SPHERITY RESEARCH ARTICLE

Verifiable, Access-Controlled Digital Product Passports

Control-Plane Governance, Evidence-Graph Data Planes, Battery and BESS Applications, Industrial AI, and the Convergence with European Business Wallets

Carsten Stöcker
Spherity GmbH, Germany

Prepared: August 2026
Evidence cut-off: 31 July 2026

Core proposition. Trustworthy DPP and DBP transactions require two coupled planes: a control plane for legal-person identity, role, mandate and policy; and a data plane for decentralised, provenance-bearing product evidence.

Abstract

Digital Product Passports (DPPs) are commonly presented as product records reached through a data carrier. That description is legally useful but architecturally incomplete. A scalable industrial DPP ecosystem must also determine which legal person is acting, in which market role, under whose mandate, for which purpose, and with what right to see or change particular evidence. This article develops a two-plane model: a control plane for identity, role, mandate, trust, policy and decision; and a data plane for decentralised product data, signed attestations, provenance, lifecycle events and evidence graphs. It applies the model to Digital Battery Passports (DBPs) for traction batteries and to the wider, presently voluntary concept of a system-level passport for battery energy storage systems (BESS). It distinguishes the operational DPP Registry from decentralised DPP content and analyses how a future European Business Wallet (EBW), still a legislative proposal at the evidence cut-off, could reduce duplicated onboarding while preserving sectoral governance. A complete mapping of the 52 CIRPASS-2 lifecycle risks shows that signatures and authentication address only part of the threat model: authoritative role issuance, least-privilege access, revocation, freshness, accountable updates, resilient resolution, confidentiality controls and provenance-aware validation are also required. An energy data-X market-role use case illustrates runtime authorisation across organisations. The article then proposes verifiable evidence graphs as an AI-ready data-plane pattern and develops a BESS reference architecture. It concludes with a research agenda extending passport logic across a continuum from passive products to connected systems, AI services and hybrid physical-agentic products, while clearly separating current legal duties from forward-looking design proposals.

Keywords. Digital Product Passport, Digital Battery Passport, DPP Registry, European Business Wallet, legal-person identity, product-linked identity, verifiable credentials, authorisation, evidence graph, BESS, trusted AI, industrial AI, supply-chain compliance, cyber-physical products

Contents

List of Figures

List of Tables

Executive proposition

The DPP is evolving from a largely static disclosure instrument into a governed interface to product evidence. The transition is not a single technology upgrade. It changes the unit of trust from "a document published by a company" to "a purpose-bounded evidence transaction performed by an identified and authorised actor." The resulting architecture has two coupled planes. The control plane answers who may do what, for which product or asset, on whose authority, and under which rule. The data plane supplies the product facts, events and provenance that a decision consumes. Neither plane is sufficient alone. Identity without evidence produces an authenticated assertion that may still be wrong. Data without governed access produces either an unusable silo or an indiscriminate disclosure channel.

The target architecture is framed in Figure 1.

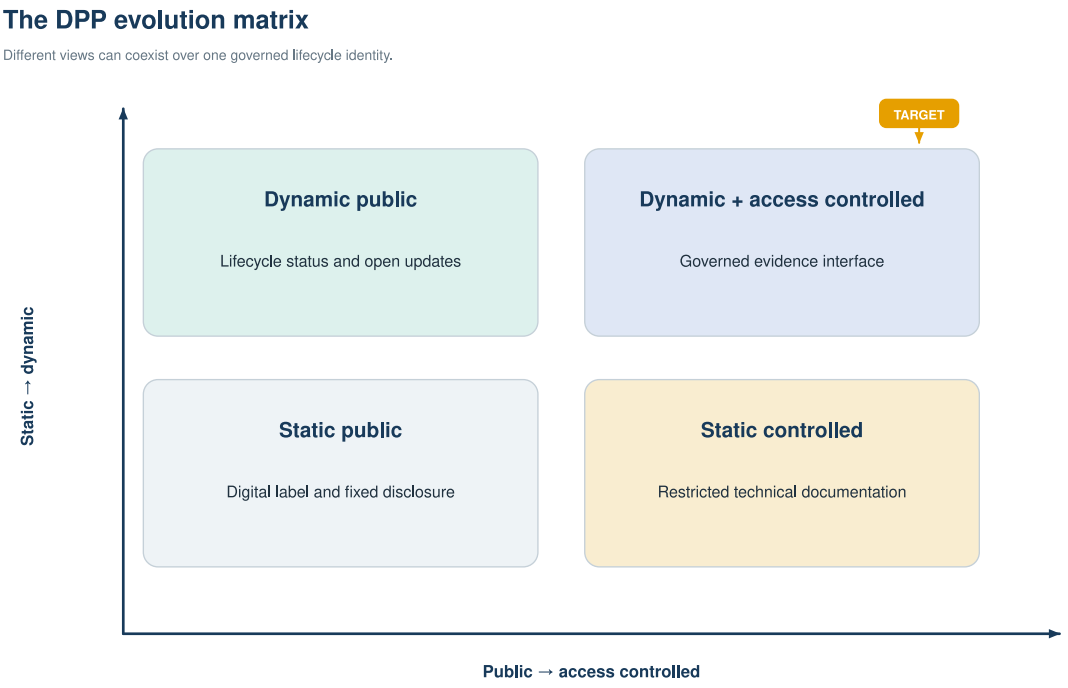

Figure 1: DPP evolution matrix: from static public disclosure to dynamic, access-controlled evidence. *Spherity research adapted from Stöcker [6].*

