrity, and legal accountability cannot be cryptographically guaranteed across EU jurisdictions, market confidence in the passport system collapses—degrading the DPP from a dynamic business driver into a high-risk administrative tax.

4. THE INTERNET OF PRODUCT DATA: DIGITAL PRODUCT PASSPORTS POWERED BY DATA SPACES

A scalable DPP ecosystem requires more than a compliance interface or a centralized repository. It demands a distributed architecture enabling policy-enforced data exchange, semantic interoperability, verifiable trust and downstream value creation. The **structural interaction between DPPs and Data Spaces** represents the optimal industrial implementation model: product data remains under the absolute control of the data owner, while becoming FAIR and cryptographically verifiable through standardized technical, semantic and governance rules. This structural interaction is detailed in Figure 2, which outlines a three-stage execution workflow decoupling application-layer queries from sovereign B2B data governance: (1) decentralized counterparty authentication using interoperable identity claims (eIDAS 2.0 EBWs, VCs, or PKI), (2) machine-executable usage policy enforcement via Data Space Control Planes (ODRL), and (3) auditable peer-to-peer delivery of structured payloads (W3C/JSON-LD domain ontologies or Asset Administration Shells) directly from the authoritative data provider.

³ Regulation (EU) 2025/40 of the European Parliament and of the Council of 19 December 2024 on packaging and packaging waste, amending Regulation (EU) 2019/1020 and Directive (EU) 2019/904, and repealing Directive 94/62/EC (Text with EEA relevance): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202500040

⁴ REACH Regulation explained, available at https://environment.ec.europa.eu/topics/chemicals/reach-regulation_en

⁵ CARBON TRUST, “What are Scope 3 emissions and why do they matter?” Available at <https://www.carbontrust.com/en-eu/our-work-and-impact/guides-reports-and-tools/what-are-scope-3-emissions-and-why-do-they-matter>

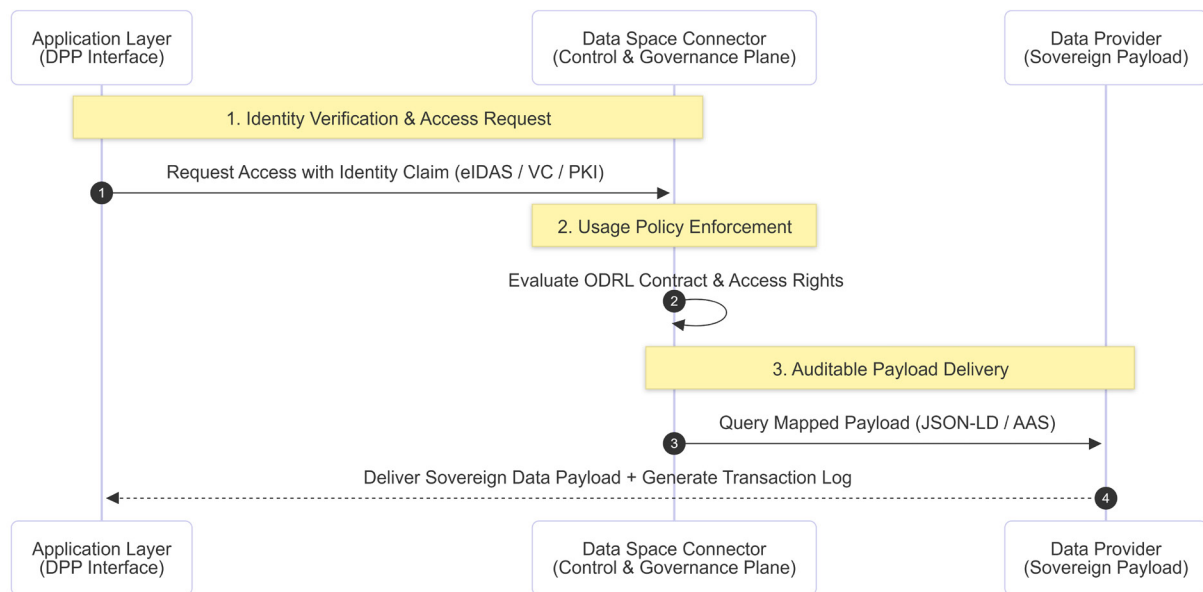


Figure 2. Simplified Interaction Flow of the Data Space Engine

4.1. Data Spaces as the B2B backbone for a trusted internet of product data

Deploying a DPP ecosystem at scale demands an architecture capable of operating across untrusted, multi-tier industrial value chains. Rather than acting as a single-purpose governance layer, **data spaces constitute the foundational B2B infrastructure backbone of the Internet of Product Data (IoPD)**. They provide an integrated, multi-dimensional execution environment that natively combines sovereign usage control, semantic alignment, and distributed trust mechanics.

By decoupling physical data storage from discovery and exchange, product lifecycle data remains within the enterprise boundary (ERP, PLM, MES, Edge) of the data generator, exposed exclusively through standardized, policy-enforcing data space connectors (e.g., Eclipse Dataspace Components (EDC)⁶, Simpl-open stacks⁷) compliant with the Dataspace Protocol (DSP)⁸, Gaia-X/IDSA reference architectures and the emerging normative framework of ISO/IEC DIS 20151-1 (Information technology – Data Spaces – Part 1: Framework and architecture)⁹.

As illustrated in Figure 3, the operational execution of these connectors relies on a strict structural decoupling between the Control Plane (governance, identity assertion, ODRL policy negotiation, catalogue discovery, and auditable transaction logging) and the Data Plane (payload-agnostic peer-to-peer delivery, protocol translation, streaming, and cryptographic signing). This architecture enforces machine-executable usage control prior to data transit, guaranteeing data sovereignty across federated B2B networks regardless of the underlying semantic model or trust framework.

⁶ Eclipse Dataspace Components available at <https://projects.eclipse.org/projects/technology.edc>

⁷ The Simple programme, available at <https://simpl-programme.ec.europa.eu/book-page/simpl-programme>

⁸ The Dataspace Protocol, available at <https://internationaldataspaces.org/offers/dataspace-protocol/>

⁹ ISO/IEC FDIS 20151-1: Cloud computing and distributed platforms – Dataspaces [Part 1: Concepts and characteristics] Available at <https://www.iso.org/standard/86589.html>

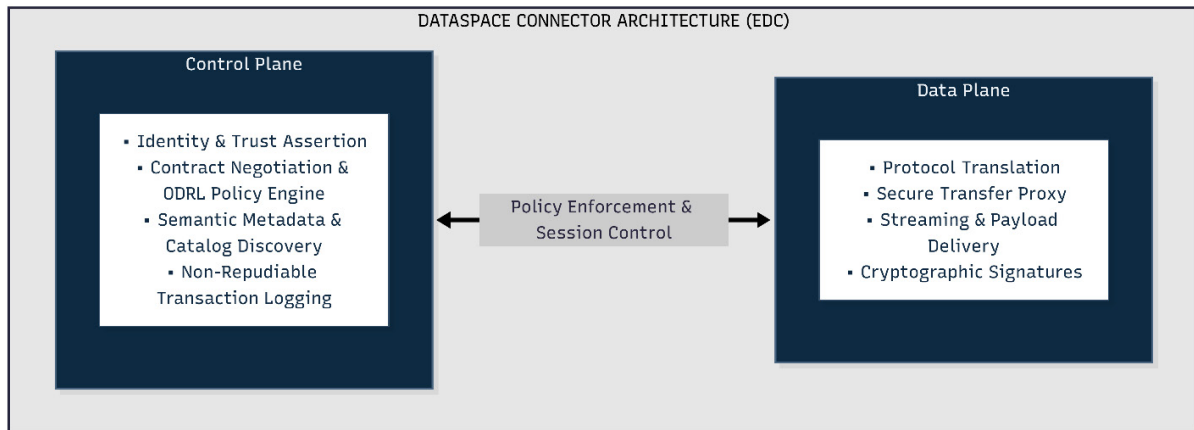


Figure 3. Decoupled Dataspace Connector Architecture (Eclipse Dataspace Components - EDC)

Alignment with CIRPASS 2 Architectural Recommendations (D4.1)

Furthermore, the IoPD architecture directly operationalizes the baseline recommendations established in CIRPASS Deliverable D4.1 (System Architecture for the Digital Product Passport)¹⁰ across a four-layer functional convergence stack (Figure 4). While CIRPASS D4.1 specifies functional building blocks for identity, exchange governance, semantic payloads, and value-added applications, the IoPD framework supplies the concrete B2B execution mechanism—leveraging DSP connectors, Asset Administration Shell (AAS) metamodels, and eIDAS 2.0 European Business Wallets (EBWs).

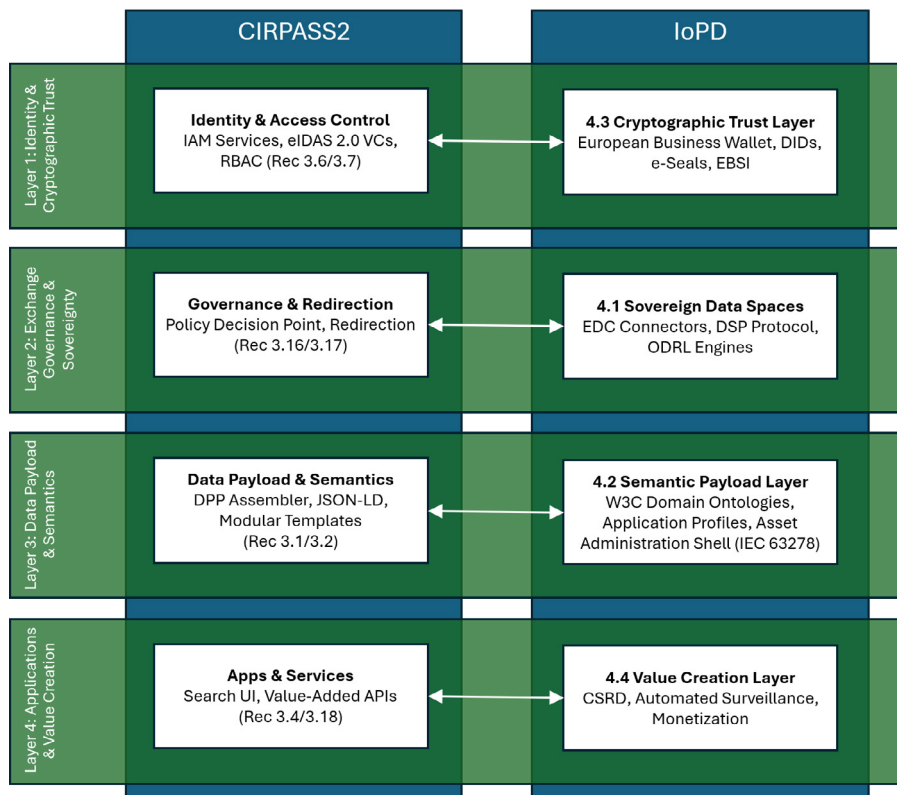


Figure 4. Architectural Convergence Stack: Mapping CIRPASS-2 Architecture to the Four-Layer IoPD Execution Engine.

¹⁰ <https://doi.org/10.5281/zenodo.15388412>

A comprehensive 25-point mapping matrix linking every CIRPASS D4.1 recommendation directly to its technical execution within the IoPD stack is provided in Annex A.

4.1.1. Resolving Scalable Data Governance and Sovereignty Risks (Challenge 3.1)

Data spaces mitigate governance and sovereignty risks by replacing binary access permissions with machine-executable **Usage Policies**. Operating via the Connector Control Plane, data space participants utilize standardized policy specification languages—such as the Open Digital Rights Language (ODRL)—to attach fine-grained usage constraints directly to dataset attributes (e.g., bills-of-materials, chemical compositions, or carbon footprints). Prior to payload delivery, automated bilateral contract negotiations evaluate:

- **Access Policies:** Verifying counterparty prerequisites and authorization status.
- **Usage Control Policies:** Enforcing post-ingress execution constraints at the Data Plane (e.g., prohibiting third-party redistribution, restricting persistence, or limiting data consumption strictly to regulatory verification).

4.1.2. Embedding Semantic Interoperability as an Essential Dimension (Challenge 3.2)

From their inception, data space architectures have recognized that sovereign data exchange is meaningless without shared semantic context. Rather than treating semantics as an external dependency, data spaces incorporate semantic interoperability as an essential, native dimension of the data sharing paradigm.

Through federated metadata catalogues and standardized semantic descriptors, data spaces ensure that published data products carry explicit, machine-interpretable meaning. When an economic operator queries a data space catalogue, the discovery mechanism exposes not only network endpoints, but also the structural schemas and shared domain vocabularies required to interpret the payload. This allows heterogeneous enterprise systems to parse compliance and circularity attributes (e.g., primary PCFs, reparability metrics) without semantic degradation or manual mapping.

To support this semantic interoperability, a number of complementary semantic artefacts are required. Following the DSSC Blueprint, four layers can be distinguished, each contributing to semantic and technical interoperability.

1. **Vocabularies:** Define concepts, classifications, and code lists that establish a common terminology.
2. **Ontologies:** Formally describe the meaning of these concepts and their relationships. For DPPs, core ontologies provide reusable cross-domain concepts, while domain ontologies extend them with sector-specific concepts, enabling cross-sector semantic interoperability.
3. **Application Profiles:** Specify how concepts should be used within a particular business context, including constraints and validation rules (e.g., the SEMIC methodology for Core Vocabularies and Application Profiles¹¹).
4. **Data schemas:** Provide technology-specific representations of application profiles (such as JSON Schema, XML Schema, or SHACL), deployed by standardized REST APIs to exchange and validate information in the data plane.

¹¹ <https://interoperable-europe.ec.europa.eu/collection/semic-support-centre/application-profiles-what-are-they-and-how-model-and-reuse-them-properly-look-through-dcat-ap>

Together, these artefacts form the semantic foundation of DPP-enabled data spaces. To deploy these semantic assets across federated networks, data spaces rely on a governed Vocabulary Service as defined by the DSSC Blueprint. This public repository enables participants to discover, publish and maintain shared models, directly fulfilling Article 33(b) of the EU Data Act (Regulation EU 2023/2854¹²), which mandates data providers to describe their data structures, formats, vocabularies, classification schemes, taxonomies and code lists in a publicly available and consistent manner.

This native semantic mapping operates in full compliance with the European standardization mandate under **CEN/CENELEC JTC 24**, embedding harmonized specifications for unique identifiers (EN 18219), data carriers (EN 18220), lifecycle APIs (EN 18222), authentication mechanisms (EN 18230), and decentralized resolution protocols (EN 18240) directly into the connector control plane.

Technical interoperability within the IoPD backbone operationalizes the essential requirements established under **Article 33 of the EU Data Act (Regulation (EU) 2023/2854)**. To formalize these provisions across the European Single Market, the European Commission issued **Standardization Request M/614** (adopted July 2025) for a **European Trusted Data Framework**.

Executed jointly by **CEN/CENELEC JTC 25** (Data Spaces and Data Management) and **ETSI TC DATA**, this formal standardization pipeline codifies specifications from key data space initiatives (Gaia-X, IDSA, Eclipse Foundation) into binding European normative standards. In this ecosystem, the **Data Spaces Support Centre (DSSC)**—funded under the Digital Europe Programme (DEP) and extended through **DSSC-2 (2025–2029)**—serves as the primary pre-standardization incubator, directly feeding its technical blueprints and building blocks into the formal deliverable workflows of JTC 25 and ETSI TC DATA.

4.1.3. Enforcing Institutional Trust, Data Provenance, and Compliance Liabilities (Challenge 3.3)

Trust is the cornerstone of the data space model, providing the primary technical framework to resolve compliance liabilities and provenance risks. Data spaces integrate trust natively by enforcing mutual counterparty identity assertion, compliance verification against reference architectures, and non-repudiable transaction logging.

Every interaction—from catalogue discovery and contract negotiation to actual payload transfer—generates cryptographic audit logs recorded via distributed registries or immutable transaction logging services. Data providers obtain verifiable, legally binding proof of which counterparty accessed specific product attributes, at what exact timestamp, and under which ODRL contract terms. This deterministic provenance framework eliminates data tampering risks, counteracts greenwashing liabilities, and protects against unauthorized industrial data harvesting.

4.1.4. Transition to FAIR and Cryptographically Verifiable Product Intelligence

Through this integrated backbone, product data transitions from static, document-based declarations into FAIR (Findable, Accessible, Interoperable, Reusable) and cryptographically verifiable digital product intelligence. Applying FAIR principles to product data payloads is insufficient; making the underlying semantic artifacts (vocabularies, ontologies, application profiles, schemas and mappings) FAIR is the foundational mechanisms enabling seamless cross-domain interoperability.

¹² https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202302854

A DPP payload achieves true interoperability only if the model it conforms to is itself Findable (registered in a vocabulary hub), Accessible (resolvable IRIs, documented API), Interoperable (aligned with adjacent models via published mappings) and Reusable (governed by clear licensing, versioning, provenance). As specified in the DSSC Blueprint¹³, FAIR principles must apply directly to “the operational specifications of the data spaces themselves”. Federated data space catalogues leverage these FAIR semantic artifacts to enable programmatically discoverable product twin endpoints. Querying systems execute event-driven calls to retrieve real-time, multi-source lifecycle updates directly from the authoritative source systems, eliminating the need to copy raw records into centralized repositories.

4.1.5. Publishing and Reusing Semantic Models: The Vocabulary Service

Deploying FAIR semantic assets (Section 4.1.4) requires an addressable, governed registry where models can be published, maintained and reused. According to the DSSC Blueprint, this is the role of the Vocabulary Service, which hosts the vocabularies, ontologies, application profiles, schemas and mappings on behalf of participating data spaces. Concrete reference implementations serving the DPP ecosystem include the IDTA semantic repository (publishing AAS Submodel templates and concept descriptions) and the cross-project DPP Vocabulary Hub (consolidating CIRPASS-2 and adjacent EU-project vocabularies).

The Vocabulary Service provides persistent identifiers, supports model discovery through shared metadata, and facilitates version and lifecycle management. By maintaining reusable cross-model mappings over time, it enforces semantic continuity across multi-tier value chains, operationalizing the public disclosure mandates established under Article 33(b) of the EU Data act.

4.1.6. Strategic Value Extension: Unlocking Voluntary B2B Data Monetization

Establishing a trusted, semantically enabled, and sovereign B2B exchange backbone converts the DPP from a regulatory tax under the ESPR into a commercial value engine. Because the data space natively manages counterparty trust, semantic discovery, and policy enforcement, economic operators can utilize the exact same connector network to commercialize non-mandatory, voluntary datasets. Manufacturers, tier-N suppliers, and service providers can deploy fee-based API endpoints, data clean rooms, and subscription services for premium product intelligence—such as real-time battery health telemetry, predictive maintenance algorithms, and circular finance metrics—generating recurring B2B data revenues.

4.2. Data Modelling Paradigms: Structuring Semantic Payloads from DSSC Artifacts to the Asset Administration Shell (AAS)

A core design principle of the IoPD is the absolute separation between the transport governance layer (Data Spaces) and the underlying data payload. Data space connectors operate as format-agnostic exchange mechanisms enforcing usage policies regardless of the specific semantic representation deployed by economic operators.

¹³ <https://blueprint.dssc.eu/?pane=technical&technical=best-practice-defining-data-exchange-protocols>

The architectural framework shown in Figure 5 operationalizes this payload separation by decoupling unique asset identification and granularity mapping (Box 1) from the underlying semantic payload options (Box 2). Economic operators can deploy lightweight W3C JSON-LD domain ontologies or structured Asset Administration Shell (AAS) digital twins based on asset complexity, ensuring full machine interpretability through shared semantic dictionaries and formal IRDI/URI concept registries (Box 3).