The article makes four contributions. First, it converts the author's two 2×2 matrix methodologies into a reference architecture grounded in the Ecodesign for Sustainable Products Regulation (ESPR), the Batteries Regulation, the DPP Registry, European digital-identity law and the proposed EBW. Second, it specifies market-role governance as an institutional design problem rather than a credential-format problem. Third, it shows how evidence graphs can preserve provenance and validation context across supply-chain and AI decisions without moving all operational data into a graph. Fourth, it tests the model against traction batteries, BESS and every risk in the CIRPASS-2 risk catalogue. The result is intended as a design and governance framework, not as a claim that every proposed component is already mandated by EU law.

1 Introduction: from disclosure artefact to governed evidence infrastructure

European product policy is creating a new digital interface between products, economic operators, authorities, service providers and end users. Under Regulation (EU) 2024/1781 [1], a DPP is a product-specific data set accessible electronically through a data carrier in accordance with a delegated act. Regulation (EU) 2023/1542 [2] makes a battery passport mandatory from 18 February 2027 for each light means of transport battery, each industrial battery with a capacity greater than 2 kWh, and each electric-vehicle battery. These instruments turn product information from a scattered collection of declarations, technical files, labels and enterprise records into a lifecycle-accessible compliance object. The policy promise is substantial: better market surveillance, more informed purchasing, safer repair and repurposing, improved recycling, more reliable due diligence, and lower reporting friction.

Yet a product record does not become trustworthy merely because it is digital, signed or reached through a QR code. Every high-value use of a DPP raises governance questions. Is the presenter the manufacturer, importer, authorised representative, repair workshop, market surveillance authority, customs officer, second-life operator or recycler it claims to be? Is that legal person entitled to act in that role for this jurisdiction and product class? Is the human or software agent acting under a valid mandate? Does the requester need the full evidence or only a derived conformity statement? Is the evidence current, traceable to an authoritative source, and still valid after an incident, ownership transfer or product modification? Can an authority distinguish an authentic but incomplete DPP from a complete but fraudulent one? These are not edge cases. They are the conditions under which the DPP moves from publication to operational decision support.

The CIRPASS-2 risk study makes this point empirically. Its 52 risks span creation, storage, retrieval, update and deletion. They include excessive or insufficient disclosure, false economic operators, impersonation, denial of service, carrier substitution, interception, strategic intelligence leakage, inaccurate updates and false end-of-life reporting [3]. Some risks are technical; others arise from incentives, unclear responsibility, bad process or abuse by an otherwise authorised party. Consequently, no single control, neither a signature, a blockchain, a central registry nor an access-control list, can secure the DPP lifecycle. A layered system must combine institutional authority, technical verification and accountable operational procedures.

This article addresses five research questions. RQ1 asks how control-plane and data-plane responsibilities should be separated without fragmenting the user journey. RQ2 asks how legal-person identity, representation and market-role credentials can support runtime access decisions. RQ3 asks what the DPP Registry does, and deliberately does not do, in this architecture. RQ4 asks how traction-battery and BESS use cases expose different passport boundaries and evidence needs. RQ5 asks how the same infrastructure could support trusted industrial AI and an AI Service Passport while remaining honest about legal status.

The proposed answer is a federated trust architecture. The control plane provides legal-person identity, product-linked identity, role, mandate, credential status, purpose, policy and audit. The data plane provides identifiers, observations, declarations, certificates, lifecycle events, transformations, evidence relationships and proofs. A policy decision point joins them at runtime. The DPP Registry indexes identifiers and registration metadata and supports authorities and customs; it is not the universal store for detailed DPP content. A future EBW could provide a reusable container and trust service for legal-person credentials, mandates, qualified attestations and presentations. Sectoral authorities would still determine what a "recycler," "workshop" or "energy market participant" is allowed to do.

This framing matters for European competitiveness. If every DPP service rebuilds company onboarding, power-of-attorney management, role verification, revocation checking and evidence exchange, Europe will digitise obligations while preserving administrative duplication. If common trust services and sector-specific policy can interoperate, the same verified company identity and authoritative evidence may support customs, market surveillance, financing, reporting, repair, recycling and supply-chain transactions. The macroeconomic gain comes not from replacing every database, but from making evidence reusable under policy.

Table 1 records the legal and policy baseline used in the analysis.

Table 1: Legal and policy status at the evidence cut-off

Instrument or capability	**Status, 31 July 2026**	**Architectural consequence**
ESPR, Regulation (EU) 2024/1781	Enacted; product-group duties depend on delegated acts	Horizontal DPP framework; Articles 9–15 govern system design.
Batteries Regulation (EU) 2023/1542	Enacted; DBP duty applies from 18 February 2027	Passport for each LMT, industrial >2 kWh and EV battery.
DPP Registry	Operational since 20 July 2026	Indexes identifiers and registration metadata; does not centralise the complete DPP.
DPP harmonised standards	Six standards cited by Decision (EU) 2026/1736	Interoperability baseline; access/security and authentication standards not yet OJEU-cited at cut-off.
European Business Wallet	Commission proposal COM(2025) 838; Council position adopted	Potential future legal-person, mandate and evidence presentation layer; not enacted law.
BESS system passport	Architectural/sector proposal	Must be distinguished from the mandatory product-level battery passport.
AI Service Passport	Architectural proposal	Not a DPP category mandated by ESPR or the AI Act.

Source: Spherity research; legal status and claim boundaries are documented in the source register.

2 Methodology, scope and epistemic discipline

The research combines doctrinal analysis, architecture synthesis, risk-to-control mapping and reference-use-case design. The legal baseline comprises ESPR, the Batteries Regulation, the eIDAS framework as amended, the Single Digital Gateway and Once-Only Technical System (OOTS), the Union Customs Code, market-surveillance law, the AI Act, the Cyber Resilience Act (CRA), NIS2 and the Commission proposal for an EBW. Legal texts and official Commission, Council, Parliament and standards-body materials are treated as primary sources. The evidence cut-off is 31 July 2026. This date is material because the DPP Registry became operational on 20 July 2026, its first user guide was updated on 28 July [4, 5], and the EBW legislative file was still in negotiation.

Three author-linked sources provide conceptual and implementation evidence. The author's 2×2 Matrix essay supplies the static-to-dynamic and public-to-access-controlled vision [6]. Two EBW papers develop the industrial identity and simplification thesis [7, 8]. The energy data-X paper provides an implemented market-role pattern for cross-company energy data exchange [9]. The evidence-graph paper supplies the data-plane model for provenance-aware industrial AI [10]. Because these sources include the author's own work and projects connected to Spherity,

the article separates observed implementation facts, legal requirements, architectural inference and normative proposal.

The risk analysis uses the full CIRPASS-2 list rather than a selected subset. Each risk is assigned to a primary lifecycle phase, threat type, relevant plane, preventive or detective controls, residual risk and implementation priority. The mapping is intentionally many-to-many: one risk may require governance, identity, policy, data integrity and availability controls. Conversely, a control such as credential-status checking mitigates several impersonation and unauthorised-update risks. Appendix A preserves one row per CIRPASS-2 risk to make omissions visible.

The architecture method is capability-based. It asks which decisions the ecosystem must make before selecting a specific data model, credential format, wallet, connector or storage product. The analysis therefore distinguishes an obligation from one implementation option. For example, integrity and issuer binding may be implemented through W3C Verifiable Credentials, signed JSON, qualified electronic seals or another conformant mechanism. An Asset Administration Shell (AAS) [11] may be a strong source model or adapter without becoming the universal data plane. A dataspace connector may enforce usage policy without being legally mandatory for DPP access. A graph may materialise evidence relationships without replacing the time-series platform that stores high-frequency telemetry.

The article uses a "legal status ladder" to discipline claims. "Enacted" denotes binding Union law in force, although application dates may be future. "Operational" denotes deployed infrastructure or guidance. "Proposed" denotes a legislative or policy proposal. "Standardised" denotes a published or OJEU-cited standard, with the status stated precisely. "Implemented in a reference use case" denotes demonstrated functionality, not a general legal requirement or production guarantee. "Architectural proposal" denotes the author's synthesis. This classification is crucial where policy momentum can otherwise be mistaken for current obligation.

Limitations remain. The DPP legal framework is horizontal and product-specific delegated acts will determine detailed data requirements and access rights. The Commission Registry services and user journeys will evolve. Market-role authority differs across Member States and sectors. The BESS reference architecture spans products, systems and operational services that are governed by different bodies of law. The AI Service Passport is not a statutory DPP category. Finally, evidence quality cannot be inferred from cryptographic validity alone. The proposed model makes these limitations explicit and turns them into requirements for governance, interoperability testing and empirical evaluation.

3 Legal and operational baseline at the evidence cut-off

ESPR establishes the horizontal DPP framework. Product-specific delegated acts determine whether a DPP is required, the data elements, data carrier, access rights, update responsibilities and other product-group details. Articles 9 to 15 create the core system logic, including unique identifiers, access, processing and the DPP Registry. The Registry was placed into operation on 20 July 2026 under Commission Implementing Regulation (EU) 2026/1778 [12]. Its purpose is indexing and supporting verification and enforcement, not centralising every detailed product record. The Commission describes registration data, identifiers and high-level metadata as Registry content, while the responsible economic operator or service provider continues to host detailed DPP information in a decentralised manner.