Figure 5. Federated Semantic Data Payload Metamodel

4.2.1. Mitigating Semantic Interoperability and System Integration Friction (Challenge 3.2)

Industrial product data originates from disparate, vendor-locked enterprise environments (ERP, PLM, MES, compliance databases) utilizing non-standardized schemas. Exchanging data across value networks traditionally requires bespoke, point-to-point interface mappings creating the prohibitive integration bottleneck.

Decoupling internal data persistence from external data exposure through standardized REST APIs and data space connectors resolves transport-level friction, allowing downstream applications (e.g., recyclers, market surveillance authorities, DPP Providers) to access data endpoints without custom protocol adapters.

However, transport-layer standardization is necessary but insufficient to achieve semantic interoperability. Standardized endpoints and connectors eliminate transport protocol overhead, but semantic-level friction persists unless all participants conform to a shared data model or deploy explicit mediation layers. True semantic alignment requires hosting shared domain models, application profiles, and cross-model mappings within a governed Vocabulary Service, completing the stack necessary to interpret product data across heterogeneous enterprise systems without semantic degradation.

4.2.2. Semantic Anchoring: Concept Descriptions and Standardized Dictionaries

A structural container alone is insufficient to guarantee machine interpretability; consuming applications must understand the exact domain context of each data attribute. Semantic anchoring bridges payload representations directly within the four-level DSSC stack (section 4.1.2) by binding data elements to standardized dictionaries, formal ontologies and concept registries.

- **Persistent Concept Anchors (IRDI and IRIs):** International Registration Data Identifiers (IRDIs, e.g., ECLASS, IEC CDD) and persistent IRIs serve as universal concept anchors across vocabularies, ontologies and application profiles. Within industrial digital twin models, like AAS, every property is bound via semanticId to a globally resolvable IRDI or IRI, pointing to a ConceptDescription that carries a formal data specification (e.g., IEC 61360) defining units, data types, and explicit semantic definitions.
- **Machine-Executable Context:** When a DPP consumer queries an AAS Submodel via a data space connector, explicit semantic references travel alongside the dataset. This enables automated machine-to-machine validation, allowing downstream algorithms to verify compliance thresholds (e.g., ESPR recycled plastic minimums, REACH chemical limits or primary PCF values) without human intervention or manual data re-interpretation.

4.2.3. Multi-Granularity Digital Twins: Model, Batch, and Serialized Item Payloads

Regulatory compliance under the ESPR requires managing product data across distinct granularities: **Model/Type level** (e.g., general product line specifications), **Batch level** (e.g., chemical or alloy production lots), and **Item/Instance level** (e.g., unique serialized assets like EV batteries or industrial machinery).

However, operationalizing this granularity exposes a critical identification friction in commercial trade: **the Sales-Unit vs. Physical-Asset discrepancy**. Standard commercial identifiers (e.g., GTINs, standing for Global Trade Item Number) typically identify the stock-keeping unit (SKU) or sales unit (e.g., a multi-pack containing three physical products plus packaging) rather than individual physical assets inside the bundle. This creates structural ambiguity when mapping ESPR product requirements alongside Packaging and Packaging Waste Regulation (PPWR) obligations. Thus, structured digital twin metamodels like AAS natively supports this hierarchical structure through linked payloads:

- **Type AAS:** Identified via AssetInformation/assetKind = Type, contains immutable design parameters, material declarations, and baseline compliance certificates applicable to an entire product family.
- **Instance AAS:** Identified via AssetInformation/assetKind = Instance, inherits Type AAS attributes while dynamically capturing individual asset events—such as operational telemetry, maintenance records, part replacements, and state-of-health updates—throughout the product’s operational life.
- **Batch AAS:** Identified via AssetInformation/assetKind = Batch, capturing attributes shared by all items produced within the same production or manufacturing lot - such as batch-level composition, processing parameters, or quality data - sitting between the Type AAS (applicable to the entire product family) and the Instance AAS (applicable to a single serialized item).
- **Sales-Unit / Aggregation AAS:** Decouples commercial trade units from physical product payloads by establishing parent-child relationships (ReferenceElement links). The sales unit (GTIN) hosts packaging and distribution metadata, while dynamically referencing the child Instance AAS payloads for the enclosed physical products.

This multi-granularity capability ensures that downstream operators (e.g., repair shops or remanufacturers) can append verified lifecycle events to the Instance payload without corrupting or overriding the manufacturer’s baseline Type data.

4.2.4. Architectural Synergy: The AAS Payload Inside the Data Space Envelope

The synergy between Data Spaces and structured digital twin payloads illustrates the technical core of the Internet of Product Data:

1. **The Data Space (Control Plane)** manages identity authentication, Usage Policy negotiation (ODRL), and transaction logging, governing *who* can access the data and *under what conditions*.
2. **The AAS (Data Plane Payload)** defines *what* data is delivered, exposed through the standardized AAS Repository and Submodel Repository interfaces defined in AAS Part 2, delivering a semantically harmonized, machine-readable digital twin payload structured according to IDTA Submodel Template specifications.

By packaging AAS Submodel queries inside policy-enforced Data Space transactions, the architecture ensures that product intelligence is both **sovereignly governed at the boundary and instantly usable at the destination**.

4.2.5. Implementation Pattern: Realizing the Digital Product Passport within AAS

In domain ecosystems that select asset-centric digital twin architectures (such as industrial equipment, automotive, or smart manufacturing), the Asset Administration Shell (AAS) provides a standardized implementation pattern to encapsulate the Digital Product Passport without requiring an ad-hoc data format. This pattern operates in full alignment with the payload-agnostic principles of the Internet of Product Data, serving as a domain-specific realization alongside ontology-based models (JSON-LD/ RDF).

Attribute-level mapping: Core DPP identity and status attributes map directly onto existing AAS elements:

- The DPP identifier corresponds to the AAS id.
- The unique product identifier corresponds to AssetInformation/globalAssetId.
- The DPP's granularity (model, batch, or item-level) corresponds to AssetInformation/assetKind (see Section 4.2.3).
- The last-updated timestamp corresponds to the updatedAt attribute in Administrative Information.

The remaining DPP-specific attributes - status, schema version, and the identifiers of the economic operator and facility responsible for the product - are not native AAS elements. IDTA addresses this with a dedicated DppMetadata Submodel (IDTA 02099-1)¹⁴, which carries these attributes and acts as a wrapper around the regulation-specific content submodels that make up the rest of the passport. This keeps the DPP payload fully native to the AAS structure: no parallel data format is needed alongside it, and the passport can be retrieved through the same standardized AAS interfaces described in Section 4.2.4. Full technical detail on the retrieval interfaces is available in the AAS Part 2 API specification.

Linking the DPP to regulation-specific submodels: The DPP Metadata Submodel references the set of regulation-specific submodels included in a given passport via a content-specification field. Since

¹⁴ International Digital Twin Association (IDTA): "IDTA 02099-1: Digital Product Passport - Part 1 Metadata" (May 2026). Available at https://industrialdigitaltwin.org/wp-content/uploads/2026/05/IDTA-02099-1_Submodel-Digital-Product-Passport-Part-1.pdf

the exact format of this reference is left open by the DPP data model, IDTA recommends using the semanticId of the relevant Submodel Template Specification as the reference value - giving it a globally resolvable, standards-based identity rather than a proprietary label.

Resolving and assembling a passport: Figure 6 illustrates one way this resolution and assembly can happen in practice: a DPP client resolves a product identifier to its AAS via the AAS Discovery Service, retrieves the AAS descriptor and its Submodel endpoints from the Registry Service, fetches the DppMetadata Submodel to identify the relevant content submodels, and retrieves each of those submodels in turn before assembling the complete passport document. The full set of interaction patterns is defined in the AAS Part 2 API specification.

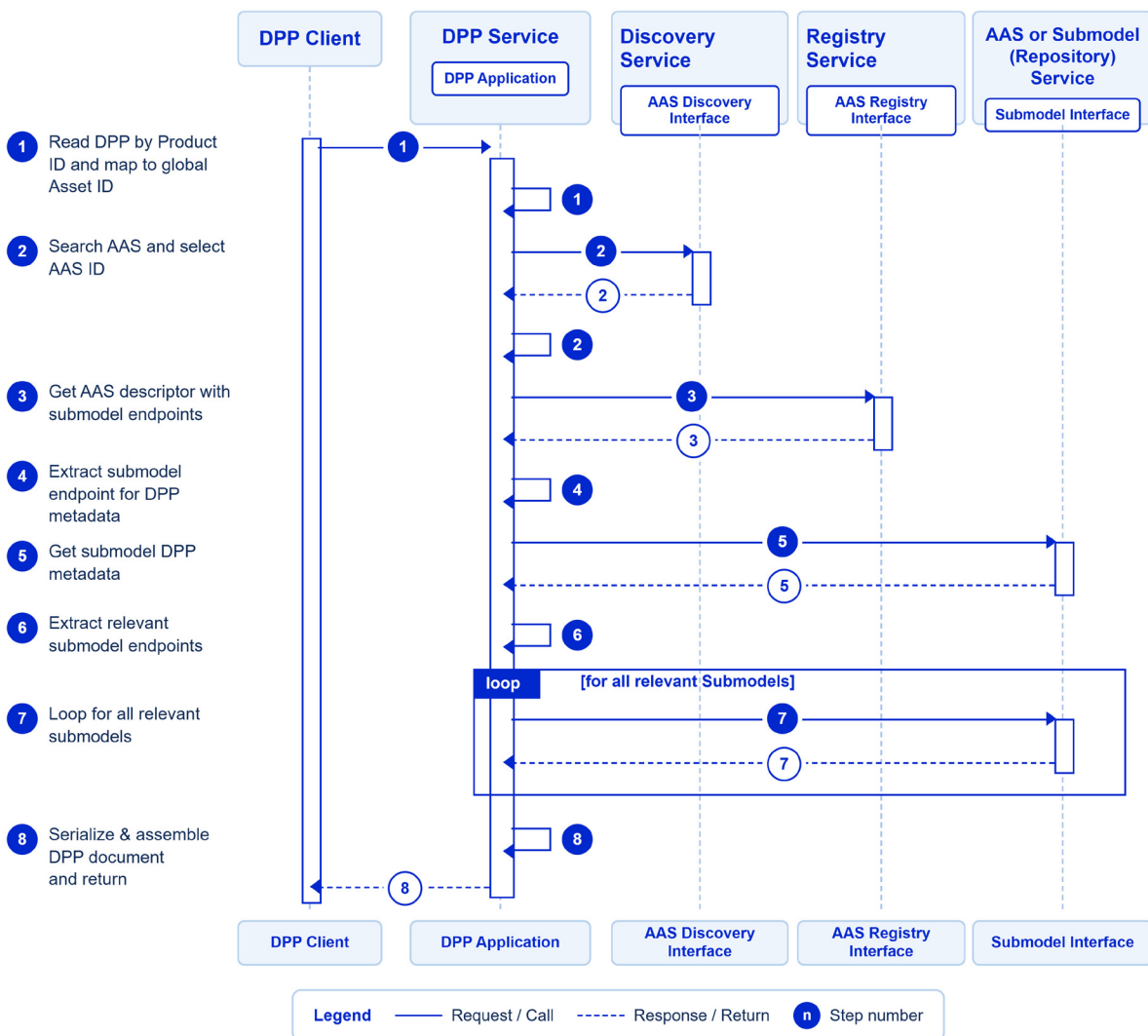


Figure 6. Implementation Pattern for AAS-Based DPP Resolution and Assembly¹⁵

¹⁵ Execution sequence illustrating how application-layer services resolve product identifiers to retrieve and serialize AAS-structured submodels when economic operators deploy the Asset Administration Shell as an optional digital twin payload model. Operating across standard AAS Part 2 interfaces (Discovery, Registry, and Submodel Repository Services), the client queries the DppMetadata wrapper submodel (IDTA 02099-1) to dynamically identify, fetch, and assemble regulation-specific content submodels into a unified passport payload. (Source: Adapted from IDTA-01002, Asset Administration Shell Specification – Part 2: Application Programming Interfaces, v3.2).

4.3. Trust and Identity Frameworks: From Hierarchical PKI to Decentralized Verifiable Credentials

Data governance and semantic harmonization are ineffective if ecosystem participants cannot verify counterparty identity, issuer authorization, and payload authenticity. To eliminate reliance on centralized identity providers or manual compliance auditing, the IoPD architecture accommodates a progressive trust continuum—bridging traditional hierarchical Public Key Infrastructures (PKI) with decentralized, eIDAS 2.0-aligned European Business Wallets (EBWs) and W3C Verifiable Credentials (VCs). Bridging Hierarchical PKI (X.509) and Decentralized eIDAS 2.0 EBWs.

Establishing trust in B2B federated networks requires distinguishing between network transport security and legal organizational identity:

- **Hierarchical PKI & X.509 Certificates (Baseline Transport Trust):** Traditional X.509 certificates issued by centralized Certificate Authorities (CAs) serve as a legacy baseline for establishing secure point-to-point communication channels (e.g., mutual TLS between Data Space Connectors). While effective for transport-layer encryption, centralized PKI structures introduce single-point-of-failure vulnerabilities, administrative overhead, and vendor lock-in when scaling across multi-tier cross-border value chains.
- **eIDAS 2.0 European Business Wallets (Decentralized Governance Target):** To achieve true identity sovereignty, the IoPD leverages the eIDAS 2.0 framework via European Business Wallets (EBWs). EBWs provide a decentralized mechanism for economic operators to manage organizational identities, present digital mandates, and issue Qualified Electronic Seals (e-Seals) onto DPP declarations. This mechanism cryptographically binds product claims directly to the legal identity of the enterprise, establishing strict non-repudiation and legal liability under European law without central authority bottlenecking.

4.3.1. Verifiable Credentials & DIDs: Payload Integrity and Portable Claims

VCs and Decentralized Identifiers (DIDs) establish cryptographic trust at the **attribute and assertion level**. VCs enable lifecycle declarations—such as REACH compliance certificates, recycled content percentages, or carbon footprint calculations—to be issued as portable, tamper-evident digital objects.

When a downstream actor or market surveillance authority queries a product attribute, the payload is delivered alongside a cryptographic proof. Receiving systems independently verify that the attribute has not been altered in transit and that the issuing key matches an authorized issuer, eliminating the need for bilateral database integrations or manual conformity audits.

4.3.2. The European Blockchain Services Infrastructure (EBSI) as a Trust Registry

To prevent fragmentation and vendor lock-in, this trust architecture is designed to be compatible with the European Blockchain Services Infrastructure (EBSI), while remaining fully aligned with the open, interoperable approach established by the CEN/CENELEC JTC 24 standards and the European Commission's DPP framework. EBSI can serve as a decentralized, EU-operated trust registry for specific supply-chain use cases, hosting decentralized identifiers (DIDs) and public keys to support cross-border resolution and verification of credentials. By designing the DPP ecosystem to be standards-compliant

and infrastructure-agnostic, it can optionally leverage EBSI where appropriate, without relying on private blockchain silos, and in full conformity with the EU's central DPP Registry and the broader set of harmonized EN standards that ensure openness and global interoperability.

4.3.3. Architectural Convergence: Wallets, Connectors, and Payloads

The operational synergy between the trust layer and the data space occurs during session initialization:

1. **Identity Challenge:** Prior to negotiating data access contracts (ODRL), the requesting Data Space Connector presents an organizational Verifiable Credential issued via its EBW (or a validated X.509 assertion during transition phases).
2. **Automated Verification:** The receiving Connector Control Plane validates the credential against federated trust registries (e.g., EBSI or eIDAS Trusted Lists) to verify counterparty identity and legal standing.
3. **Policy Gating:** Access policies are evaluated only after cryptographic counterparty identity is established, ensuring that sensitive data exchange endpoints are never exposed to unauthenticated network actors.

4.4. Semantic Governance: Artifact Lifecycle and Structural Maintenance

Long-lived DPP ecosystems require explicit governance mechanisms extending beyond transport security and counterparty trust. The long-term interpretability of product passports depends on the institutional governance of the semantic artifacts—vocabularies, ontologies, application profiles, schemas, and mappings—that define payload context. Without structured semantic governance, domain models inevitably diverge over multi-decade asset lifecycles, triggering mapping obsolescence, breaking M2M integrations, and rendering historical passport data uninterpretable.

Operationalizing semantic governance requires managing four technical dimensions:

- **Versioning and Backward Compatibility:** Enforcing strict semantic versioning (SemVer) and deprecation protocols to guarantee that historical passport assertions remain resolvable and legally binding across regulatory revision cycles.
- **Cross-Model Mapping Stewardship:** Maintaining machine-executable transformation rules and alignment graphs within Vocabulary Services to sustain interoperability between evolving sectoral ontologies (e.g., CIRPASS-2, IDTA AAS Submodels, GTS).
- **Institutional Custody and Change Management:** Establishing clear custodian roles, open RFC processes, and structural change boards responsible for validating schema extensions without creating domain silos.
- **DSSC Building Block Alignment:** Decoupling the governance of static semantic specifications from the operational processes that drive their evolution, in strict accordance with the DSSC Data Models Building Block.

Systematizing these governance protocols prevents semantic fragmentation, minimizes multi-tier integration overhead, and ensures that dynamic product intelligence remains FAIR across the entire lifecycle.

4.5. Exploiting Data with DPP Applications: The Value Creation Layer

The ultimate ROI of the Internet of Product Data extends far beyond passive regulatory compliance under ESPR. Once industrial product data is sovereignly governed (Data Spaces), semantically harmonized via Domain Ontologies or AAS) and cryptographically anchored (via EBWs or PKI), top-tier software applications can programmatically consume it. Decoupled from physical data management, the DPP transforms into an extensible digital infrastructure for data-driven innovation, circular business models and AI-powered industrial analytics.

Figure 7 details the structural mapping between top-tier value creation domains—Circular Models & Servitization (Section 4.5.2), AI Readiness & Industrial Intelligence (Section 4.5.3), and Sovereign Data Monetization (Section 4.5.4)—and the underlying federated B2B infrastructure layer. Standardized REST APIs and semantic query interfaces decouple top-tier software applications from underlying data spaces, which enforce usage policies (ODRL) over modular semantic payloads (JSON-LD ontologies or AAS) and identity frameworks (EBWs, VCs, or PKI).