The Registry user guide [5] illustrates the current enrolment trust path. An applicant signs in through EU Login, enrols an organisation, supplies legal identifiers and contact and representation information, downloads a Commission-sealed declaration, signs it with a qualified electronic signature or seal via a qualified trust service provider, and uploads it for validation. Once the

organisation is verified, its administrator can register DPP information, including a unique product identifier that resolves to the hosted DPP. This is a practical, document-centred onboarding workflow. It establishes an accountable organisation and representative, but it is not yet a universal, continuous wallet-based authorisation layer.

The Batteries Regulation [2,13] creates the first prominent sectoral DPP implementation. Article 77 and Annex XIII specify the passport scope and information categories. Responsibility lies with the economic operator placing the finished battery on the market or putting it into service; component and module suppliers contribute evidence but do not thereby become the legally responsible passport issuer. The regulation differentiates access categories and permits restricted access for information such as detailed composition where justified. The battery passport is therefore already more than a public label. It is a structured lifecycle record with differentiated users and update responsibilities.

The system boundary requires care. A traction battery is a regulated product within the passport scope. A stationary industrial battery above 2 kWh is likewise in scope. A BESS, however, is an engineered system comprising battery units, battery-management systems, inverters, energy-management software, communications, safety systems, site configuration and grid or market services. A product-level battery passport does not automatically describe the installed system, its configuration, operational history or contractual market role. A BESS passport can be proposed as a voluntary system dossier or sectoral extension, but it should not be presented as an already mandatory Union passport for the complete installation.

European identity law supplies relevant primitives. The eIDAS framework [14] regulates electronic identification and trust services, including qualified electronic signatures and seals. Directive (EU) 2025/25 [15] on digital tools in company law introduces the EU Company Certificate and a digital EU power of attorney, with implementation dates extending beyond the evidence cut-off. These instruments improve authoritative company and representation evidence. The EBW proposal, COM(2025) 838 [16], aims to provide legal persons and public bodies with a wallet for identity, attributes, mandates, trusted exchange and signatures or seals. It explicitly anticipates machine and agentic uses. Nevertheless, at 31 July 2026 it remained a Commission proposal: the Council had adopted its negotiating position on 9 June 2026 [17], while European Parliament work was ongoing [18].

Standards status is similarly dynamic. Commission Implementing Decision (EU) 2026/1736 [19, 20] cited six harmonised DPP standards covering exchange protocols, identifiers, data carriers, persistence, lifecycle APIs and system interoperability. Two further standards concerning access-rights management/security/confidentiality and data authentication/reliability/integrity were expected later in 2026 and should not be treated as OJEU-cited at the cut-off. W3C Verifiable Credentials Data Model 2.0, Data Integrity, DID Core, JSON-LD, SHACL and PROV-O [21–26] provide broadly applicable technical components, but W3C itself does not define a complete authorisation regime. Sectoral governance must supply validation and policy.

Figure 2 links the product and organisation identity domains.

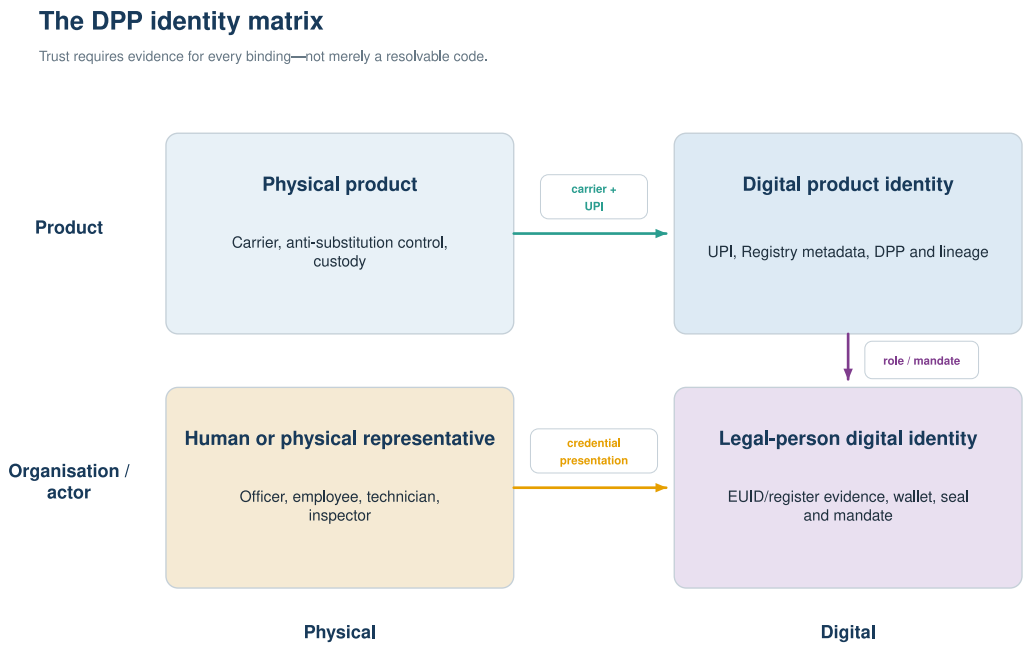

Figure 2: DPP identity matrix: linking physical and digital identities for products and legal persons. *Spherity research adapted from Stöcker [6].*

Table 2 allocates the main responsibilities between the two planes.

Table 2: Control plane and data plane responsibilities

Dimension	Control plane	Data plane
Question	Who may do what, for which object, purpose and time?	What evidence supports the claim or decision?
Core objects	Legal person, role, mandate, issuer, policy, status, decision	Product identity, claim, observation, document, event, version, provenance
Typical services	Wallet, trust list, credential verifier, policy engine, audit	DPP host, API, AAS, document store, evidence graph, historian
Failure if isolated	Authenticated actor may still submit false or unsupported claims	Accurate data may be disclosed or changed by an unauthorised party
Binding	Decision token or capability scoped to transaction	Evidence projection and update linked to the decision

Source: Spherity research; legal status and claim boundaries are documented in the source register.

4 The two 2×2 matrices as an architectural research agenda

The first matrix positions DPPs along two axes: static versus dynamic and public versus access controlled. A static-public DPP resembles a digital label or fixed compliance disclosure. It is valuable for consumer information and basic verification, but it captures only a snapshot and cannot safely expose confidential evidence. A static-controlled DPP adds differentiated access, for example, an authority can inspect a technical document not available to the public, but its temporal model remains limited. A dynamic-public DPP publishes lifecycle changes, such as repair or recall status, but risks leaking commercial or security-sensitive information. The target

quadrant is dynamic and access controlled: a living evidence interface whose views and actions depend on verified role, purpose and policy.

The matrix should not be read as an evolutionary claim that every use must move to maximum dynamism and restriction. Public, stable facts remain appropriate for an open view. Product instructions, basic sustainability indicators and recall information may need frictionless access. Conversely, composition details, vulnerability information, commercial dependencies and high-resolution operational data may require restricted views. The architectural insight is coexistence: one product identity can support several policy-governed projections over a changing evidence base.

The second matrix distinguishes physical versus digital identity and product versus organisation. Legal-person identity occupies the organisation/digital quadrant. The product identifier and product-linked identity occupy the product/digital quadrant. The physical product is bound to its digital representation through a data carrier, identifier and anti-substitution controls appropriate to the risk. Human representatives and software agents operate on behalf of the legal person through mandates. The runtime transaction therefore links at least four things: product identity, organisation identity, actor or agent authority, and requested operation.

This identity matrix reveals why a QR code alone cannot create trust. The code can resolve a product identifier, but it does not prove that the affixed carrier belongs to the physical product, that the hosted data comes from the responsible economic operator, or that the requester is authorised. Each relationship needs evidence. Product-to-carrier binding may use tamper-evident labels, secure elements, serialisation, manufacturing records or inspection procedures. Product-to-DPP binding uses the unique identifier and Registry metadata. Organisation-to-claim binding may use a signature or seal and trusted issuer chain. Actor-to-organisation binding uses representation or mandate. Request-to-purpose binding uses policy and transaction context.

The matrices also clarify the shift from document exchange to decision infrastructure. A document-centric process asks whether a file is present and signed. An evidence-centric process asks which claims are needed for a decision, who issued each claim, under what authority, with which validity interval, based on which observation or source, and whether contradictory or missing evidence remains. The latter can support partial disclosure and automated validation because it models evidence at a finer granularity.

The resulting architecture is not a single European database. It is a federation with shared identifiers, minimum interoperability rules, authoritative trust anchors, decentralised stores and policy-enforcement points. The control plane can be shared across many evidence transactions; the data plane can remain distributed across product manufacturers, suppliers, service providers, authorities and system operators. Common trust services reduce repetitive onboarding, while local policy preserves the competence of sectoral authorities.

The matrices therefore generate testable hypotheses. H1: reusable legal-person and mandate credentials reduce onboarding cost only if sectoral role issuers and relying parties accept common assurance profiles. H2: access-controlled dynamic DPPs reduce confidentiality risk only if policy decisions use both actor attributes and data classifications. H3: evidence graphs improve AI auditability only if provenance, validation results, versions and credential status are preserved. H4: Registry–wallet convergence improves enforcement only if identifier binding and revocation can be checked reliably at runtime. H5: a system-level BESS passport creates additional value only if its boundary and update responsibility are explicit.

5 Control plane: identity, authority, policy and accountable action

The control plane is the set of services and governance arrangements that decide whether an actor may perform an operation. Its minimum inputs are the product or asset identifier, the requesting legal person, the human or machine representative, the asserted market role, the mandate, the requested action, the purpose, the data classification and relevant context. Its outputs are an allow, deny or obligation-bearing decision and an auditable explanation. The decision may require selective disclosure, data minimisation, a time limit, an onward-sharing restriction or additional approval.