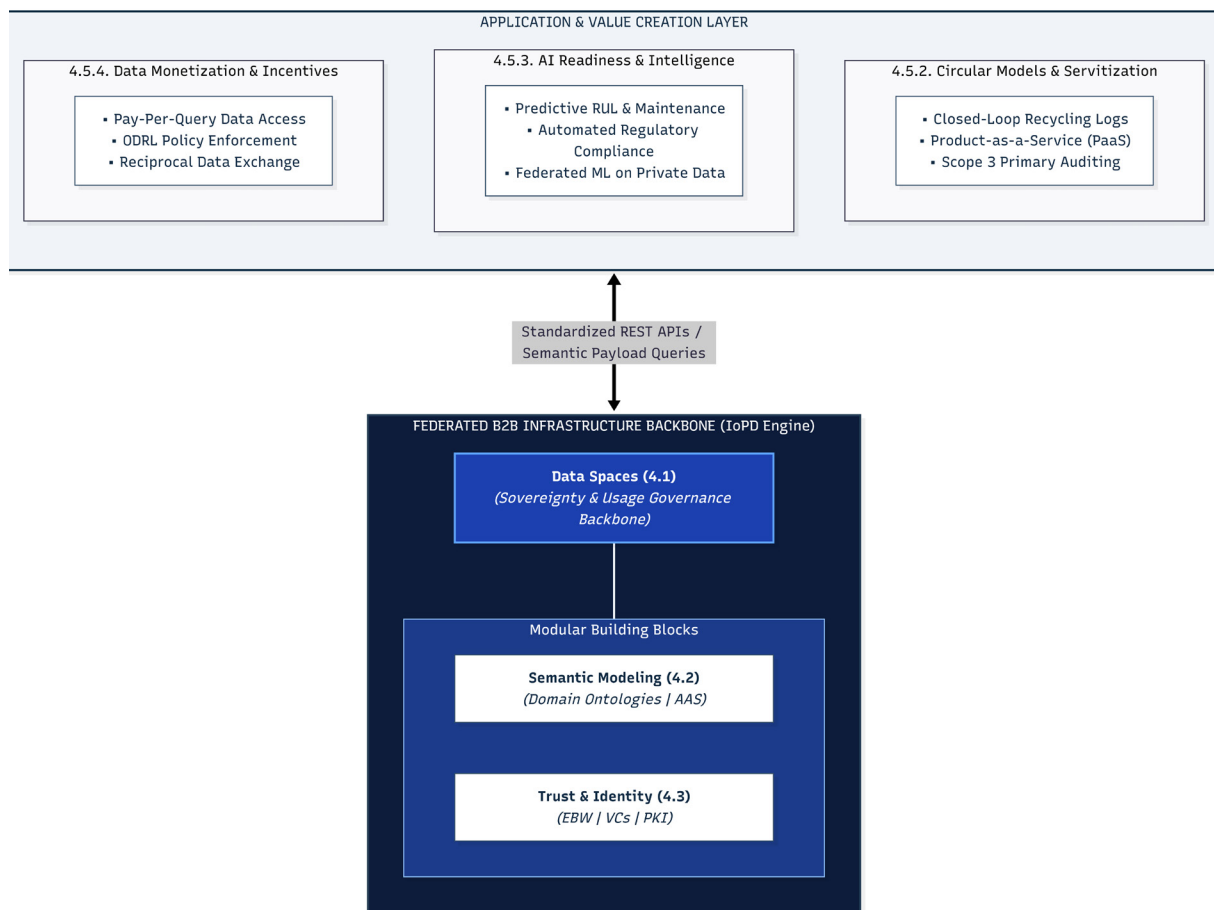


Figure 7. Decoupled IoPD Application and Value Creation Layer

4.5.1. Decoupling Infrastructure Backbone from Application Interfaces

The IoPD architecture enforces strict separation between the federated B2B infrastructure layer and application-level interfaces. Software vendors, DPP Providers, OEMs, and public bodies build application portals, market surveillance tools and analytics dashboards that interact with underlying data spaces via standardized REST APIs, GraphQL endpoints, and semantic query protocols.

This API-driven decoupling guarantees two key operational outcomes:

- **Preventing Platform Lock-in:** Economic operators retain complete freedom to swap application providers or internal enterprise systems (ERP, PLM) without migrating core data governance policies or asset identities.
- **Dynamic Attribute Aggregation:** Downstream applications aggregate lifecycle data on demand across multi-tier suppliers—fetching material origins, carbon footprints, or repair histories—while the data space connector transparently enforces usage policies (ODRL) in the background.

4.5.2. Value Creation Beyond Compliance: Circular Business Models and Servitization

While baseline ESPR mandates focus on public compliance declarations, the IoPD enables voluntary B2B value creation across three high-impact industrial domains:

- **Closed-Loop Circular Economy:** Recyclers, remanufacturers, and refurbishers query verified material composition, disassembly sequences, and chemical safety profiles (REACH/PoP) directly from authoritative data providers. This automated verification minimizes manual sorting overhead, optimizes material yield, and guarantees high-grade feedstock recovery.
- **Product-as-a-Service (PaaS) and Servitization:** Manufacturers transition from transactional equipment sales to performance-based contracts. By combining static design attributes (Type data) with dynamic operational telemetry (Instance data), asset managers monitor real-time utilization, enforce usage contracts, and automate preventive maintenance workflows.
- **Scope 3 Decarbonization and Automated Auditing:** Instead of relying on generic secondary databases, enterprises pull primary, cryptographically verified Carbon Footprint (PCF) assertions directly from Tier-N suppliers, eliminating greenwashing risks.

4.5.3. AI Readiness: Enabling Automated Industrial Intelligence

Federated B2B Data Spaces provide the trusted, semantically organized data foundation required to train and deploy Artificial Intelligence (AI) models at scale. By replacing fragmented files and proprietary silos with machine-readable payloads (JSON-LD / AAS), the IoPD enables automated industrial analytics:

- **Predictive Life-Cycle Optimization:** Machine Learning (ML) algorithms analyse operational parameters and stress factors across serialized asset fleets to forecast Remaining Useful Life (RUL) and optimize maintenance schedules.
- **Automated Regulatory Verification:** Semantic reasoning engines match incoming supply chain assertions against updated EU delegated acts, flagging compliance deviations or material toxicity risks automatically.
- **Federated Learning on Confidential Data:** Data space usage policies allow industrial consortiums to train distributed AI models across competitive enterprise datasets without exposing underlying raw trade secrets or proprietary process parameters.

4.5.4. Commercial Value: Service Innovation and Voluntary Data Monetization

Data sharing across competitive supply chains requires explicit economic incentives. The IoPD leverages Data Space policy engines (ODRL) to operationalize voluntary data monetization. Data providers can attach commercial terms—such as micro-payments, pay-per-query access, or reciprocal data exchange agreements—to premium data submodels (e.g., advanced diagnostic algorithms, high-resolution usage logs). Automated smart contracts execute transaction logging and billing upon policy verification, converting regulatory compliance overhead into a recurring revenue stream.

4.6. Reference implementation: The IMX Council Battery DPP Showcase

To validate that the Internet of Product Data (IoPD) architecture is an operational technical reality rather than a theoretical ambition, reference implementations are essential. While Section 5 examines full-scale industrial deployments and commercial use cases, this subsection details the International Manufacturing-X Council (IMXC) Battery DPP Showcase¹⁶, reference implementation presented at Hannover Messe 2026. Anchored in the official IMXC architectural specification, this flagship showcase serves as the primary global testbed, proving cross-border, cross-sector, and multi-domain interoperability across federated B2B value networks.

The methodological progression of the showcase is structured across three core pillars (Figure 8): connecting cross-domain industrial federation (vertical data spaces and global manufacturing hubs) with an open, standardized technical stack (DSP, EDC, ODRL, VCs, and AAS) to achieve empirical validation of a sovereign multi-domain Battery Digital Product Passport.

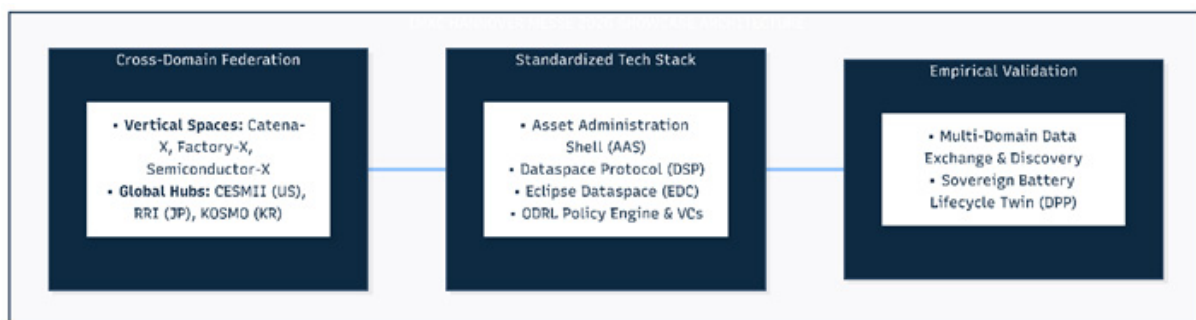


Figure 8. IMXC Showcase Methodological Framework¹⁷

¹⁶ Adapted from International Manufacturing-X Council, 'International Digital Value Creation (DVC) Networks for Manufacturing Competitiveness & Sustainability, White Paper, Hannover Messe 2026. Available at https://imxc.org/wp-content/uploads/IMXC-White-Paper-HM-2026_pdf.pdf

¹⁷ Adapted from International Manufacturing-X Council, 'International Digital Value Creation (DVC) Networks for Manufacturing Competitiveness & Sustainability, White Paper, Hannover Messe 2026. Available at https://imxc.org/wp-content/uploads/IMXC-White-Paper-HM-2026_pdf.pdf

4.6.1. Global Ecosystem Alignment and Cross-Domain Federation

Framed within the international Manufacturing-X initiative, the showcase operationalizes a federated data network connecting major industrial ecosystems across Europe, North America, and Asia. Architecturally, the IMXC specification addresses a fundamental challenge in global value chains: **cross-domain data space interoperability**.

Rather than confining product data to vertical industry silos, the showcase demonstrates seamless data exchanges between distinct domain data spaces (e.g., extracting semiconductor compliance data from Semiconductor-X¹⁸, machine operational logs from Factory-X¹⁹, and battery manufacturing parameters from Catena-X²⁰). By enforcing the open Dataspace Protocol (DSP) as the core usage governance backbone, the network achieves global federation without requiring participants to adopt proprietary platforms or centralize data storage.

4.6.2. End-to-End Interoperability Stack and Execution Flow

The IMXC reference implementation validates the complete IoPD execution stack by orchestrating cross-domain industrial data spaces—such as Catena-X, Factory-X, and Semiconductor-X—through a decoupled control and data plane topology (Figure 9). By bridging shop-floor data ingestion with sovereign B2B exchanges, this execution flow operationalizes real-time product twins across four integrated stages:

1. **Shop-Floor Ingestion & Edge Abstraction:** Industrial machinery streams operational parameters via OPC UA protocols directly into enterprise systems (ERP/PLM).
2. **Semantic Structuring via IDTA Submodels:** Data payloads are packaged into standardized Asset Administration Shell (AAS) submodels (Digital Nameplate, Carbon Footprint, State-of-Health).
3. **Policy Negotiation and Sovereign Transfer:** EDC connectors negotiate machine-executable usage constraints in ODRL prior to peer-to-peer data plane transfer.
4. **Decentralized Identity & Trust Assertion:** Organizational identities and assertions are cryptographically anchored using Verifiable Credentials (VCs) and DIDs.

¹⁸ <https://www.semiconductor-x.com/>

¹⁹ <https://factory-x.org/>

²⁰ <https://catena-x.net/>

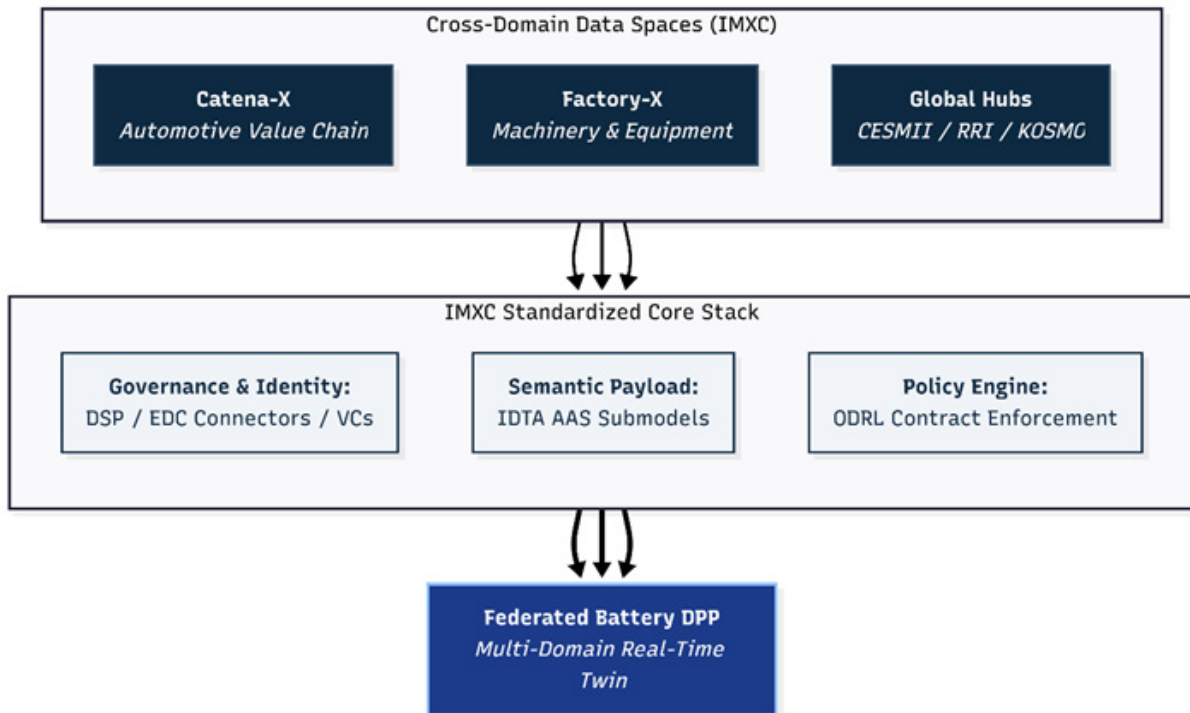


Figure 9. IMXC Technical Interoperability Stack and Execution Topology²¹

4.6.3. Strategic Key Takeaways for Industrial Scaling

The IMXC showcase presented at Hannover Messe 2026 establishes crucial empirical benchmarks for scaling the Digital Product Passport under the ESPR:

- **Validation of Open Standards:** Confirms that open, non-proprietary standards (DSP, AAS, ODRL, VCs) are mature enough to replace monolithic compliance platforms.
- **Scalability Across Supply Chain Tiers:** Demonstrates that Tier-N suppliers can participate in multi-national passport ecosystems without exposing trade secrets or supplier-customer relationships.
- **Industrial Blueprint for EU Compliance:** Provides a validated, repeatable technical blueprint for economic operators preparing for mandatory battery and industrial product passports across European and global markets.

²¹ Adapted from International Manufacturing-X Council, 'International Digital Value Creation (DVC) Networks for Manufacturing Competitiveness & Sustainability, White Paper, Hannover Messe 2026). Available at https://imxc.org/wp-content/uploads/IMXC-White-Paper-HM-2026_pdf.pdf

5. DPP Practical implementations with Data Spaces

The following use cases illustrate different ways in which sectoral data spaces can support DPP-related information flows. They should be understood as complementary industry implementations rather than as competing or prescriptive architectures. Their longer-term scalability depends on their ability to interoperate across sectoral and organisational boundaries.

5.1. The Tyre Industry Use Case: Lifecycle Data Sharing

The tyre DPP pilot in the CIRPASS2 project²², described in Figure 10, explores how an existing industry data space can support the exchange of tyre lifecycle information and create value across multiple stages of a tyre's life. The pilot builds on the Global Data Service Organisation (GDSO), an industry-led initiative established to standardise tyre data and facilitate its access and exchange, and on the Tyre Lifecycle Data Service (TLDS) connector.

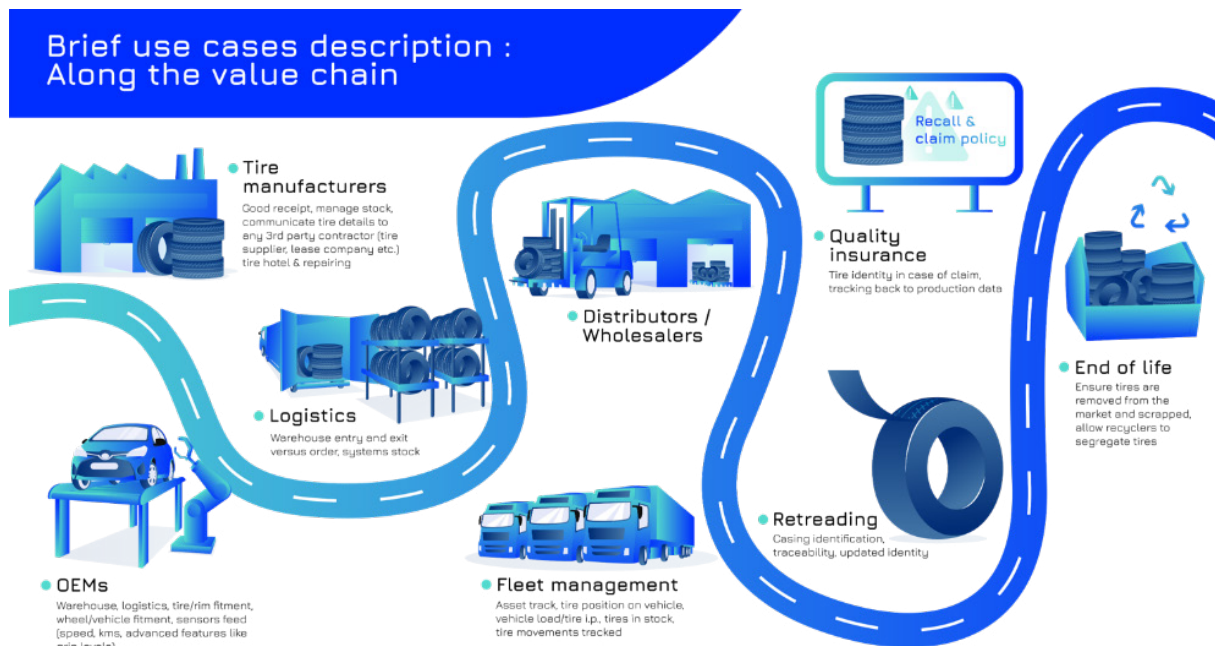


Figure 10. CIRPASS2 Tyre Industry Use Case description

This industry initiative and its data services were developed independently of, and ahead of, the final regulatory requirements for the tyre Digital Product Passport under the ESPR.

The objective of the pilot is to demonstrate how sharing standardised lifecycle data may create value for different stakeholders across the tyre value chain (Figure 11). The pilot should be understood as an exploration of the value and practical implications of lifecycle data sharing, rather than as an endorsement of GDSO or TLDS as the regulatory implementation of the future tyre DPP. The applicable EU requirements for tyres will depend on the relevant ESPR delegated act and subsequent implementation measures.

²² CIRPASS2 Tyre Digital Product Passport, available at <https://cirpass2.eu/pc1-michelin/>

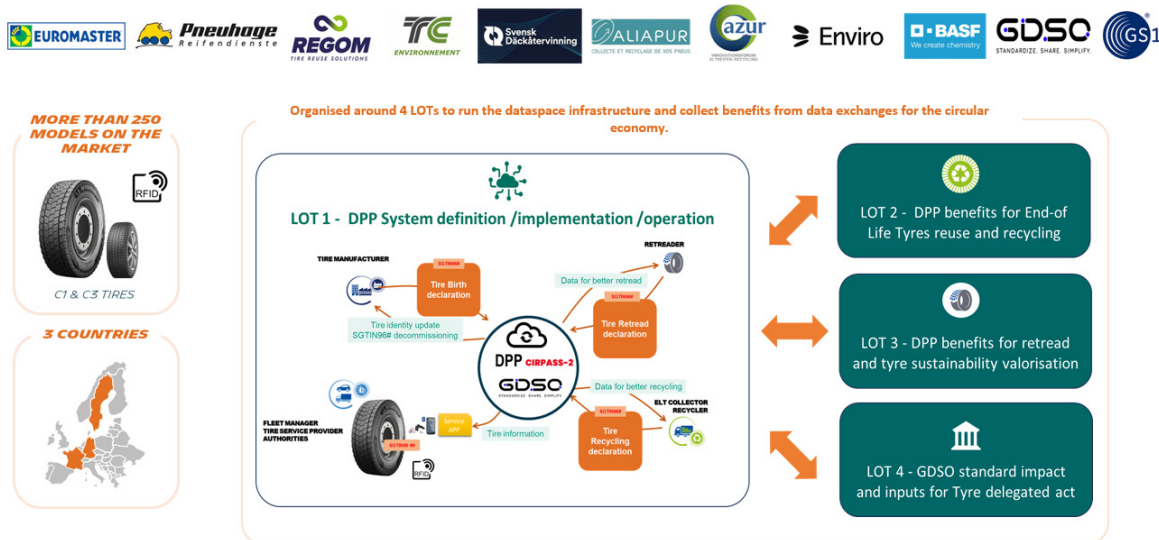


Figure 11. CIRPASS2 Tyre Industry Use Case: DPP System Definition, Implementation and Operation

5.1.1. Strategic focus and lifecycle scope

The pilot addresses the strategic need to maintain the tyre identity and history after major events occurring in the real world, including reuse, retreading, collection and end-of-life treatment. Using the TLDS, the use case follows the tyre from manufacture through subsequent lifecycle events, supporting multi-life scenarios rather than a single linear product life. Lifecycle transitions are represented through standardised declarations or events associated with authorised participants in the data-sharing environment. This event-based approach provides a persistent link between the physical tyre identity and relevant lifecycle information. Such information could support future DPP use cases, subject to the final regulatory and technical requirements. The purpose of this approach is not simply to reproduce information already held by individual organisations, but to explore whether making selected lifecycle information available to authorised stakeholders can generate operational, circular-economy and information value (Figure 12).