Legal-person identity is the anchor, not the complete answer. A legal identifier such as a national registration number, VAT identifier, Legal Entity Identifier or EUID helps identify an organisation. An authoritative register or qualified attestation can bind attributes to that organisation. A qualified electronic seal can bind a data object to a legal person and protect integrity. None of these facts alone establishes that the company is a recognised recycler for a particular waste stream, an authorised workshop for a product family, a customs declarant for the transaction, or a balance responsible party in an energy market. Authentication answers "who presented this credential or proof?" Authorisation answers "may this actor perform this operation now?"

Representation adds a second layer. A person may be employed by a company yet lack authority to register a DPP, disclose confidential composition data or report a battery as recycled. A service provider may manage DPPs for several clients. An AI agent may execute a workflow but only within a bounded mandate. The control plane therefore needs machine-verifiable representation: principal, delegate, scope, object or product family, permissible actions, validity period, delegation rights and revocation. Directive (EU) 2025/25 and the EBW proposal point toward reusable European company and power-of-attorney evidence, but relying parties must still interpret scope.

Product-linked identity (PLI) is the bridge between the actor and the product context. PLI is used here as an architectural term for verifiable assertions that bind a legal person to a product, product family, installation or lifecycle role. Examples include "workshop W is authorised to service product family P," "recycler R holds permit Q for battery chemistry C in jurisdiction J," or "economic operator E is responsible for DPP identifier D." A PLI credential should contain the issuing authority, subject legal person, role, scope, jurisdiction, product or asset binding, assurance level, validity, status endpoint and applicable policy vocabulary.

Figure 3 shows the coupled control- and data-plane architecture.

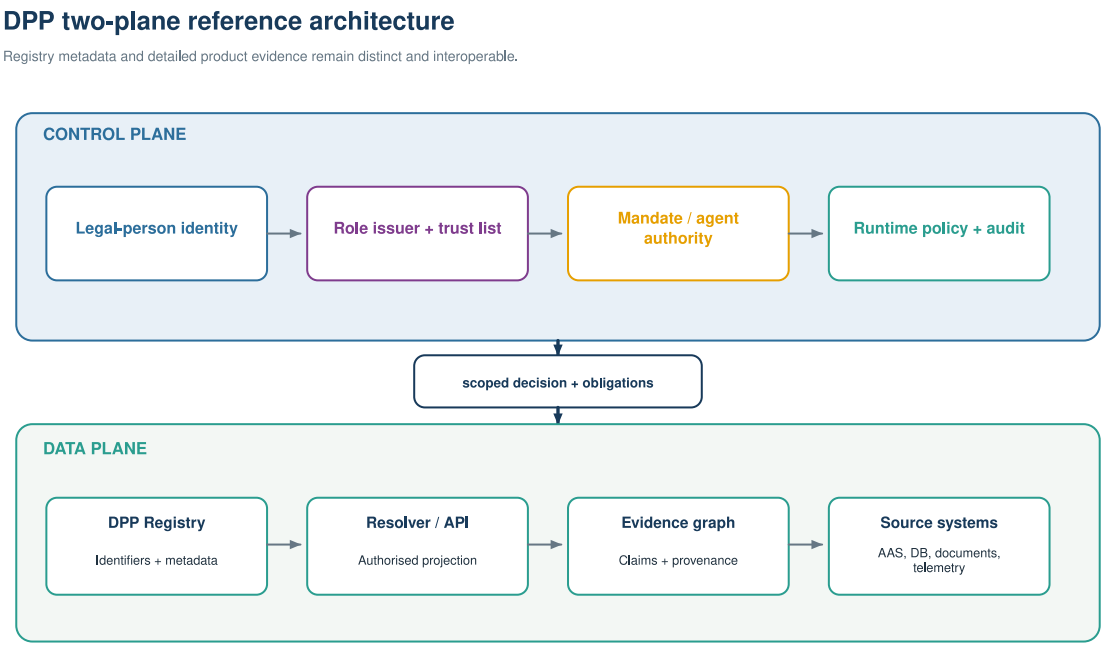

Figure 3: Two-plane DPP system reference architecture. *Spherity research based on ESPR, the DPP Registry User Guide, W3C specifications and Stöcker [1, 5, 10, 21].*

At runtime, the verifier follows a trust chain. It authenticates the presentation, resolves the legal-person identity, verifies issuer authority, checks credential integrity and status, validates mandate and role scope, evaluates requested purpose and data policy, and records the decision. The chain must fail safely. A syntactically valid credential from an unauthorised issuer is not sufficient. An expired or revoked role must not be accepted. A valid role outside its jurisdiction or product scope must not be silently generalised. If evidence is missing, the policy engine should request additional proof or deny the sensitive operation.

This logic fits a zero-trust posture [27]: no request is trusted merely because it originates inside a corporate network or recognised dataspace. Each transaction is evaluated using identity, device or workload context, policy and evidence. However, zero trust is a security architecture, not a substitute for sectoral law. It does not determine who is legally competent to issue a recycler role or how long a repair authorisation remains valid.

An EBW will improve the user and machine journey by holding legal-person credentials, qualified attestations, representation evidence and role credentials and by producing verifiable presentations. A wallet should not become the central policy authority. Issuers remain responsible for authoritative attributes; relying parties remain responsible for the decision; governance frameworks define trust lists, schemas, assurance levels and liability. The wallet is an orchestrator and controlled disclosure surface.