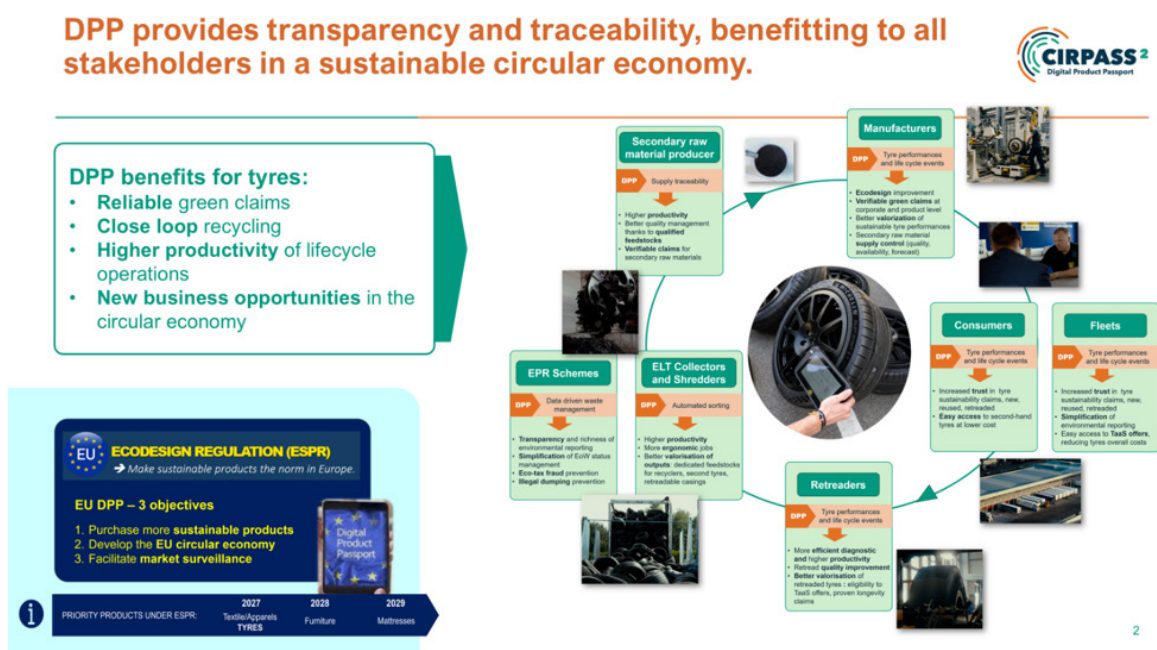


Figure 12. CIRPASS2 Tyre Industry Use Case: DPP Benefits for tyres

5.1.2. Actors, roles and data space architecture

GDSO defines three core roles—manufacturers, readers and end of life tyre (ELT) operators—who act as both data providers and consumers within the tyre data space. As depicted in Figure 13, the pilot ecosystem includes a representation of ELT collectors and shredders, recyclers producing secondary raw materials, EPR organisations, and service providers such as REGOM offering automated ELT sorting connected to GDSO services. GDSO provides an industry governance framework for the relevant data and access rights of the data space through bylaws, rules of procedure and service terms of use, while **GS1** contributes to identification standards; fleets, dealers, e retailers and consumers access tyre information indirectly via the other connector Tyre Information Service (TIS), in production since 2022.

Tyre DPP pilot architecture – Test interoperability between CEN/CENELEC DPP standards and data space building blocks.

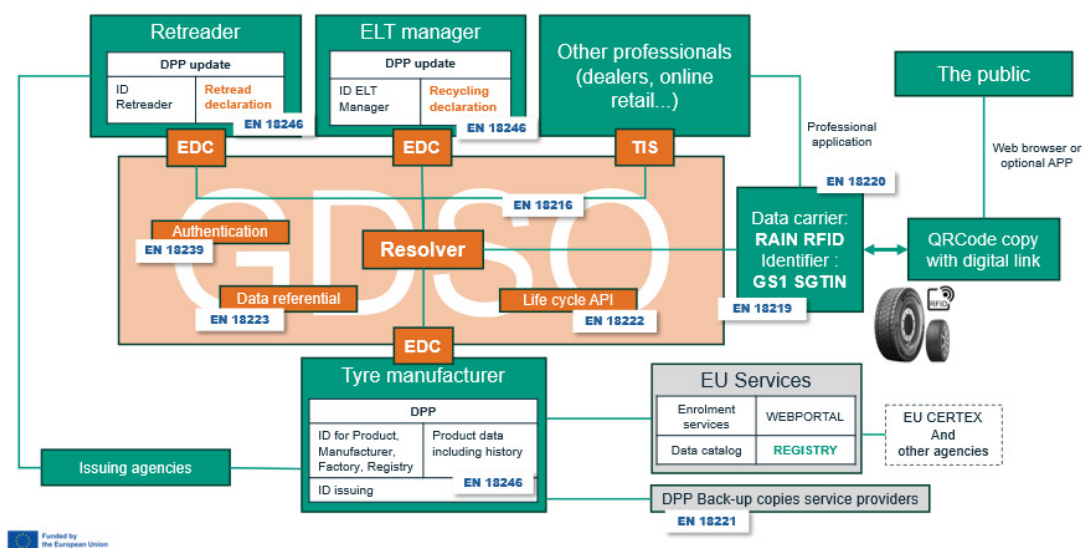


Figure 13. CIRPASS2 Tyre Industry Use Case: Tyre DPP Pilot Architecture

5.1.3. DPP content, identification and access via the data space

The pilot uses the TLDS data model to represent the tyre identity and the lifecycle information, covering most of the data needed by the involved tyre industry stakeholders and it can be aligned with evolving EU DPP mandatory fields. Data are structured across model level (regulated performance and product attributes), batch level (production data such as date and composition) and item level (individual lifecycle events and aftermarket configurations), supporting both model centric and item centric DPP views.

GDSO Services are designed as an industry standard where individual tyres are uniquely identified using the GS1 SGTIN 96 coding. For the tyre pilot a persistent RAIN RFID tag following ISO 20909/20910²³ and EN 18229 scheme 4 was selected as data carrier with QR codes optionally used on invoices; stakeholders in the tyre pilot can access full tyre information, while it is foreseen that in production item level data will be restricted to actors with legitimate interest to be defined by the future ESPR tyre delegated act.

²³ ISO 20909:2019: Radio frequency identification (RFID) tyre tags. Available at <https://www.iso.org/standard/69435.html>

The use case therefore illustrates an important data-space principle: the objective is not necessarily to place all product information in a single central repository, but to enable authorised stakeholders to obtain relevant information from the appropriate source. The specific data fields, access rights and technical implementation required for the future regulatory tyre DPP will depend on the applicable EU regulatory and standardisation framework.

5.1.4. Activities, use cases and benefits enabled by data spaces

The relevance of the tyre case to the DPP discussion lies primarily in what can be done with shared lifecycle data. The pilot is running to illustrate potential value in three complementary areas:

- **Operational value:** better retreading decisions, diagnostics, fleet management, identification of valuable casings, inventory management and more efficient ELT logistics.
- **Circularity value:** support for reuse and retreading, improved sorting of end-of-life tyres, more homogeneous recycling batches, and improved quality control for secondary raw materials.
- **Information and compliance value:** support for waste management and EPR reporting, improved traceability, evidence for eco-design and sustainability communication, and potential future data-enabled “tyre-as-a-service” based on robust digital identity and history.

These examples should be read as use cases and potential sources of value enabled by access to trusted lifecycle information, while quantitative benefits have not been measured by the pilot yet. Instead, the advantages of the technical choices made in the pilot for implementing the DPP entail the following:

First, a product identification scheme (not a DPP one) that supports all use cases requiring access to tire information to maximize the return on investment related to RFID, whether it’s the cost of the tag itself or the reading systems. The goal is to avoid the proliferation of data carriers on the same tire or the fragmentation of identification solutions in the industry, which represent additional costs for all.

Second, the innovative implementation of a data space to pool access management and service maintenance tasks. A huge gain in efficiency, compared to a situation where we would all have to manage the identification of rights holders, user support, API maintenance, data models, dictionaries, etc., ourselves. Tyres compliant to DPP becomes automatically eligible to services supported by the GDSO beyond ESPR

Finally, a deliberate choice to rely on tyre industry standards for both electronic identification and access management, in order to preserve the independence of after-sales players, particularly with regard to manufacturers’ proprietary networks, and to provide long-term investment confidence to the value chain.

5.1.5. Challenges and roadmap for scaling

The main challenges include closing data gaps, harmonising semantic models (e.g. GDSO ontologies), integrating legacy systems, establishing appropriate governance and access rights, and maintaining incentives for stakeholders to contribute and update lifecycle information.

TLDS offers unlimited access to tyre data for retreaders and ELT collectors on the condition that they actively feedback updating lifecycle information, aligning economic motivation with data space participation. The TLDS is planned to go live globally in 2027, ahead of the expected EU tyre DPP obligation around 2028/29, representing one sectoral building block in a wider interoperable required ecosystem with other manufacturing and mobility data spaces.

Indeed, the tyre industry data space should not be considered an isolated vertical data silo. Its longer-term value depends also on interoperability with adjacent sectoral data spaces, allowing relevant information to flow across organisational and industry boundaries while preserving data sovereignty, access control and the authority of the respective data sources.

5.2. Textile Industry Use Cases

While data space technology remains a novel and largely unfamiliar concept to the broader textile sector, its potential to transform the industry's fragmented digital landscape is immense. Historically reliant on isolated systems, manual reporting, and limited supply chain visibility, the textile ecosystem now faces mounting pressure from evolving EU mandates—such as Ecodesign for Sustainable Products Regulation (ESPR) and Extended Producer Responsibility (EPR).

Within the SAGE project (Data Space for a Sustainable Green Europe), Recognizing that traditional point-to-point connections cannot scale to meet these complex compliance demands, forward-thinking industry frontrunners and technology pioneers—including entities like Reverse Resources, Texroad, reverse.fashion, Avery Dennison, Erion, and GS1—have stepped forward within the SAGE project to proactively test green data space infrastructure for the sector. **Textile Circularity** use case is exploring how to use a federated Green Deal Data Space (GDDS) architecture to bridge supply chain silos, streamline compliance, and keep material resources in continuous circulation and demonstrates how secure, sovereign data sharing can convert regulatory burdens into operational efficiency, trust, and and profitable circular business models.

The CIRPASS2 project advances the EU Digital Product Passport (DPP) for textiles through six complementary pilots that span workwear, apparel and footwear, bedding, and mattresses. Led by IOXIO, the Circular Workwear pilot models data needs across the full value chain to enable reuse, repair, remanufacture and recycling via DPPs. KEZZLER demonstrates item-level Connected Product Management to support circular business models and EU DPP compliance for both SMEs and large operators. EON scales circular systems with a global apparel brand, focusing on resale, repair and recycling while feeding event data back into the DPP. Avery Dennison's atma.io drives a Textile Loop that assigns unique digital IDs and tracks products through sorting, repair, upcycling and recycling services. TripleR.io deploys MattressID with five European manufacturers to enable refurbishment and improved dismantling for recycling. Finally, Scantrust proves that textile SMEs can issue DPPs on down-feather bedding and measure positive impacts on circularity economics. However, only IOXIO's DPP use case includes a data space, the other textile use cases using other technologies for its DPP developments.

In the SM4RTENANCE project, the use case led by PIACENZA 1733 is aligned with the SAGE finding that fragmented, point-to-point data exchange cannot scale to meet the textile sector's compliance demands, while extending the analysis further upstream, to the manufacturing tier that directly supplies the brands.

Piacenza Group, a fine-wool manufacturer based in Biella, Italy, supplying leading fashion and luxury houses, and coordinator of the Horizon 2020 TRICK²⁴ project, is piloting a Minimum Viable Data Space connecting its own production entities, Piacenza and Cerruti, which continuously exchange spinning, weaving and finishing capacity for the same production lots. The structure of the pilot addresses the complexity to manage the sustainability and compliance data collection and management when subcontracting is adopted, which is the a widely common business model in textile, for more than 90%

²⁴ www.trick-project.eu

formed by SMEs with an average dimension of 10 employees. Piacenza and Cerruti are part of the same group but well represent the needs and problems of the sector because the last one has been acquired by Piacenza in 2022 and its IT infrastructure and legal entity is fully separated from Piacenza. In addition, both Piacenza and Cerruti exploit additional subcontracting from suppliers outside the group in the case of small lots, where internal production is not convenient.

SM4RTENANCE pilot, “Optimization of Production Performance through DPP”, integrates standardised DPP data into the existing **TRICK** platform developed in TRICK project demonstrate that both product and asset circularity can be managed through a single data backbone. This upstream, supplier-side perspective is precisely the segment CIRPASS2 identifies as the least covered by current DPP practice. It also surfaces a structural driver: individual brands impose their own proprietary data requirements, forcing manufacturers such as Piacenza to build a dedicated data-collection workflow per client, multiplying IT costs and compressing seasonal deadlines; the burden compounds further down the chain for Tier-2/3/4 SME suppliers, and again downstream where e-commerce platforms request DPP data item by item.

A single, standardized, federated data space—as piloted between Piacenza and Cerruti and designed for future extension to raw-material and yarn suppliers—is the only sustainable route to reconcile brand-level compliance demands with the economics of a highly fragmented, SME-dominated value chain. As illustrated in Figure 14. SM4RTENANCE Textile Value Chain Data Exchange: Chaotic Many-to-Many Interfacing vs. Federated Data Space Repository., replacing chaotic many-to-many bilateral integrations with a federated data space architecture drastically reduces complexity in deeper supply chain tiers (Tier 4 to Tier 1), operationalizing a ‘collect once, use many times’ paradigm where suppliers upload verification evidence a single time for all downstream clients.

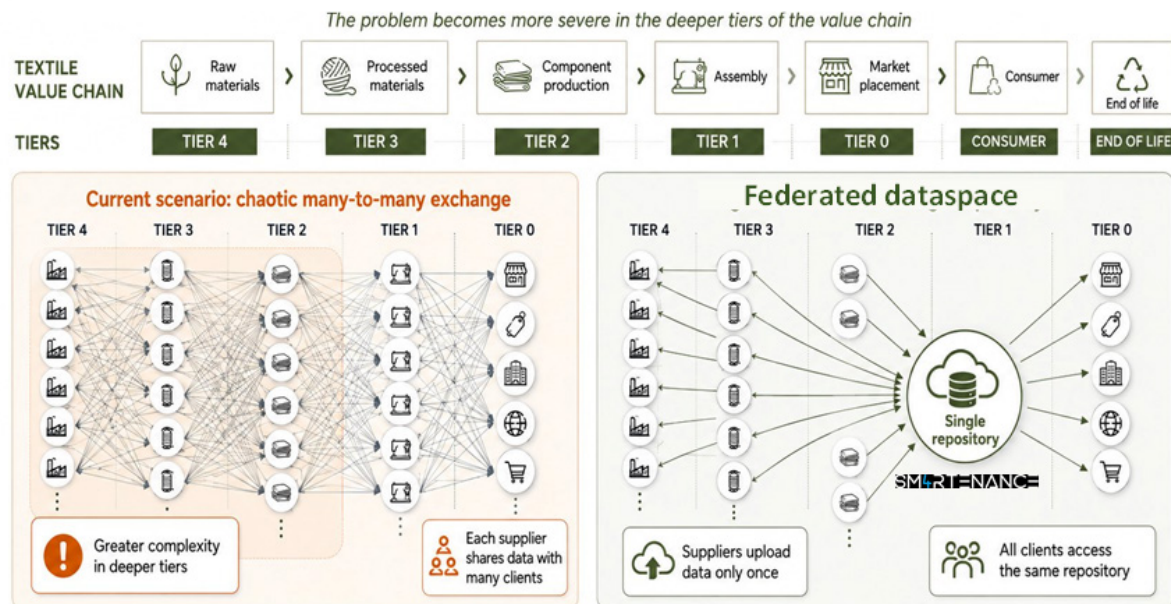


Figure 14. SM4RTENANCE Textile Value Chain Data Exchange: Chaotic Many-to-Many Interfacing vs. Federated Data Space Repository.

5.2.1. Strategic focus and lifecycle scope

From the SAGE project perspective, the strategic focus of Circular Textiles Data Space use case is to operationalize interoperable, decentralized data-sharing network across the European textile value chain. Strategically, it shifts the market away from fragmented, manual point-to-point reporting toward a sovereign “collect once, use many times” architecture. Data spaces could offer a cost-effective, scalable trust infrastructure for European micro-SMEs (which comprise 89% of the sector) to comply with emerging JTC 24 interoperability norms. Standardizing access technology reduces integration friction for legacy, sector-specific IT vendors serving this market.

On the other hand, across all CIRPASS2 pilots, the strategic focus is to operationalize the DPP as an enabler of circular business models and regulatory compliance, with lifecycle coverage from design and production to distribution, use, collection, sorting, refurbishment/repair, and recycling. Thus, the lifecycle scope of Textile Use Case covers the complete circular loop of textile products, connecting every stage of the value chain into a continuous data ecosystem.

- **Upstream Manufacturing:** Encompasses raw material extraction, fiber production, yarn spinning, textile manufacturing, product assembly, and brand distribution.
- **Use & Circular Extension:** Tracks consumer use, repair, maintenance, upcycling, resale, and redistribution loops.
- **Post-Consumer & Recycling:** Captures waste collection, automated sorting, reuse processing, pre-processing, and mechanical or chemical recycling back into secondary raw materials.

In the SM4RTENANCE project, the use case led by PIACENZA 1733 confirms the strategic focus, shifting away from fragmented, manual, point-to-point reporting toward a “collect once, use many times” architecture, and provides concrete evidence of it inside the Upstream Manufacturing segment of the lifecycle scope described above. Piacenza’s lifecycle coverage spans fibre processing, carding and drawing (currently delegated to external suppliers), spinning, warping, weaving and finishing (carried out internally, shared flexibly between the Piacenza and Cerruti facilities depending on season and machinery availability), through to inspection and delivery to clothing brands.

Because the same production lot can move back and forth between the two legal entities two or three times before completion, the strategic priority of the pilot is to give this intra-group exchange of manufacturing capacity a shared, sovereign data layer, rather than the parallel, independent ERP systems in place today following recent acquisitions (Lanificio Piemontese, Cerruti, Arte Tessile, Lanefil). The roadmap then extends the same architecture to external fibre, carding, drawing and yarn suppliers, positioning the data space as a **scalable trust infrastructure for the micro-SMEs** that dominate the sector’s supply side, fully consistent with SAGE’s assessment that they comprise the large majority of textile operators.

The lifecycle scope therefore validates, from a single industrial group’s internal value chain, the same “collect once, use many times” logic that SAGE proposes at ecosystem scale, while showing that even before reaching external suppliers, intra-group capacity sharing already generates the fragmentation a data space is meant to resolve.