The runtime verification sequence is shown in Figure 4.

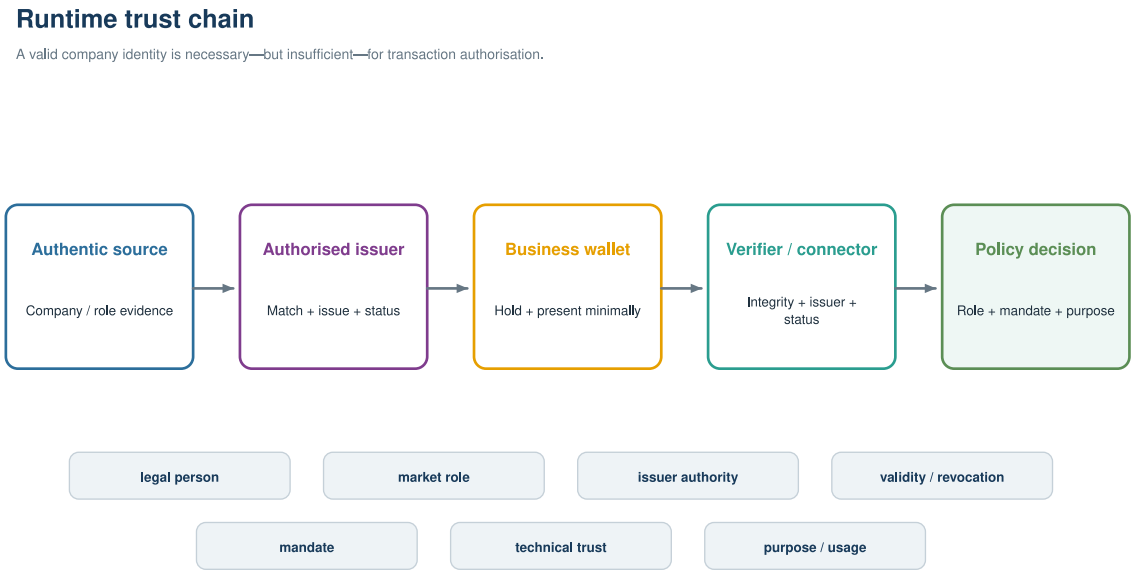

Figure 4: EBW-enabled runtime trust chain from authentic source to policy decision. *Spherity research based on Gößling et al. [9] and COM(2025) 838 [16].*

Table 3 states the Registry boundary and its required interfaces.

Table 3: DPP Registry boundaries

Registry does	Registry does not	Required interface
Verify and enrol organisations under its workflow	Replace every sectoral role authority	Legal-person and representation evidence
Register unique product identifiers and metadata	Store the complete detailed DPP by default	Resolver and decentralised host link
Support authority and customs verification	Determine factual conformity from a signature alone	Product rules and evidence validation
Provide technical resources for semantic definitions	Mandate one wallet, graph, connector or storage vendor	Open, testable interoperability profiles

Source: Author's synthesis; legal status and claim boundaries are documented in the source register.

5.1 A policy model for DPP transactions

A practical policy model should separate entitlement, context and obligation. Entitlement describes what a verified role can normally do: an MSA may inspect restricted compliance evidence, a workshop may read repair information, and a recycler may submit a treatment event. Context narrows that entitlement to a transaction: jurisdiction, product class, specific asset, case or work order, time, channel and assurance level. Obligations govern the result: minimise fields, watermark or encrypt an export, prohibit onward disclosure, retain a decision log, or require an additional signature. Separating these dimensions avoids large and opaque "role equals access" rules.

The model can combine role-based access control (RBAC), attribute-based access control

(ABAC), relationship-based access control (ReBAC) and purpose- or usage-based controls. RBAC gives administrators a comprehensible starting point. ABAC evaluates legal-person, credential, product and environmental attributes. ReBAC expresses relationships such as "operator of asset," "authorised service provider for product family," or "appointed representative of responsible economic operator." Purpose and usage policy address why evidence is requested and what may happen after disclosure. No one model covers the industrial case alone.

Policy inputs should be evidence-bearing. A claim such as 'role = recycler' is not merely a string in an account table. It should reference an issuer, legal basis or governance framework, subject legal person, facility and waste-stream scope, validity and status. Product context should resolve through the unique identifier and, where needed, Registry metadata. A mandate should identify the principal, delegate and action scope. The policy engine can then explain that access was granted because a particular authority credential and facility permit were valid for the identified battery and treatment purpose.

The policy decision point and policy enforcement point can be colocated or distributed. A DPP service may evaluate policy directly. In a dataspace, a connector may enforce the provider's policy after verifying wallet presentations. An enterprise gateway may call an external decision service. The security requirement is binding: the decision must be cryptographically and temporally associated with the request and response so that a token issued for one product, field or purpose cannot be replayed for another. Short-lived capabilities, audience restriction, proof of possession and transaction identifiers can reduce this risk.