5.2.2. Actors, roles and data space architecture

The SAGE project's Circular Textiles Data Space relies on a multi-stakeholder ecosystem governed by a sovereign, decentralized technical framework that strictly separates control operations from data transfer, as shown in Figure 15.

Architecturally, the SAGE Green Deal Data Space (GDDS) operates as a decentralized network where proprietary information remains strictly under local ownership rather than being uploaded to a central database. The architecture guarantees data sovereignty by separating the infrastructure of trust into a Control Plane and a Data Plane. The Control Plane, acting as “the brain,” utilizes data space connectors (such as the Eclipse Dataspace Connector) to verify participant identities, check usage permissions, negotiate contracts, and issue cryptographic access tokens without ever inspecting the underlying business data. Once the Control Plane completes its handshake, the Data Plane—functioning as “the pipe”—streams the actual encrypted data payload directly peer-to-peer between the provider and consumer. This design replaces complex, point-to-point data connections with a streamlined “one-to-many” architecture that enables secure, repeatable data sharing across multiple external partners through a single integration point.

The circular model we are aiming for requires data from different value chain actors

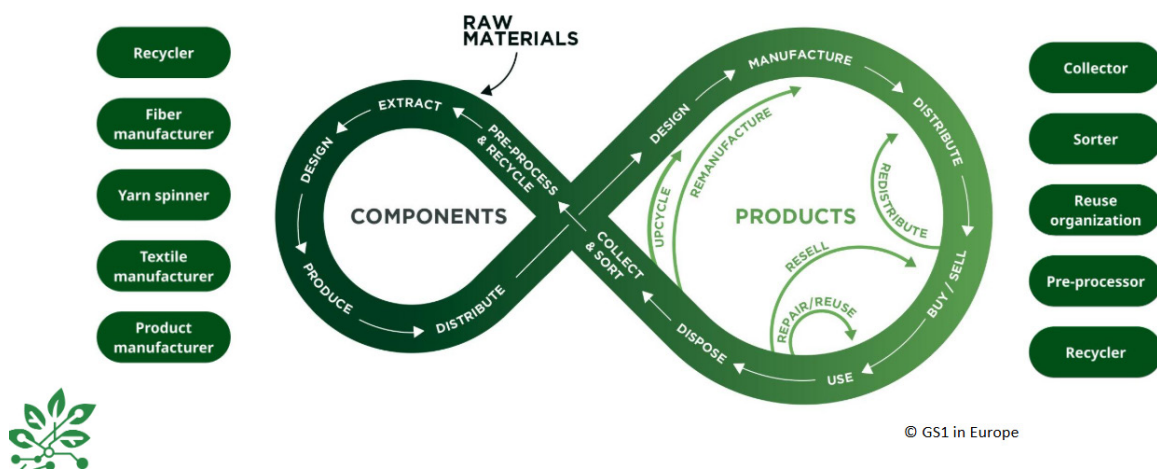


Figure 15. SAGE Circular Textiles Data Space Multi-Stakeholder Model & Framework

In the CIRPASS2 project, the biggest need for improved data exchange is on the Supply Side (Upstream) of the textile value chains. Based on the “Study on DPP content for textile apparel products under ESPR” by JRC, the Global Textile Scheme Initiative differentiates in its GTS industry vocabulary between the following roles:

- Manufacturer – Importer – Other, as the parties that will be legally obliged need to provide the DPP
- Factories – as the facility that really produces the finished product
- Production Material suppliers, providing materials like fabric, buttons zipper to the factory and
- Raw material providers, providing raw materials like e.g. Cotton or Polyester.

In the SM4RTENANCE project, the use case led by PIACENZA 1733 provides a working instance of the Control Plane / Data Plane separation described for SAGE's Green Deal Data Space, and confirms that,

as CIRPASS2 also observes, **the largest exchange need sits on the supply side of the value chain**, where GS1 identifiers such as GLN and GTIN are rarely deployed today.

The actors are Piacenza and Cerruti as data providers/consumers (both legal entities of Piacenza Group), Domina as the technology provider bridging legacy ERP systems and building the DPP data model, and Syxis as the data space technology provider. The architecture is a Minimum Viable Data Space built on open-source Sovity Community Edition connectors implementing the Dataspace Protocol and ODRL-based policy enforcement, with identity managed through a Sovity DAPS built on Key cloak issuing Dynamic Attribute Tokens, and a Sovity Portal serving as the central interface for participant onboarding, connector registration, catalog browsing and contract management, deliberately chosen to avoid vendor lock-in. This mirrors, at pilot scale, the “one-to-many” logic SAGE targets: each entity connects once to shared connector infrastructure instead of maintaining bilateral integrations. Roles remain to be fully formalised for external participants, but Piacenza already acts, in GTS terms, primarily as Manufacturer and Factory, receiving still largely non-standardised upstream data from raw-material and production-material suppliers, most of which lack unique operator, facility or product identifiers, an identifier gap the pilot’s future extension to suppliers is explicitly designed to help close, in line with the emerging JTC 24 / GTS Multi-ID direction referenced elsewhere in this chapter. The architecture also includes a Logging House component, which provides centralized observability and audit trail capabilities across the data space, recording contract negotiation events and data transfer transactions to support transparency, accountability and dispute resolution among participants.

5.2.3. DPP content, identification and access via the data space

For the purpose of framework testing in SAGE, the baseline assumption is that the EU delegated acts under the Ecodesign for Sustainable Products Regulation (ESPR) are fully enacted, establishing a finalized, legally binding set of required DPP data points for textiles. Technical guidance for these parameters draws directly from the European Commission’s Joint Research Centre (JRC) study²⁵, which outlines core data attributes including fiber composition, verified recycled content, chemical compliance, durability metrics, and end-of-life processing instructions. By treating regulatory definitions and data schemas as an established baseline, the SAGE project shifts its core focus from defining *what* data must be shared to proving *how* that data can be exchanged securely at scale. To maintain machine-readability and seamless interoperability across heterogeneous software platforms, DPP data relies on open, global identification standards provided by partners like GS1. Physical products and material batches are linked to unique digital product codes, while processing facilities and operating entities are mapped using Global Location Numbers (GLNs). This standardized scheme ensures that automated sorting machinery, brand traceability platforms, and compliance databases can interpret product origins and material composition across complex cross-border supply chains.

The SAGE project will be testing the access to DPP content via the data space’s sovereign, decentralized architecture that separates governance checking from actual data transfer. Proprietary product data is never uploaded to a central database; instead, it remains securely at the owner’s local infrastructure. When an external brand, PRO, auditor, or LCA service requests DPP information, the GDDS Control Plane verifies the requester’s identity, checks permissions, and executes automated usage contracts. Once validated, a cryptographic access token is issued, allowing the requested data payload to stream peer-to-peer over the Data Plane. This granular control enables data owners to expose public DPP information to

²⁵ González-Torres, M., Arcipowska, A (2026), “Study on DPP content for textile apparel products under ESPR”, JRC SCIENCE FOR POLICY REPORT. Available at https://susproc.jrc.ec.europa.eu/product-bureau/sites/default/files/2026-05/Textiles_DPP_20260513.pdf?_hsenc=p2ANqtz--ok23I22mLeg7ZD65J8cyzNW2wZVj8sNiMMbFexDJncIFqzvGm1s5GEeRkV-mAebfgDCbo2V-1w--VPP57L1eurec-CTreZdRwqbQ-anfQ75MFQljc&_hsmi=419911130

consumers while restricting sensitive operational and supplier data exclusively to authorized regulatory or business partners. Other projects, such as CIRPASS2, work with other standardization bodies such as Global Textile Scheme (GTS) and other identifiers, like e.g. the LEI number.

In the SM4RTENANCE project, the use case led by PIACENZA 1733 confirms, at pilot scale, that DPP content can be reliably extracted from existing ERP systems rather than requiring parallel data entry, while also confirming CIRPASS2's observation that projects beyond SAGE rely on standardisation bodies and identifiers other than pure GS1, since Piacenza's traceability records are built on Italian Customs-audited preferential-origin certification rather than GLN/GTIN.

Domina's extraction tool interfaces with both companies' ERPs and consolidates their outputs into a simplified, common data model covering product information, material components, traceability events, producer information and activity information, formatted in XML and JSON. Access follows the same governed pattern SAGE tests: RESTful APIs (including a dedicated traceability-data endpoint, secured today by API key with TLS integration planned) expose this dataset to the Sovity-based connectors, which apply ODRL usage policies limiting purpose to traceability and sustainability reporting and aligning retention with production cycles, so that proprietary batch-level data stays under each company's control until a specific request is authorised.

Country-of-origin and preferential-certification data, in particular, illustrate why identification cannot rely on product identifiers alone: Piacenza's existing customs-audited process already grants reliable per-lot origin traceability, and the pilot's contribution is to make that same reliability portable and machine-readable through the data space, rather than to replace it with a new identification scheme.

5.2.4. Activities, use cases and benefits enabled by data spaces

The implementation of a Green Deal Data Space for textiles in SAGE transforms isolated circular economy efforts into a connected, automated ecosystem by enabling targeted activities, defined use cases, and tangible systemic benefits. Key activities centre on bi-directional data exchanges that bridge upstream garment design with downstream end-of-life management.

Primary Enabled Use Cases

- **Automated EPR & PRO-IS Monitoring:** Establishes an EU-level Producer Responsibility Organization Information System (PRO-IS) where post-consumer data flows directly to PROs and independent auditors to streamline reporting and compute eco-modulation fees.
- **DPP & Recycled Content Verification:** Automates the movement of verified recycling inputs – tracked in real time from monitored waste through textile-to-textile (T2T) platforms – into brand DPP service, Life Cycle Assessment (LCA) tools, and third-party certification platforms.
- **Circular Intelligence & Policy Statistics:** Aggregates real-time operational data for public authorities to measure progress against EU Green Deal targets without imposing redundant administrative survey burdens on businesses.

The primary advantage of the data space architecture is its shift from chaotic point-to-point connections to a streamlined “one-to-many” network operating on a “collect once, use many times” operational model. This structural shift drastically reduces administrative reporting costs, simplifies auditing, and prevents double-counting in waste management reporting.

In the SM4RTENANCE project, the use case led by PIACENZA 1733 operationalises the same “one-to-many”, collect-once-use-many-times model SAGE targets, following a seven-step data space

methodology (prepare data, onboard the organisation, publish data in the catalogue, select and configure data, define the mode of exchange, adapt the application architecture, implement and run the use case).

Its first Proof of Concept traced across the group: Piacenza Cashmere supplied the raw material, Cerruti carried out spinning and weaving, and Piacenza performed finishing, with DPP, PEF and manufacturing data shared at each transfer, demonstrating end-to-end lot-level traceability across legally distinct but operationally interdependent entities.

Enabled activities extend beyond the DPP itself to agile supply-chain management, continuous monitoring of purchase and sales orders, inventory levels, order progress, demand forecasts, and raw-material, chemical and energy consumption, feeding both compliance and operational decision-making from the same shared dataset.

Reported pilot indicators show a data-sharing achievement above 90%, data accuracy around 99%, and a system error rate below 1%, evidence that the architecture is viable beyond a laboratory exercise.

Consistent with SAGE's projected benefits, the primary advantage observed is structural: a **single integration point per company** replaces multiple bilateral, custom connections, directly reducing the administrative and IT cost of reporting DPP, PEF and traceability data across a group whose production process spans over seventy manufacturing steps.

5.2.5. Challenges and roadmap for scaling

Some challenges identified by the SAGE project when scaling the Circular Textiles Data Space across Europe imply the requirement of resolving deep data bottlenecks, including:

- **Data Silos and Heavy Administrative Burdens:** Current value chains suffer from siloed data systems, limited interoperability, and lack of standardization. Managing isolated point-to-point connections creates excessive reporting complexity and high administrative costs for manufacturers, brands, PROs, and post-consumer actors
- **Regulatory Complexity and Policy Uncertainty:** Stakeholders must navigate a rapidly evolving and overlapping legislative landscape, including ESPR (DPP), WFD (EPR), Green Claims Directive, CSDDD, and national laws like France's AGEC. Implementing uniform technical workflows amid shifting policy timelines creates implementation hesitation.
- **Trust and Data Sovereignty Concerns:** Upstream brands and manufacturers are frequently reluctant to expose supply chain relationships or material specifications due to intellectual property and commercial privacy risks. Scaling requires proving that the data space maintains strict data sovereignty without centralizing sensitive business details.
- **Digitalization:** Low levels of digitalization in textiles is a challenge in both product creation and managing post-consumer textiles. Actors must often take steps to professionalize their operational data, for example with logistics or inventory management software, and strong incentives are needed for the investment and behavior change.

Overcoming the digital, technical, and trust barriers in the textile data space requires a phased strategic roadmap that directly aligns technical architecture with market incentives and regulatory mandates.

Other challenges encountered within the CIRPASS2 project, as the product related data that are needed for any DPP mainly come from the suppliers, also the data spaces approach makes most sense when it supports automated data exchange along the upstream part of the value chains and doing so in close alignment with the current JTC 24 norms. This brings the following two areas of challenges:

- A. Identifier challenges:** Downstream totally common and established GS1 standards like e.g. GLN and GTIN are rarely in use on the supply side of value chains. EN 129 requires Unique Operator, Unique Facility and globally Unique Product Identifiers, that are Upstream not in use today. JRC recommends a voluntary use of the JTC 24 norms, but if this will happen is right now wide open. GTS just started addressing this gap with an EN 18219 conformant Multi ID scheme, that was designed for the supply side, but it will take time to spread this into very global textile supply chains.
- B. Content related challenges:** The data points the manufacturers-importers-others will need to provide a DPP seems for textile products are relatively clear when it comes to the textile ontology developed within CIRPASS 2. A deeper and backwards oriented look into the data points that are needed in each step of the value chain showed, that even for the Unique operators required to provide DPP's additional data will be needed and – even worse – beginning with the factories the data of each data providing step are not identical, which means that the manufacturer-importer others needs from the factory slightly different, but important data points and the factory different ones from their production material suppliers.

In the SM4RTENANCE project, the use case led by PIACENZA 1733 confirms every challenge SAGE identifies, data silos, regulatory uncertainty pending the EU Delegated Act for textiles, trust and sovereignty concerns, and low supplier digitalisation. It adds a **further dimension** that becomes visible only once a real manufacturer sits between many brands and many suppliers: each fashion group currently imposes its own proprietary data requirements, so Piacenza must build and maintain a dedicated data-collection workflow per client, multiplying IT development costs within tight seasonal deadlines; this burden lands hardest on Tier-2/3/4 SME suppliers, who often lack the resources to comply at all, risking exclusion from supplier lists. The absence of a unified reference data model compounds the problem, echoing EURATEX's position that suppliers are forced to collect different data for every customer. E-commerce platforms add a further layer, requesting DPP data item-by-item for every SKU listed online, a cost the pilot's partners consider unsustainable at scale without a shared repository. Beyond the identifier and content-related challenges already flagged for CIRPASS2, the Piacenza pilot's roadmap therefore points to a centralised, institutionally backed, federated repository, extending the current Piacenza-Cerruti Minimum Viable Data Space to raw-material and yarn suppliers, as the only way to convert today's per-brand, per-platform data multiplication into a single, standardised, sovereignty-preserving exchange that scales to the sector's overwhelmingly SME-based supply base.

Thus, aligning DPP applications along a whole Textile and Apparel industry will entail a challenge by itself, especially given the short timeline for the Textile and Apparel sectors to be obliged upon the ESPR regulations.

5.3. Furniture Industry Use Cases

The furniture industry provides a relevant application domain for demonstrating how Digital Product Passports (DPPs) and Data Spaces can support circularity across a long and distributed product lifecycle. The sector involves diverse materials, components and value-chain actors, while furniture products can remain in use for extended periods and undergo repair, refurbishment, reuse and multiple ownership cycles.

The Cir4Fun²⁶ approach addresses these characteristics by combining a product-centric DPP with a Furniture Data Space, enabling trusted exchange of product and lifecycle information across the value chain. This provides the basis for improving product transparency, supporting circular services and feeding lifecycle information back into sustainable and circular product design.

²⁶ <https://cir4fun.eu/>

5.3.1. Strategic focus and lifecycle scope

The furniture sector provides a particularly relevant use case for demonstrating how Digital Product Passports (DPPs) and Data Spaces can support circularity across a long and distributed product lifecycle. Furniture products often remain in use for many years and may pass through multiple ownership cycles, repair interventions, refurbishment activities, reuse and, ultimately, end-of-life treatment. Consequently, the availability of reliable product information beyond the manufacturing and sales phases is particularly important.

The strategic focus is therefore on enabling **information continuity across the furniture lifecycle**, from design and production through distribution and use, repair and maintenance, reuse and refurbishment, to dismantling, recycling and other end-of-life processes. The DPP acts as a lifecycle information carrier that can be progressively enriched when relevant events occur.

For furniture, relevant information includes product characteristics and identification, bill of materials (BOM), material composition and provenance, durability, reliability, repairability, upgradability, reusability, recyclability, environmental impacts, carbon footprint, safety, usage and end-of-life information. This information supports different decisions depending on the lifecycle stage and stakeholder involved.

The Cir4Fun approach is particularly focused on enabling the transition from static product information towards a **living product information record**, where authorized lifecycle events can be associated with the product. For example, information concerning logistics, maintenance, repair, component replacement, refurbishment or recycling can be added or updated during the product's lifetime. This allows the same product identity to support several successive circular-use cycles.

The approach also supports the integration of DPP information with eco-design activities. Information generated during the use, repair, refurbishment and end-of-life stages can provide feedback for future product development and contribute to improving durability, repairability, reuse and recyclability.

5.3.2. Actors, roles and data space architecture

The furniture DPP involves a broad ecosystem of stakeholders, including component and material manufacturers, furniture manufacturers, distributors and retailers, consumers, repair and maintenance operators, reuse and refurbishment operators, waste-management and recycling organizations, public authorities and digital service providers.

Component manufacturers and material suppliers provide information on components, materials, composition and provenance. **Furniture manufacturers** create product-level information and sustainability data and have a central role in establishing and maintaining the product DPP. **Distributors and retailers** contribute commercialization and logistics information. **Consumers** primarily access selected DPP information; but may also contribute relevant lifecycle information where appropriate. **Repair and refurbishment operators** use and update information related to maintenance, repairs and second-life activities. **Waste-management and recycling operators** use material and composition information to support appropriate end-of-life treatment and can contribute information on material recovery or disposal.

The Cir4Fun architecture follows a **product-centric and federated approach**, with the Furniture Data Space providing the trusted environment for data exchange across the furniture value chain. In this context, **Furniture-X** provides a relevant sectoral Data Space perspective for connecting furniture

manufacturers, suppliers, service providers and downstream circularity actors, while the Cir4Fun DPP provides the product-centric information layer. This is consistent with the Cir4Fun architecture, which identifies the DPP ecosystem, Data Space domain and Ecodesign Management System as three complementary system domains.

The DPP system manages product identity, DPP metadata, lifecycle information and access mechanisms; the Furniture Data Space supports trusted and sovereign exchange of information between participating stakeholders; and the Ecodesign Management System uses product and lifecycle information to support sustainable and circular product design.

A Responsible Economic Operator (REO) has responsibility for the DPP and its authoritative product information. At the same time, information can originate from different organizations throughout the value chain. The architecture therefore enables distributed contributions while maintaining a consistent product-level view. The DPP can also act as an entry point to additional information and services held within stakeholder Data Spaces or other connected systems.

This approach is particularly relevant for furniture because the complete set of information required to support circularity cannot normally be generated or maintained by a single organization. Data Space mechanisms enable stakeholders to retain control over the information they provide while making relevant information discoverable and accessible to authorized participants.

5.3.3. DPP content, identification and access via the data space

The Cir4Fun furniture DPP uses a structured, furniture-specific information model to support interoperability across stakeholders and lifecycle stages (Figure 16). The model combines a common furniture vocabulary with structured relationships and information models. It supports both an **Asset Administration Shell (AAS)-based representation** and an **ontology-based representation**, providing complementary mechanisms for structured and semantic interoperability.

The DPP content covers several main categories:

- **Product identity and composition:** product characteristics, nameplate information, manufacturer, product type, BOM, components and materials;
- **Performance and use:** usage, durability, reliability and functional characteristics;
- **Circularity and end-of-life:** repairability, upgradability, reusability, refurbishment, remanufacturing, recyclability, material recovery and waste management;
- **Environmental and lifecycle information:** environmental impact, carbon footprint, sustainability indicators and lifecycle events;
- **Traceability and provenance:** product origin, material provenance, logistics and relevant historical records;
- **Compliance and documentation:** certificates, standards, instructions and other information relevant to professional users and authorities.

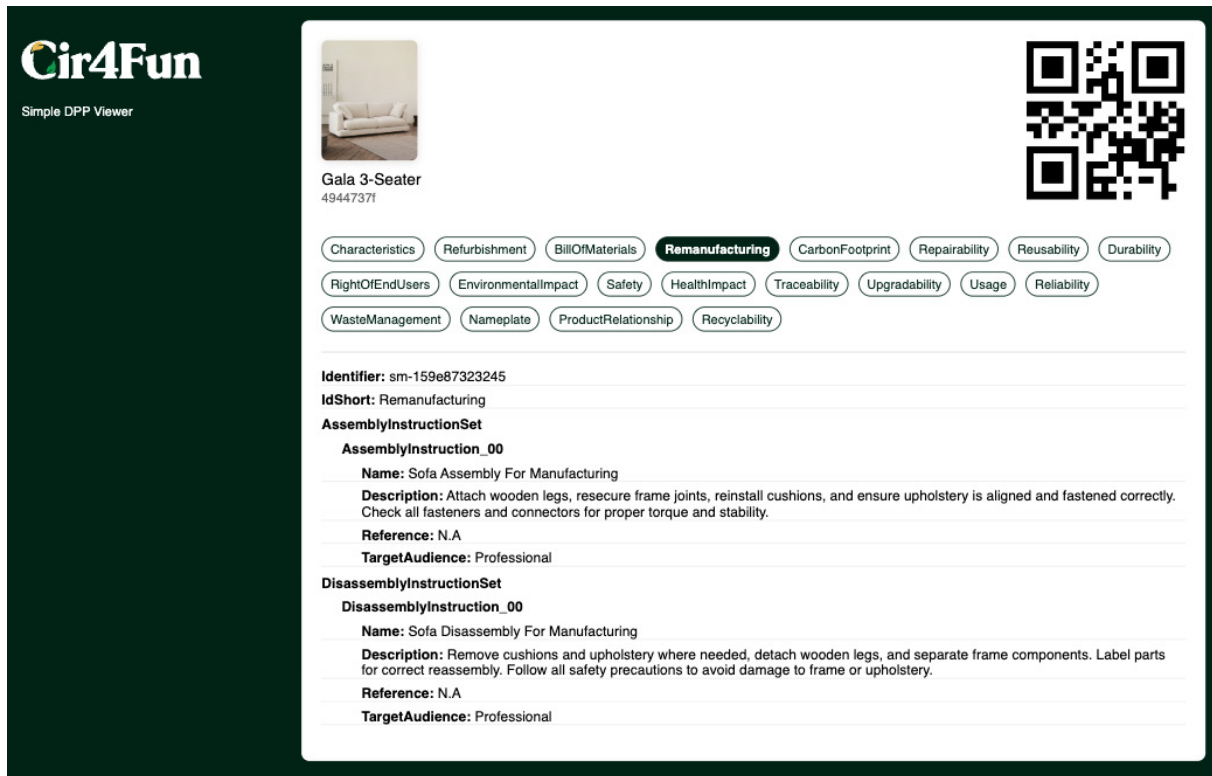


Figure 16. An example of furniture DPP representing its attributes

A **Unique Product Identifier (UPI)** provides the link between the physical product and its DPP. The identifier can be associated with a suitable data carrier, such as a QR code, enabling consumers and professional stakeholders to access the DPP.

The access model is role-based. Consumers may access selected product, sustainability, repair and recyclability information, while professional stakeholders such as repairers, refurbishers and recyclers may require more detailed technical and lifecycle information. Authorities can access information relevant to compliance and market surveillance. Sensitive information should remain accessible only to authorized stakeholders.

The DPP can also provide an entry point to additional information available through the Furniture Data Space. Thus, the DPP does not need to contain every piece of information generated throughout the value chain; instead, it can provide a product-level reference through which relevant information and services can be discovered and accessed according to the applicable access rights.

5.3.4. Activities, use cases and benefits enabled by data spaces

The combination of DPP and Data Spaces enables several furniture-sector use cases.

Product and material provenance: The DPP can provide information about product origin, materials, components and their provenance. This improves transparency for users and supports professional stakeholders in assessing the composition and origin of products and materials.

Maintenance and repair: Repair operators can access relevant product information, care and repair instructions and component information. Repair events and replaced components can subsequently be recorded, creating a more complete product history and supporting future maintenance or refurbishment.

Reuse and second-life applications: Product information concerning composition, durability, previous interventions and lifecycle history can support the assessment of furniture for reuse. This is particularly relevant to second-hand markets, where the availability of trusted information can improve confidence and support more appropriate valuation of products.

Refurbishment: Refurbishment operators can use product and component information to determine appropriate interventions and identify materials or components that can be repaired or replaced. Information about refurbishment activities can subsequently contribute to the product's lifecycle history. Reverse logistics and end-of-life management: The DPP can support the identification and classification of furniture when it is returned, collected or reaches end of life. Information on composition, previous treatments and condition can help determine whether the appropriate route is reuse, repair, refurbishment, dismantling or recycling.

Disassembly and recycling: Recyclers and waste-management operators can use information about materials, components and disassembly to improve sorting and recovery. This is particularly important for furniture products containing combinations of wood, wood-based panels, textiles, plastics, metals, coatings, adhesives and other materials. Better information can support more effective material separation and recovery.

Consumer transparency and lifecycle services: A consumer-facing DPP application can provide access to selected product information, including product identity and composition, sustainability information, repair guidance, recyclability information, origin and lifecycle information. This can improve transparency and allow users to retain relevant product information for future reference. The Cir4Fun consumer application follows this principle by retrieving and presenting DPP information without modifying the underlying DPP.

Eco-design and continuous improvement: Aggregated lifecycle information can provide feedback to manufacturers concerning product durability, repair needs, refurbishment, material recovery and other circularity aspects. This can support eco-design decisions and contribute to the development of products that are easier to maintain, repair, reuse and recycle.

The principal benefit of the Data Space approach is that these activities can be supported by information originating from different organizations without requiring all stakeholders to maintain a common centralized database. It therefore combines lifecycle transparency with data sovereignty and interoperability.

5.3.5. Challenges and roadmap for scaling

The implementation of DPPs in the furniture sector faces several challenges.

First, **data heterogeneity and interoperability** remain important issues. Furniture products vary significantly in their materials, components, construction methods and product categories. A common vocabulary and interoperable information models are therefore required while retaining sufficient flexibility for product-specific information. The use of furniture-sector semantic resources together with AAS and ontology-based approaches provides a foundation for addressing this challenge.

Second, **data completeness and quality** need to be ensured across the value chain. Important information is generated by different stakeholders and at different lifecycle stages. The DPP therefore needs clear responsibilities for data provision, validation and maintenance, together with mechanisms for recording the provenance of information.

Third, **lifecycle continuity** is particularly challenging for furniture because products can remain in use for decades and may change ownership several times. The UPI and associated data carrier must remain usable throughout these transitions, while the DPP must support the progressive addition of lifecycle information without compromising the integrity of previously recorded information. The Cir4Fun architecture explicitly supports such progressive enrichment through authorized lifecycle events.

Fourth, **end-of-life data and material** recovery present specific challenges. Stakeholder investigations identified difficulties related to material mixing, chemical contamination, inconsistent waste classification, limited traceability of individual components and the economic feasibility of disassembly. Reliable information on material composition, previous treatments, disassembly and recycling can help address these issues, but standardized approaches and economically viable recovery processes are also required.

Finally, **stakeholder adoption and governance** will determine the scalability of the approach. The furniture value chain includes many SMEs and organizations with different levels of digital maturity. The participation model therefore needs to minimize technical barriers while providing clear benefits for manufacturers, service providers, consumers and recyclers. Data access, privacy, security and responsibilities for updating lifecycle information also need to be clearly defined.

A pragmatic roadmap is to begin with a **core furniture DPP** covering product identity, composition, BOM, sustainability and circularity information, and then progressively introduce lifecycle services for logistics, repair, refurbishment, reuse and end-of-life management. Integration with the Furniture Data Space, including relevant sectoral initiatives such as Furniture-X, can subsequently enable more distributed and automated exchange of information, while integration with the Ecodesign Management System can create a feedback loop from lifecycle experience to future product design.

The furniture use case therefore demonstrates how a DPP can evolve from a compliance-oriented information mechanism into a shared lifecycle information infrastructure for circularity, with Data Spaces providing the trusted environment for cross-organizational exchange.

5.4. Semiconductor Industry: Semiconductor-X

The semiconductor industry is characterized by one of the world's most complex and globally distributed supply chains. Semiconductor products can pass through more than one thousand process steps and numerous international borders before becoming part of a final system. Production is distributed across material suppliers, equipment manufacturers, front-end fabs, foundries, assembly and test providers, distributors, and downstream manufacturers.

This complexity is further increasing with the transition towards chiplet-based and heterogeneous semiconductor architectures. A single semiconductor product may combine multiple dies from different technologies, manufacturing sites, and suppliers within one package.

Semiconductor-X²⁷ therefore focuses on establishing interoperable data models and sovereign exchange mechanisms that can connect these distributed production and supply-chain stages without requiring companies to centralize commercially sensitive information. Chiplet integration and resilient heterogeneous supply chains are explicit application areas of Semiconductor-X, that aims to strengthen

²⁷ <https://www.semiconductor-x.com/>

the resilience, sustainability, and digital sovereignty of the European semiconductor ecosystem through interoperable digital twins and federated data spaces.

Semiconductor-X builds on Catena-X and Tractus-X concepts and combines Asset Administration Shells (AAS), digital twins, and federated data-space technologies to exchange information between organizations while allowing authoritative data to remain under the control of its respective source. This approach is consistent with the wider DPP architecture presented in this paper, in which standardized product information and identifiers provide a product-centric entry point, while data spaces govern the broader B2B exchange of distributed lifecycle information.

5.4.1. Strategic focus and lifecycle scope

One of the strategic focuses of Semiconductor-X is to enable the **trusted and internationally interoperable exchange of sustainability information across the global semiconductor value chain**, particularly towards downstream customers and industries. A key use case is the exchange of **Product Carbon Footprint (PCF)** information, allowing downstream manufacturers to incorporate semiconductor-related emissions into the environmental assessment of their own products.

Because semiconductor supply chains are globally distributed, sustainability information requires alignment with internationally applicable approaches such as the **PACT (Partnership for Carbon Transparency) framework and the TfS (Together for Sustainability) methodology**, as well as the Catena X PCF Use Case (Product Carbon Footprint Exchange KIT), combined with interoperable digital product models and data-space standards. Semiconductor-X therefore provides a foundation for exchanging sustainability information consistently and securely across organizational and national boundaries.

Beyond PCF, the same infrastructure can support additional sustainability, traceability, quality, documentation, software, and lifecycle information required by downstream industries. It is therefore important to distinguish between a future **regulatory DPP core**, containing information mandated by applicable legislation and required by downstream OEMs, and **additional industrial information and services** exchanged voluntarily between business partners. This separation allows the infrastructure to evolve with future regulatory requirements without limiting its use to regulatory compliance. Semiconductor-X is based on:

1. the use of **eIDAS 2.0 and comparable trusted and interoperable identification systems** at a global scale;
2. the implementation of the **Catena-X framework**;
3. the use of the **DSP/DCP data-space protocols**, with IDSA serving as an important architectural and standardization anchor;
4. the use of **Tractus-X Kits and the Eclipse Tractus-X EDC** to support secure data exchange based on **ODRL policy enforcement**;
5. a **highly secure DPP identification mechanism** based on EN 18219 Scheme 2, using a cryptographically random opaque identifier, and Scheme 3, using DIDs combined with opaque random identifiers, in order to support confidentiality by design;
6. a **Zero Trust, three-level data-space architecture** designed to balance cybersecurity and data-sensitivity requirements at each level: Level 1 – basic, Level 2 – trusted, and Level 3 – critical.

5.4.1.1. *Need for a holistic lifecycle perspective for sustainability data calculation:*

From a lifecycle perspective, this is an important factor that must be considered in lifecycle-oriented DPP approaches: the sustainability impact of a semiconductor cannot be determined from its manufacturing footprint alone, as its use in downstream applications may enable significantly greater emission reductions over the lifetime of the overall system. PCF, for example, illustrates why semiconductor sustainability cannot be assessed solely on the basis of manufacturing emissions. A prominent example is **silicon carbide (SiC) power semiconductors**. Their production can require more energy and therefore result in a higher manufacturing footprint than conventional silicon-based components. During their use phase, however, their higher efficiency can reduce electrical losses in power electronics, electric drives, and industrial machinery. The additional emissions (footprint) generated during semiconductor production can therefore be outweighed by significantly greater emission reductions (handprint) during downstream operation.

The semiconductor sustainability paradox is that a component may have a higher manufacturing footprint while generating an even larger carbon handprint during its use phase. Thus, the purpose of the DPP and data-space infrastructure is not simply to calculate a single sustainability score, but to provide the trusted product identity, provenance, methodological context, and interoperable sustainability data required for such assessments. This demonstrates why semiconductor sustainability requires a **holistic lifecycle and data-space approach**.

5.4.2. Actors, roles and data space architecture

Unlike many comparatively linear supply chains, the semiconductor industry is **not generally organized according to a simple one-up-one-down structure**. In particular, the fabless business model creates highly interconnected value networks in which a semiconductor designer may simultaneously coordinate multiple foundries, IP providers, packaging and test partners, material suppliers, and downstream customers. The resulting information flows are therefore **many-to-many and network-oriented**, rather than following a single sequential supply-chain path.

This network structure has important consequences for the DPP and data-space architecture, as no single participant possesses all the information required to describe the complete lifecycle of a semiconductor product, and no single actor should be required to centralize the underlying industrial data. Semiconductor-X therefore follows a **federated data-space approach**, in which authoritative information remains under the control of the respective organizations and can be exchanged through standardized, policy-controlled interfaces according to the specific business relationship and use case.

5.4.2.1. *Trusted organizational identity*

Every protected cross-organizational exchange requires a trusted identity for the participating organization and, where necessary, its roles and authorizations. Within Europe, **eIDAS 2.0 provides an important trust framework for electronic identification and electronic attestations**. The architecture must, however, remain internationally interoperable because semiconductor supply chains extend far beyond the European Union. Semiconductor-X therefore supports initiatives to establish an international trust framework system supported by government level organizations based on eIDAS-based identity frameworks.

5.4.2.2. Three-level Zero Trust data-space architecture:

Because semiconductor information differs considerably in sensitivity, Semiconductor-X proposes together with Manufacturing-X a **three-level dataspace architecture within a common Zero Trust model**²⁸. Zero Trust applies at all three levels: no actor, system, or network location is inherently trusted (Figure 17). The levels define progressively stronger requirements for authentication, authorization, disclosure, and technical containment and an increase in complexity and operational costs.

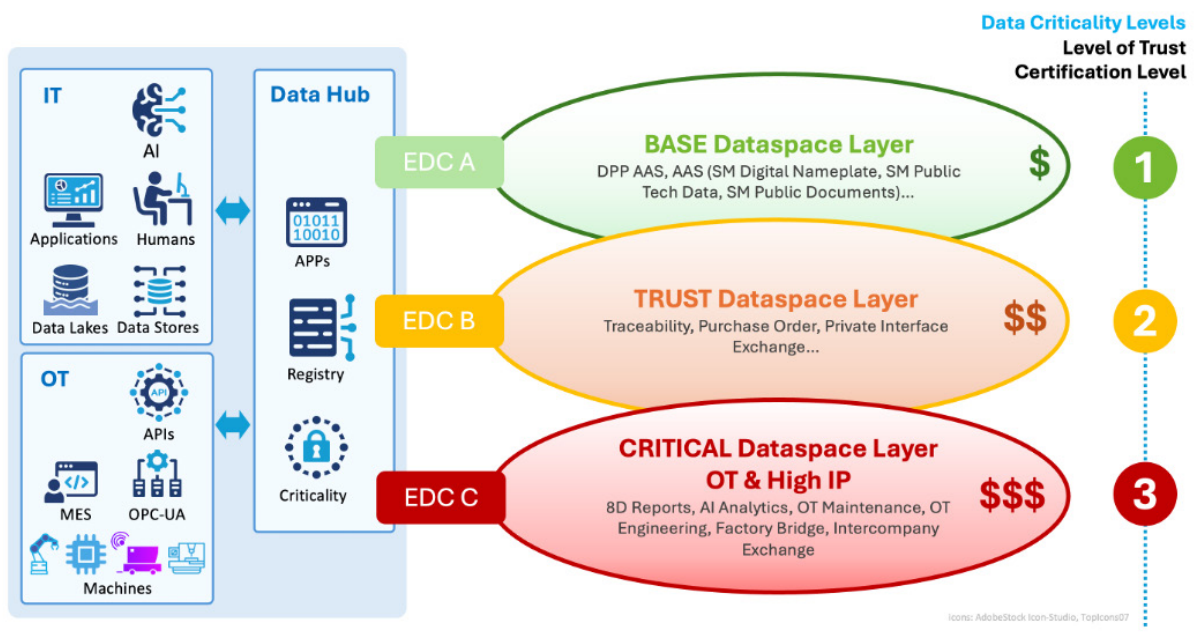


Figure 17. E2E Security Architecture of Industrial Dataspaces

Level	Information class	Typical semiconductor information
Level 1 – Basic	Public or low sensitivity	Regulatory DPP information, public sustainability declarations, product documentation
Level 2 – Trusted	Confidential B2B	PCF, provenance, quality data, supplier-specific documentation, selected lifecycle information
Level 3 – Critical	Highly confidential / strategic	Process information, yields, capacity, fab allocation, detailed supplier networks, security-relevant production information

Table 1. Semiconductor-X DPP Information based on the E2E Security Architecture of Industrial Dataspaces Model

²⁸ E2E Security Architecture of Industrial Dataspaces; Avgoustinos, Haris; Gossner, Harald; Jochem, Michael et al.; Manufacturing-X Topic Group, August 2026. Available at https://mx-guidanceboard.org/wp-content/uploads/Manufacturing-X-E2E-Security_202606.pdf

The important architectural principle is that **the DPP does not need to expose the same amount of information at every security level**. Further is the Basic level easier to implement especially for SMEs. A Level 1 DPP may, for example, state a verified PCF value. Level 2 may provide authorized customers with additional methodology, provenance, validity period, and sustainability evidence. Level 3 may contain the detailed production data needed to calculate or audit that value, while keeping this information entirely within the manufacturer's protected environment. The layers therefore represent different **views onto authoritative information rather than separate copies of the same complete dataset**.

5.4.3. DPP content, identification and access via the data space

5.4.3.1. DPP Contents and semantics

Highly confidential production information should generally remain outside the directly accessible DPP and be exposed only as **derived information, verified claims, controlled queries, or explicitly authorized data products**. This leads to an important distinction for a future semiconductor DPP:

- **The regulatory DPP core** should contain or reference the information that is legally required and intended to be accessible to the respective regulatory audience.
- **The industrial DPP extension** can provide additional sustainability, traceability, quality, software, lifecycle, and technical information to authorized business partners through the data space.

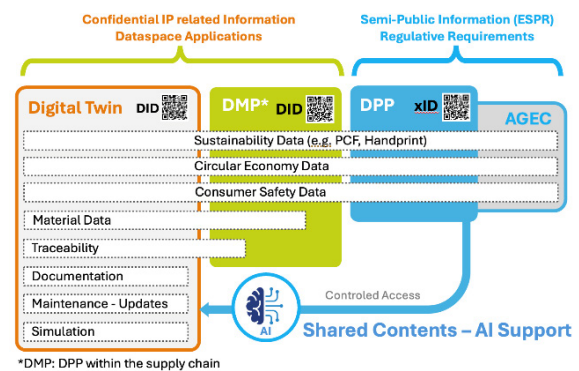


Figure 18. Semiconductor-X DPP Contents

In Semiconductor-X we used the Digital Material Pass (DMP) terminology for the upstream supply chain information pipeline (and components like semiconductors) of a final product and its regulated DPP for example in “Electronic Components” to avoid confusion (Figure 18).

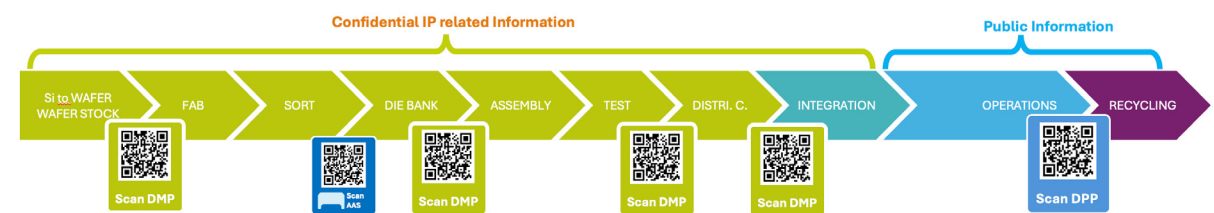


Figure 19. Semiconductor-X Confidential vs Public Information Semantics

At the semantic level, Semiconductor-X uses the Asset Administration Shell (AAS) as an important mechanism for representing digital twins and structured product information. However, the semiconductor industry already relies extensively on international SEMI standards and specifications, which describe manufacturing equipment, production communication, process and product information, and other semiconductor-specific data structures. A scalable semiconductor DPP must therefore integrate with this existing international standards landscape rather than establish a parallel or isolated

information model. The objective is to enable information to be translated and exchanged without loss of semantic meaning. This requires open and transparent data-conversion schemes between the relevant representations. Mapping rules between SEMI-based models, AAS submodels, sustainability models such as PCF, and other industry data formats should therefore be openly specified and, where possible, AI-supported.

For the **semiconductor industry, however, semantic interoperability must be combined with confidentiality by design** (Figure 19). Product and sustainability information can be highly sensitive because seemingly innocuous data can reveal production locations, supplier relationships, capacity, product ramp-up, technology generations, yields, or other commercially relevant information. Semiconductor-X therefore combines semantic interoperability with a **Zero Trust, policy-controlled and identity-based data-space architecture**.

5.4.3.2. Identification - Security Consideration – Identifier-Based Information

Disclosure:

A relevant threat in semiconductor DPP implementations is the **unintended disclosure of confidential production intelligence through the product identifier itself**. Where model numbers, batch numbers, production locations or sequential serial numbers are embedded in a publicly accessible DPP identifier, third parties may correlate observations over time and infer production volumes, ramp-up or ramp-down, capacity utilisation, yield trends, product success or customer allocation.

In semiconductor supply chains, this risk is amplified by the possibility of correlating identifiers across material lots, wafers, dies, packages and downstream products. Such disclosure may occur as a **side effect of an otherwise standards-compliant identification scheme**, without any direct compromise of the DPP system. It may nevertheless undermine trade-secret and business-confidentiality protections and, where the Cyber Resilience Act applies, could contribute to non-compliance with the CRA requirements for cybersecurity risk assessment, confidentiality protection, data minimisation, limitation of attack surfaces and security-by-design.

For this reason, **EN 18219:2026 Schema 2** (<https://www.beispiel.com/<UUID>>) with a UUID or similar should be preferred where an opaque, random Identification Link according to IEC 61406-1 is sufficient and batch-number or serial number are presented in the DPP payload. **Schema 3** may be used where decentralised and cryptographically verifiable identities are required, provided that the DID uses a non-semantic, non-sequential and non-enumerable identifier (<https://resolver.io/did:web:example.com:<secure-identifier>/?service=item-dpp>).

The remaining schemas are less suitable for confidentiality-sensitive semiconductor applications where their structured or semantically meaningful identifiers expose or facilitate derivation of product, serial, batch or organisational information.

The public DPP identifier should therefore provide uniqueness and resolvability while preventing the disclosure or inference of commercially sensitive manufacturing information. Regarding the requirements of the EU Cyber Resilience Act (CRA), Schemas 1, 4 and 5 may create additional CRA-relevant confidentiality and attack-surface risks when implemented with structured, semantic, sequential or readily observable identifiers, whereas Schema 2 explicitly supports masking of model and serial information through random identifiers and Schema 3 can provide an opaque identifier combined with cryptographically verifiable identity.

5.5.3.3. DPP composition and hierarchical product structures:

A further challenge is the **composition of DPPs for complex products**. A semiconductor package may consist of several chiplets, each with its own DPP or digital twin. The same problem appears at higher levels, where electronic assemblies, machines, and industrial systems are composed of multiple components, each potentially carrying its own product information.

Providing a single, consolidated DPP facade simplifies access for the downstream OEM, but requires the DPP provider to **aggregate and reconcile data from multiple component-level DPPs**. Conversely, exposing every component DPP separately simplifies data provision but transfers the complexity to the receiver, who must navigate the product structure, resolve dependencies, and understand how the individual components contribute to the overall product.

Semiconductor-X therefore proposes a **dual approach**: regulatory and product-level information, such as PCF, should be **aggregated at the final product level according to a defined methodology**, while detailed information that remains relevant to individual components—such as technical documentation, maintenance information, repair instructions, provenance, and recycling data—can remain at component level and be linked through the product structure.

This creates a hierarchical DPP model in which the **product-level DPP provides the regulatory and sustainability facade**, while component-level DPPs preserve the detailed information required for technical and lifecycle use cases.

5.4.4. Activities, use cases and benefits enabled by data spaces

Semiconductor-X demonstrates how a federated data space can become a common infrastructure for cross-company collaboration across the semiconductor supply and value chain. The data space enables trusted, confidential, interoperable, sovereign and policy-controlled exchange of information between organizations and systems at a new level of simplicity, while allowing the data to remain under the control of its authoritative source.

The demonstrated projects use cases cover a broad range of industrial activities, including **end-to-end supply-chain simulation, production planning, yield improvement, root-cause analysis and data-quality management, as well as PCF determination, cleanroom-emission optimization, abatement maintenance, traceability, outsourcing, commercial processes, trustworthiness, entitlement management, cross-data-space transfer and EDC-based contract and policy enforcement**.

These use cases illustrate the main value of the data-space approach: **the same interoperable and trusted infrastructure can support sustainability, production optimisation, resiliency, quality, and new digital services and AI-applications without requiring a separate paradigm or architecture for each use case**. This elevates interoperability from only Data- to Process-Interoperability.

Within this broader infrastructure, the DPP acts as an important product-centric enabler and access point. It provides a persistent product identity and a standardized set of product-related information that can be referenced and reused across different data-space applications. In this sense, the DPP mechanics combined with the digital twin offer a structured continuous product-information layer that makes relevant data easier to discover, interpret and connect across the value chain and the life cycle.

Semiconductor-X therefore distinguishes between DPP-oriented use cases and Digital Twin use cases. The DPP focuses on product-level information that needs to remain available across organizational and lifecycle boundaries, such as sustainability information, regulatory conformity evidence, material information, product identification, entitlement and end-of-life information.

The non-regulated Digital Twin complements the DPP where deeper operational, manufacturing or lifecycle information is required. Examples include backward traceability to wafer lots and materials, lot and batch genealogy, process provenance, quality and binning information, product history, maintenance, replacement, upgradeability, decommissioning and recycling intelligence.

This separation allows the DPP to provide a stable product-level facade, while the data space gives authorized users-controlled access to more detailed Digital Twin and supply chain information where required.

The key benefit is therefore a shared data-space foundation on which DPPs, Digital Twins and further industrial applications can coexist and reuse the same identity, trust, policy and interoperability mechanisms. In this architecture, the DPP becomes an important enabler for connecting product information with a broader ecosystem of sustainability, operational, AI- and lifecycle-services.

5.4.5. Challenges and roadmap for scaling

In conclusion, Semiconductor-X has identified several **industry-specific challenges for scaling**, including:

- appropriate DPP granularity while preserving global production flexibility;
- confidentiality, trusted access and long-term cryptographic security;
- global interoperability and semantic scalability across heterogeneous international data-models and computing ontologies.

5.4.5.1. Semiconductor-specific supply-chain and model/item granularity challenges:

The semiconductor industry has an exceptionally **complex, dynamic, and globally distributed supply chain**. A semiconductor product may pass through several countries and organizations before reaching the downstream customer. The increasing adoption of **chiplet-based architectures** further intensifies this complexity, because a final semiconductor package can combine dies originating from different technologies, manufacturers, fabs, and production routes.

At the same time, semiconductor manufacturing requires a high degree of **production flexibility**. The same semiconductor model may be produced in several qualified fabs or transferred between manufacturing locations according to available capacity, yield, supply-chain disruptions, or geopolitical conditions. Production allocation **can change on a daily basis** without changing the functional product model delivered to the customer.

Consequently, **model-level sustainability values based on representative or averaged production data are particularly important for scalable semiconductor sustainability reporting**. More granular information, for example at batch level, should only be introduced where the benefits justify the implications for operational flexibility, supply-chain resilience, and confidentiality.

5.4.5.2. Confidentiality, trusted access and long-term security

Scaling semiconductor DPPs requires **confidentiality-by-design**. Product identifiers, registries and resolution services must not expose information from which production volumes, fab allocation, customer relationships, batch sizes or product ramp-up can be derived. In particular, **a compromise of a DPP registry should not itself reveal commercially sensitive production intelligence**. Registries should therefore contain only the minimum information required for identification and resolution, using opaque and non-enumerable identifiers rather than meaningful serial, batch or production information.

Access must also distinguish clearly between trusted supply-chain participants requiring protected B2B information and third parties accessing public or regulatory DPP information. At the same time, onboarding mechanisms must remain sufficiently lightweight to enable SMEs to participate without weakening trust requirements. A challenge addressed by the presented three level architecture of the dataspace.

Because of the long-term requirements of the DPP, we look forward to a trust architecture that additionally support cryptographic agility and long-term post-quantum readiness. DPP identities, credentials, signatures and resolution mechanisms should be designed so that cryptographic algorithms and keys can be migrated without breaking or disclosing persistent and confidential product identities or lifecycle records.

5.4.5.3. Global interoperability and semantic scalability

A semiconductor DPP cannot scale as an isolated European or Continental information model. Semiconductor-X therefore emphasizes international interoperability, including the integration of established SEMI standards, AAS-based models, sustainability methodologies and other sector-specific representations through open semantic mappings and conversion mechanisms to accelerate the process and get a broad acceptance.

The objective is to allow different trusted models to coexist and interoperate without loss of meaning for example through the implementation of an RDF/JSON-LD approach of the AAS²⁹. This becomes particularly important as DPPs are composed across chiplets, components, modules, machines and complete systems and address a cross-domain worldwide supply chain.

Scalability is also a fundamental architectural requirement. Semiconductor manufacturing generates very large numbers of products, lots, process events and relationships. Semantic models, dataspace connectors, registries and resolution mechanisms must therefore operate in massive, potentially exascale data environments.

Finally, the Semiconductor-X roadmap therefore combines End2End-security-by-design, confidentiality-by-design, cryptographic agility, international semantic interoperability, handprint integration and federated data-space architectures as prerequisites for scaling DPP concepts to the global semiconductor industry.

²⁹ AAS/RDF Interoperability Approaches for DPP; Bernier, C.; Li, W., Kuiper, J.; Stojanovic, L. et.al.; (2026). Zenodo. <https://doi.org/10.5281/zenodo.20396377>

5.5. Energy Data and BESS: Market-Role Governance and Controlled Battery-Passport Access

The Energy Data-X project³⁰ (a Gaia-X lighthouse initiative establishing a federated, cross-sector data space for the energy industry) provides a primary reference implementation for governed access to Digital Battery Passports (DBP) and Battery Energy Storage System (BESS) evidence. By implementing a federated trust chain that combines authentic sources, authorized issuers, and European Business Wallet (EBW) concepts, the architecture demonstrates how market-role credentials can govern access to restricted data via connector-side policy enforcement engines³¹.

5.5.1. Strategic focus and lifecycle scope

The energy sector is becoming increasingly decentralized and data-intensive. Grid operators, suppliers, metering point operators, flexibility providers and new energy services need to exchange data across organizational and sectoral boundaries. Conventional platform accounts establish that a user has logged in but do not necessarily prove the regulated capacity in which an organization acts.

Energy data-X addresses this problem through portable company and market-role evidence. Its “Imbalance Settlement Quality” and “Flexibility Aggregation” use cases links metering, aggregation, forecasting and flexibility processes through a federated data ecosystem. Data remains in participants’ systems and is exchanged through connectors under common identity, trust and policy mechanisms.

For BESS, this approach supports both regulatory and operational lifecycles. The legally regulated passport object is the individual battery, not automatically the complete storage installation. A broader BESS evidence model may additionally cover inverters, battery-management and energy-management systems, software, operators, maintenance events and service history. Relevant applications include product safety, condition monitoring, predictive maintenance, flexibility aggregation, asset utilization, second-life assessment and responsible take-back.

5.5.2. Actors, roles and Data Space architecture

The energy data-X architecture combines authentic sources, authorized issuers, business wallets, connectors and policy engines. Authentic sources maintain company or governed market-role information. An authorized issuer binds that information to an identified legal person in a verifiable credential for PLI access. The organization stores and presents the credential through its EBW, while the connector verifies it and passes the result to a policy engine. The policy engine permits, restricts or denies access according to the policy associated with the requested data or service.

Relevant evidence can include the EUID, an EU Company Certificate (EUCC), a Market Partner ID and a market-role credential. Market roles such as supplier, grid operator, metering point operator or Balance Responsible Party define different responsibilities and permitted actions. Established technical trust, including the German Smart Metering Public Key Infrastructure, can coexist with wallet-based company and role credentials.

³⁰ Energy Data-X Gaia-X Lighthouse Project. Available at: <https://www.energydata-x.eu/en/>

³¹ Spherity Research (2026), “Energy Data-X: European Business Wallet & Market-Role Credentials for BESS”. Available at: <https://spherity.github.io/spherity-research/energy-data-x-European-Business-Wallet-market-role-credentials-BESS-2026.pdf>

A BESS and DBP implementation must distinguish several access categories. Market Surveillance Authorities, notified bodies and the European Commission act under statutory authority. Customs authorities exercise functions connected to border control and the DPP Registry. Repairers, remanufacturers, second-life operators and recyclers may qualify as Persons with a Legitimate Interest (PLIs), subject to the applicable legal criteria. BESS operators, maintenance providers, insurers or financiers may instead rely on contracts, consent or asset-owner authorization.

Algorithms and AI services form a further category but do not hold an independent market role or PLI status. Their authority must derive from an identified legal person through a bounded mandate specifying the permitted purpose, asset scope, actions and validity period.

5.5.3. DPP content, identification and access via the Data Space

The EU Batteries Regulation distinguishes public battery-passport information from information reserved for authorities and information accessible only to eligible PLIs. Access rights may also differ for reading, downloading, sharing, introducing, modifying or reusing information. Authentication of an organization is therefore necessary but insufficient.

The energy data-X model separates identity, role and authorization. A legal-person credential establishes which organization is requesting access. A market-role, authority, professional-role or mandate credential establishes the capacity in which it acts. The policy engine then evaluates this evidence against the product, purpose and requested operation: *Access = verified legal person + governed role or mandate + authorized issuer + valid credential status + permitted purpose + matching product policy.*

The policy check may occur during catalogue access, contract negotiation or data transfer. It should include issuer trust, credential validity and revocation status, jurisdiction, product scope and the current lifecycle state of the battery.

For a BESS, the DBP can be complemented by linked operational and lifecycle evidence, including state of health, safety events, maintenance records, repair information, transport history and evidence relating to reuse or recycling. High-frequency time series data should remain in appropriate operational systems rather than being copied indiscriminately into the passport. The DBP or BESS Evidence Graph can instead identify relevant data sources, preserve provenance and govern access to the evidence.

Algorithmic access requires additional controls. These may include the identity and legal principal of the algorithm, its version, delegated mandate, permitted action, asset scope and applicable assurance or certification evidence. Policy decisions and consequential automated actions should remain auditable.

5.5.4. Activities, use cases and benefits enabled by Data Spaces

The Energy Data-X “Imbalance Settlement Quality” use case connects several previously separate processes. A metering point operator makes meter readings available to an authorized supplier or Balance Responsible Party. The data is aggregated and provided to a forecasting service. Where a deviation from the schedule is identified, flexibility can be requested from an authorized flexibility provider. Company and market-role credentials support fine-grained access decisions throughout this process. The transferable BESS use cases include:

- Regulatory access for market surveillance and conformity assessment.
- Product-safety investigations and condition monitoring.

- Predictive maintenance and anomaly detection.
- Flexibility aggregation and charging or dispatch optimization.
- Residual-value, financing and insurance assessments.
- Repair, repurposing, remanufacturing, recycling and take-back.

Portable role evidence reduces bilateral identity and access administration. Policies can be updated without rebuilding user groups in every participating application, while credential status supports suspension and revocation. For BESS operators, governed access to reliable lifecycle evidence can improve safety, maintenance planning and asset utilization. These benefits depend on production-quality governance and remain to be validated at operational scale.

5.5.5. Challenges and roadmap for scaling

The main challenge is **the governance underlying the credentials**. Each market, authority or professional role requires an authoritative source, eligibility rules, an authorised issuer and processes for issuance, monitoring, suspension, revocation and renewal. Similar role names across ecosystems do not necessarily imply equivalent responsibilities or levels of assurance. Cross-border deployment therefore requires governed role mappings and comparable identity-proofing and monitoring policies.

Secondly, that PLI status must not be implemented as a self-declared role. Eligibility and permitted access depend on the Batteries Regulation and its implementing framework, as well as the purpose and product scope of the request. Authorities likewise require evidence of their jurisdiction and competence, and of the mandate of the officer, system or service acting on their behalf.

Third, the fact that scaling the BESS Evidence Graph also requires common semantics, validation rules and data-quality controls. Carbon-footprint, state-of-health and performance data cannot be combined reliably unless measurement boundaries, units and calculation methods are compatible. Cryptographic verification establishes the origin and integrity of a claim, but not its factual correctness.

Finally, sector coupling introduces an additional interoperability challenge. Energy–mobility applications, such as EV charging and vehicle-to-grid services, require trusted exchange among battery operators, mobility providers, charging infrastructure and electricity-market actors. Energy–manufacturing applications similarly connect industrial equipment, storage assets, production systems and energy markets. These use cases require cross-sector mappings of identities, market roles, semantics and access policies without collapsing the governance autonomy of the participating ecosystems.

Subsequent work should extend from simple access control mechanisms to governed predictive-maintenance, aggregation, optimisation and sector-coupling agents.

5.6. DPPs, Data Spaces and EBWs: WE BUILD Practical Implementations

WE BUILD³² is a European large-scale pilot for the European Business Wallet (EBW). Two complementary activities illustrate how wallet-based trust can support future DPP ecosystems.

³² **WE BUILD** (Wallet Ecosystem for Business and payments Use cases on Identification, Legal representation and Data sharing) is a European Large-Scale Pilot project co-funded by the European Commission. The consortium focuses on testing and implementing practical use cases for the European Digital Identity (EUDI) Wallet and European Business Wallet (EBW), such as cross-border company creation, financial services, and secure data sharing, to reduce bureaucracy and enhance digital trust across the EU single market. More information can be found at: <https://www.webuildconsortium.eu/>

- The Agrifood demonstrator integrates reusable organisational onboarding and membership credentials with federated Data Space infrastructure.
- In parallel, a rail demonstrator involving voestalpine, DB Cargo and SBB focuses on verifiable product, environmental and transport evidence.

Together, they address **two distinct architectural functions**: the control plane for trusted participation and the evidence layer for verifiable product data.

5.6.1. Strategic focus and lifecycle scope

The Agrifood demonstrator addresses fragmentation across DjustConnect in Belgium, the DIH Agrifood Data Space in Slovenia and Tritom in Finland. These platforms differ in their onboarding procedures, identifiers and trust arrangements. Farmers and other participants may therefore be required to complete similar registration and verification processes several times.

The demonstrator explores whether an organisation that has been onboarded by one participating ecosystem can reuse a verifiable membership credential when joining another. The receiving ecosystem verifies the credential and requests only evidence or contractual acceptance not covered by the original onboarding. This establishes a foundation for an aggregated “Agri-X” federation while preserving the autonomy of its local ecosystems. The activity is not itself a DPP exchange implementation, but it demonstrates a trust layer that could subsequently support controlled access to product, farm and supply-chain information.

The rail demonstrator addresses another part of the DPP lifecycle. Product and compliance information for rail products is currently exchanged through partly manual processes, making verification, integration and carbon-footprint reporting costly. The demonstrator therefore pilots automated and verifiable evidence data exchange between the manufacturer voestalpine, the transport provider DB Cargo and the buyer SBB, including simulated certificate issuers.

5.6.2. Actors, roles and data space architecture

The Agrifood architecture includes participating organisations, authoritative identity sources, wallet providers, onboarding providers, credential issuers, relying parties and Data Space operators. Participating ecosystems onboard members, issue membership credentials and verify credentials issued by other recognised participants.

Corporate, farmer and agricultural identifiers differ substantially across Member States. Finland and Belgium can draw on business or farmer registers, whereas equivalent registration coverage is not available in all jurisdictions. The architecture therefore does not depend on a single cross-ecosystem participant registry. Instead, EBWs hold credentials issued by recognised authorities or ecosystem operators, while trust lists and governance rules determine which issuers and credential types are accepted.

The MVP demonstrated that an EBW-ready wallet and credential solution can be integrated directly with Eclipse Dataspace Components (EDC) infrastructure, using the Dataspace Protocol (DSP) for governance and the Decentralized Claims Protocol (DCP) for credential presentation.

Membership credentials can thus inform Data Space participation and future policy decisions without replacing the underlying data-transfer protocols.

The rail demonstrator uses a direct issuer–wallet–verifier architecture rather than a Data Space protocol. Organisations and serialized products are identified, and product passports, declarations and environmental or transport evidence are issued as W3C Verifiable Credentials. A trusted issuer list establishes the trust domain across the participants. This architecture could later be combined with a sectoral Data Space such as Rail-X.

The combined model separates three interoperable layers:

- the EBW trust layer for identities, roles, credentials and attestations;
- the Data Space control layer for participation and usage policies;
- the evidence layer for verifiable product, environmental and supply-chain information.

5.6.3. DPP content, identification and access via the data space

The Agrifood membership credential contains the participant’s organisational identity, ecosystem membership and a reference to the applicable rulebook or participation conditions. This allows a receiving ecosystem to determine which onboarding requirements have already been satisfied and which remain outstanding.

Identifier heterogeneity remains a central constraint. Depending on the jurisdiction and use case, relevant identifiers may include business-register numbers, VAT identifiers, sector-specific registrations, and agricultural subsidy identifiers—such as CAP/IACS (Common Agricultural Policy / Integrated Administration and Control System) codes.

The demonstrator primarily uses W3C Verifiable Credentials and JSON-LD, with SD-JWT-based approaches considered as an alternative. JSON-LD supports extensible semantic contexts and RDF-compatible representations, which are relevant when credential attributes are incorporated into Evidence Graphs. SD-JWT provides selective disclosure for JSON claims but depends more strongly on shared schemas and external governance to preserve semantic consistency. In either case, interoperability requires governed vocabularies, versioning and change-management procedures in addition to cryptographic verification.

The rail DPP links the serialized product to machine-readable and verifiable evidence, including product information, declarations of performance, environmental product declarations and transport-related carbon data. JSON-LD contexts support semantic linking and provenance across the evidence chain. The demonstrator also explores verifiable aggregation of carbon-footprint evidence across production and transport stages.

The rail activity demonstrates verifiable and selectively disclosable evidence, but not a granular policy engine. Access-controlled Evidence Graphs, with policies reflecting actor roles, purposes and legal entitlements, remain a subsequent architectural step.

5.6.4. Activities, use cases and benefits enabled by data spaces

The Agrifood MVP defines three principal flows:

1. A legal person completes onboarding with a participating local data-sharing ecosystem and receives a verifiable membership credential.
2. The participant presents this credential when joining another participating ecosystem. The receiving platform verifies it and, where requirements differ, requests only the outstanding evidence or acceptance of additional conditions.
3. A participant previously onboarded through conventional means requests a membership credential through its existing platform account, enabling established members to adopt the wallet-based model without repeating the full onboarding process.

These flows reduce duplicated identity proofing and administrative effort. Economically, reusable credentials lower onboarding and transaction costs, while federation broadens the number of accessible counterparties and potential services. The same trust model could support farm, field and equipment passports; machinery maintenance and lending; subsidy applications; supply-chain finance; and controlled access to sustainability or compliance information. In the rail demonstrator, voestalpine creates the product record and requests or receives environmental evidence, DB Cargo contributes transport-related evidence, and SBB verifies the resulting DPP and associated credentials. Machine-readable data can subsequently be integrated into ERP, procurement, maintenance and compliance processes. Standardised evidence templates and trusted issuers can reduce manual validation and compliance effort.

Taken together, the demonstrators show that the trust framework and the evidence layer can be implemented independently and later combined according to sector requirements.

5.6.5. Challenges and roadmap for scaling

5.6.5.1. Governance and federated assurance

Technical interoperability does not by itself create federation. Production deployment requires governance for authorised issuers, credential types, schemas, rulebooks, revocation and monitoring. Level-of-Assurance requirements must also be comparable across ecosystems, including identity proofing, onboarding controls and operational supervision. Trust cannot become automatically transitive merely because credentials are technically interoperable.

5.6.5.2. Evidence Graphs and architectural interoperability

Scaling the rail model requires consistent calculation boundaries, provenance rules and aggregation methods for environmental evidence. Future implementations should add granular policy enforcement for role-, purpose- and context-dependent access. The two demonstrators also indicate that DPP architectures should remain protocol-neutral. Some sectors may use EDC-based Data Spaces, while others may initially rely on direct credential exchange. EBWs and verifiable evidence should therefore complement, rather than depend on, one specific transfer architecture. Production readiness additionally requires validation of throughput, latency, availability, security and wallet interoperability.

5.6.5.3. Transferability, AI and future research

The Agrifood federation model is transferable to other fragmented sectors and to cross-sector applications such as energy–mobility, energy–manufacturing and quality–infrastructure–manufacturing integration. Such sector coupling may create substantial resilience and macroeconomic benefits by reducing repeated onboarding and enabling trustworthy exchange across existing ecosystem boundaries.

Over time, DPP infrastructure may also support a continuum of physical, digital and AI-enabled products. This requires moving from document-oriented exchange towards access-controlled and verifiable Evidence Graphs based on open-world semantics. Such infrastructure could enable AI agents to retrieve and process evidence while preserving provenance, authorisation and accountability.

WE BUILD demonstrates relevant building blocks for this development: reusable organisational credentials, EBW integration with Data Space infrastructure, semantic verifiable evidence and cross-organisational verification. It does not yet demonstrate a complete AI-ready DPP infrastructure. The principal next steps are governance at scale, assurance interoperability, granular policy enforcement and performance validation under industrial operating conditions.

6. Conclusions and Recommendations

6.1. Conclusions: From Regulatory Compliance to Unprecedented Data Exploitation

The operationalization of the ESPR imposes systemic, highly heterogeneous challenges across industrial value chains. While digitally mature verticals navigate complex telemetry, asymmetric supply chains face acute identification and digital capability gaps. However, framing the DPP strictly as a passive, document-based reporting burden fundamentally misinterprets its industrial potential.

The core conclusion of this work is that ESPR implementation – when built upon the Internet of Product Data (IoPD) architecture – represents the catalyst for an unprecedented paradigm shift: transitioning European industry from *compliance-by-document* to *competitiveness-by-data*. By converging B2B Sovereign Data spaces (governance), Asset Administration Shells (semantics), and European Business Wallets (trust), the IoPD architecture provides an extensible infrastructure that far transcends regulatory compliance, unlocking product data exploitation at a scale previously unattainable:

- **Unlocking “Beyond-Compliance” Data Exploitation:** The IoPD architecture bridges mandatory ESPR payloads with voluntary, high-value B2B data exchanges. By establishing a zero-trust, semantically harmonized backbone, economic operators can securely monetize premium product intelligence – such as real-time predictive maintenance streams, secondary material provenance, and performance analytics- without exposing trade secrets.
- **Production & Process Optimization:** Decoupling underlying infrastructure from application interfaces allows manufacturers to ingest verified multi-tier supply chain data directly into ERP and PLM systems. This streamlines Shop-Floor-to-Passport workflows, reduces operational friction, and drives Industry 5.0 manufacturing efficiencies.
- **Maximizing European Industrial Competitiveness:** Deploying open, non-proprietary standards prevent vendor lock-in and safeguards European data sovereignty. It empowers EU enterprises –

particularly micro-SMEs– to lead global markets through data-driven servitization, circular finance and superior product transparency.

While the IoPD baseline (Data Spaces, AAS and EBWs) address immediate ESPR requirements, its long-term value lies in providing a sovereign, machine-readable substrate for industrial AI ecosystems. By structuring lifecycle data into deterministic, identity-anchored payloads, the architecture ensures that future autonomous agents, predictive analytics, and cyber-physical systems consume verifiable product intelligence rather than ungrounded claims. As the ecosystem matures, this foundation can seamlessly integrate advanced semantic graph capabilities and low-latency processing layers to support next-generation industrial AI applications across European value chains.

6.2. Strategic Recommendations for Economic Operators

- **Adopt a “Beyond-Compliance” Data Strategy:** Shift enterprise positioning from passive regulatory reporting to proactive data asset management. Analyse upstream supplier inputs and downstream usage patterns to optimize internal manufacturing processes, enhance supply chain resilience, and enable data-driven lifecycle services.
- **Mitigate Structural and Physical Constraints Early:** Evaluate sector-specific constraints –including non-standard product form-factors, commercial privacy risks, and IP exposure– to select resilient identifier and resolution architectures well in advance of enforcement timelines.
- **Deploy Modular, Phased Implementation Roadmaps:** Avoid monolithic software migrations and complex initial on-premise developments. Utilize Data-Space-as-a-Service (DSaaS) managed infrastructure or ready-to-use commercial solutions and execute single-VC pilots. Validate peer-to-peer data handshake with trusted Tier-1 suppliers before expanding across multi-tier networks.

6.3. Strategic Recommendations for Policy Makers & Regulators

- **Establish Clear Frameworks for Data Sovereignty and Governance:** Define unambiguous legal rules regarding data ownership, liability, and usage rights in federated networks, simplifying compliance while safeguarding industrial trade secrets and encouraging voluntary data sharing.
- **Incorporate Regulatory Flexibility for Complex Edge Cases:** Design delegated acts with flexible compliance mechanisms that accommodate extreme physical, technical or IP constraints across specialized product categories without compromising overall system integrity.
- **Deploy Comprehensive Support and Accompaniment Programs for SMEs:** Combine financial support for open-source starter kits and managed DSaaS platforms with structured technical accompaniment, training and advisory services under the Digital Europe Programme (DEP) and regional innovation instruments.
- **Harmonize ESPR Data with Extended Producer Responsibility (EPR) Systems:** Interconnect DPP data endpoints directly with Producer Responsibility Organization (PRO) management frameworks to automate eco-modulation fee calculations and streamline end-of-life compliance reporting across Member States.

Annex A: Alignment Matrix with CIRPASS D4.1 Reference Architecture

This annex establishes a 1:1 technical mapping between the 25 architectural recommendations defined in CIRPASS Deliverable D4.1 (*System Architecture for the Digital Product Passport*) and their operational execution within the Internet of Product Data (IoPD) stack. It categorizes each recommendation across the four functional IoPD layers: Identity & Cryptographic Trust (Layer 1), Exchange Governance & Sovereignty (Layer 2), Data Payload & Semantics (Layer 3), and Applications & Value Creation (Layer 4).

CIRPASS2 D4.1 Recommend.			Contributing IoPD Layers		Technical Execution Mechanism in the IoPD Stack	
3.1. Standardize exchange format as JSON-LD		Layer 3 (Payload/Semantics) Layer 4 (Apps)		Serialization of domain ontologies, application profiles, or AAS submodels in W3C JSON-LD exposed via standardized REST APIs.		
3.2. Make use of modular DPP templates		Layer 3 (Payload/Semantics)		Encapsulation of modular templates via SEMIC Application Profiles or IDTA Submodel Templates (e.g., DppMetadata IDTA 02099-1) with ECLASS/IEC CDD anchoring.		
3.3. Enrich standard lifecycle API (JTC24)		Layer 2 (Data Spaces) Layer 3 (Payload/Semantics)		Dynamic CRUD lifecycle operations executed over the Dataspace Protocol (DSP) using normalized OpenAPI interfaces (supporting W3C Linked Data or AAS Part 2 APIs).		
3.4. Align with APIs for value-added services		Layer 2 (Data Spaces) Layer 4 (Apps)		Decoupled B2B software interfacing via connectors enabling circular economy services, Product Carbon Footprint (PCF) calculations, and value-added passports.		
3.5. Link to product component DPPs		Layer 3 (Payload/Semantics)		Digital Twin nesting via W3C schema:hasPart URI references or globalAssetId attributes across sub-components without physical data duplication.		
3.6. Use Verifiable Credentials for identity		Layer 1 (Trust/Identity)		Counterparty authentication via W3C/SD-JWT organizational credentials managed through the European Business Wallet (eIDAS 2.0).		
3.7. Use generic roles for RBAC		Layer 1 (Trust/Identity) Layer 2 (Data Spaces)		Qualified Electronic Attestation of Attributes (QEAA) dynamically evaluated during ODRL access policy negotiations within the EDC connector.		

CIRPASS2 D4.1 Recommend.			
Contributing IoPD Layers		Technical Execution Mechanism in the IoPD Stack	
3.8. Structure DPP for role-based access control	Layer 2 (Data Spaces) Layer 3 (Payload/Semantics)	Payload segmentation into independent domain ontologies or IDTA submodels granularly gated based on signed usage terms in the Control Plane.	
3.9. Ensure credentials issued by trusted bodies	Layer 1 (Trust/Identity)	Decentralized verification of credential issuers and public keys of QTSPs or public authorities via the EBSI trust registry.	
3.10. Expose DPPs as Verifiable Credentials	Layer 1 (Trust/Identity) Layer 3 (Payload/Semantics)	Packaging semantic payloads (W3C JSON-LD graphs or AAS submodels) into Verifiable Credentials signed via Qualified Electronic Seals (e-Seals) under JOSE/JWS envelopes.	
3.11. Ensure immutability of DPP records	Layer 1 (Trust/Identity) Layer 2 (Data Spaces)	Append-only lifecycle event recording chained via cryptographic hashes and non-repudiable digital transaction sealing.	
3.12. Provide and record update receipts	Layer 2 (Data Spaces)	Automatic, cryptographically signed bi-directional transaction receipt generation at the receiving connector upon data ingress completion.	
3.13. Utilize trusted third parties for trust anchoring	Layer 1 (Trust/Identity)	Public decentralized anchoring of revocation schemas and identity credentials on the sovereign European EBSI infrastructure.	
3.14. Establish a DPP reporting system	Layer 1 (Trust/Identity) Layer 4 (Apps)	Real-time validation of e-Seal signatures and revocation statuses via Bitstring Status Lists exposed in market surveillance portals.	
3.15. Align back-up functionality with primary storage	Layer 2 (Data Spaces) Layer 3 (Payload/Semantics)	Synchronized replication of semantic datasets (JSON-LD payloads or AAS submodels) across secondary DPPSP connector nodes maintaining identical ODRL usage control policies.	
3.16. Ensure UPI-to-URI redirection (rEO)	Layer 2 (Data Spaces)	Decentralized redirection/resolution service linking the persistent unique product identifier (UPI) to the dynamic catalog of the EDC connector.	
3.17. Establish fallback EU UPI-to-URI service	Layer 2 (Data Spaces) Layer 4 (Apps)	Centralized EC resolution mechanism acting as a redirection service of last resort upon primary rEO or DPPSP node unavailability.	

CIRPASS2 D4.1 Recommend.			Contributing IoPD Layers		Technical Execution Mechanism in the IoPD Stack	
3.18. Provide discoverable model-level data endpoint			Layer 3 (Payload/Semantics) Layer 4 (Apps)		Public exposure of Model/Type-level data (Core Vocabulary descriptors or Type AAS) at the standardized /.well-known/dppdata endpoint to prevent scraping of sensitive item-level data.	
3.19. Create data carrier for online/pre-purchase			Layer 4 (Apps)		Web URL resolution and digital links (GS1 Digital Link) routing e-commerce interfaces directly to public product submodels/ontologies.	
3.20. Product needing updates requires item-level UPI			Layer 3 (Payload/Semantics)		Instantiation of item-level digital twins (serialized W3C item graphs or assetKind = Instance) individually identified for post-sale lifecycle event logging.	
3.21. Implement caching for high volume access			Layer 2 (Data Spaces) Layer 4 (Apps)		Deployment of read replicas in the connector Data Plane and edge nodes to optimize bulk queries under strict expiration policies.	
3.22. Assign storage of DPP updates to responsible EO			Layer 2 (Data Spaces) Layer 3 (Payload/Semantics)		Distributed sovereign storage within the rEO enterprise environment (ERP/ PLM), externally exposed as immutable payload appendices (JSON-LD / AAS).	
3.23. Establish EU repository with key data for search			Layer 3 (Payload/Semantics) Layer 4 (Apps)		Centralized indexing on the EC Web Portal of non-confidential attributes extracted from SEMIC Application Profiles or DppMetadata submodels.	
3.24. Create universal symbol set for key DPP data			Layer 4 (Apps)		Normalized frontend rendering mapping IRDIs (ECLASS/IEC CDD) to standardized EU iconographic sets.	
3.25. Develop standardized display templates			Layer 4 (Apps)		Structured rendering of JSON-LD payloads via homogeneous HTML/CSS templates for direct browser access.	

Involved Organizations

BAI DATA
INTERNATIONAL DATA
ANALYTICS

imovalia
ASSOCIATION

cbt
COMMUNICATION ENGINEERING

 **POLITECNICO**
MILANO 1863

cea

 **PIACENZA**
CASHMERE

IDTA

 **EXPO21XX**
online exhibitions

 **Reverse**
Resources

 **TEXROAD**

 **MICHELIN**

GDSO
STANDARDIZE. SHARE. SIMPLIFY.

 **AVERY**
DENNISON

TNO

 **GTS**
GLOBAL TEXTILE
SCHEME

FUJITSU

 **SPHERITY**