Policy administration is a governance activity. Product rules define access categories; authorities and industry schemes translate them into implementable profiles; data providers classify fields; issuers define role semantics; and relying parties remain responsible for lawful processing. Version control is essential. If a rule changes, the audit record should show which policy version governed an earlier disclosure or update. A policy test suite should include positive, negative and boundary cases, including revoked credentials, expired mandates, conflicting roles, out-of-jurisdiction requests and degraded status services.

Privacy and confidentiality require different threat models. GDPR [28] applies where a DPP transaction processes personal data, for example when a repair or ownership event can be linked to an individual. Commercial confidentiality concerns supplier relationships, formulations, volumes and pricing. Security sensitivity concerns vulnerabilities, critical-infrastructure configuration or strategic dependencies. The policy layer should classify each field along these dimensions and apply distinct legal bases, retention and audit rules. A single "confidential" flag is inadequate.

Consent is not the default answer. Public authorities may act under law; an economic operator may need evidence to fulfil a legal obligation; a workshop may rely on a contract or statutory access right; and a data subject may not be the product owner. Wallet presentation can express user control, but it should not falsely imply that every disclosure is based on consent. The decision record should capture the applicable authority or lawful basis where relevant.

Machine actors make policy semantics more urgent. A software agent can authenticate with a workload key while acting for a company, but possession of a company credential should not authorise arbitrary actions. The agent mandate should contain permitted tools, assets, transaction limits, counterparties and escalation rules. High-impact actions, such as changing BESS protection settings or declaring a product destroyed may require step-up authentication, dual approval or independent evidence. The same mechanism can permit an agent to read public DPP fields broadly while tightly limiting control or update.

Finally, authorisation quality should be observable. Operators should monitor denied-request patterns, dormant privileges, revocation latency, policy exceptions, bulk-access behaviour and decisions made during degraded operation. Independent audits should sample both grants and

denials. A system that never denies may be over-permissive; one that denies legitimate workshops or recyclers may undermine repair and circularity. Governance must treat authorisation as a continuously tested public-interest capability.

6 Market-role governance and product-linked identity

Market-role governance begins with institutional mapping. For every role, the ecosystem must identify the authority or trusted body entitled to recognise it, the legal or contractual basis, the population and scope, evidence needed for issuance, validity and renewal rules, revocation triggers, appeal procedures, liability and relying-party obligations. Credential technology is downstream of this analysis. If two Member States recognise repair workshops under different regimes, a common credential schema can express the difference but cannot erase it.

The responsible economic operator is the key DPP role. Depending on product rules, this may be a manufacturer, importer, authorised representative or another operator placing the product on the Union market. Registry enrolment can establish an organisation and representative, while the product-specific registration binds the operator to an identifier. Controls should prevent a company from registering another operator's product identity or reusing a DPP improperly. An authoritative product-responsibility assertion, backed by Registry evidence and transaction audit, can become a PLI input.

Market surveillance authorities require broad statutory access but still operate under purpose and jurisdiction constraints. Their access should be attributable to an authority and official function, not to a generic shared account. The control plane can accept an authority credential, an officer or system mandate, a case or inspection purpose and the requested data class. For particularly sensitive evidence, policy may require a case reference, data-use obligations and enhanced logging. This is compatible with effective enforcement because automated verification can be faster than manual document exchange.

Customs presents a different integration. Customs must rapidly verify identifiers and DPP registration for goods entering the market. ESPR provides for interconnection between the DPP Registry and the EU Customs Single Window Certificates Exchange System. The control plane can distinguish routine automated identifier checks from deeper evidence access. A customs system credential and transaction context can authorise the minimum data needed for clearance while escalating inconsistencies to an officer or market-surveillance authority.

Workshops and repairers are heterogeneous. Some product sectors have manufacturer-authorised networks; others rely on independent repairers, professional qualifications or no harmonised register. The system should avoid treating "workshop" as one universal role. A PLI may derive from manufacturer authorisation, a national professional register, certification or a contract. Relying policy can accept multiple issuer types with different assurance and scopes. Right-to-repair policy also cautions against using manufacturer-issued roles to exclude legitimate independent repair.

Recycler governance is likewise sector specific. A recycler may need an environmental permit, waste-treatment authorisation and capabilities for a particular chemistry, facility and jurisdiction. A role credential should not merely say "recycler." It should bind the legal person to the authorised facility and permitted operations, enable status checking, and permit an end-of-life event only for products or waste streams within scope. Because CIRPASS-2 identifies false destruction reports and fake recyclers, the control plane should combine role verification with receipt, weighing, treatment and downstream evidence.

MSA, customs, workshop and recycler roles should be represented through a governance registry

or trust framework that distinguishes authoritative and non-authoritative issuers. The governance object is more than a list of public keys. It documents issuer competence, credential profile, assurance level, status service, audit requirements and liability. Trust lists can be federated by sector and jurisdiction and referenced by policy. This supports mutual recognition without pretending that every role is harmonised.

Figure 5 separates governance authority from credential operation and runtime use.

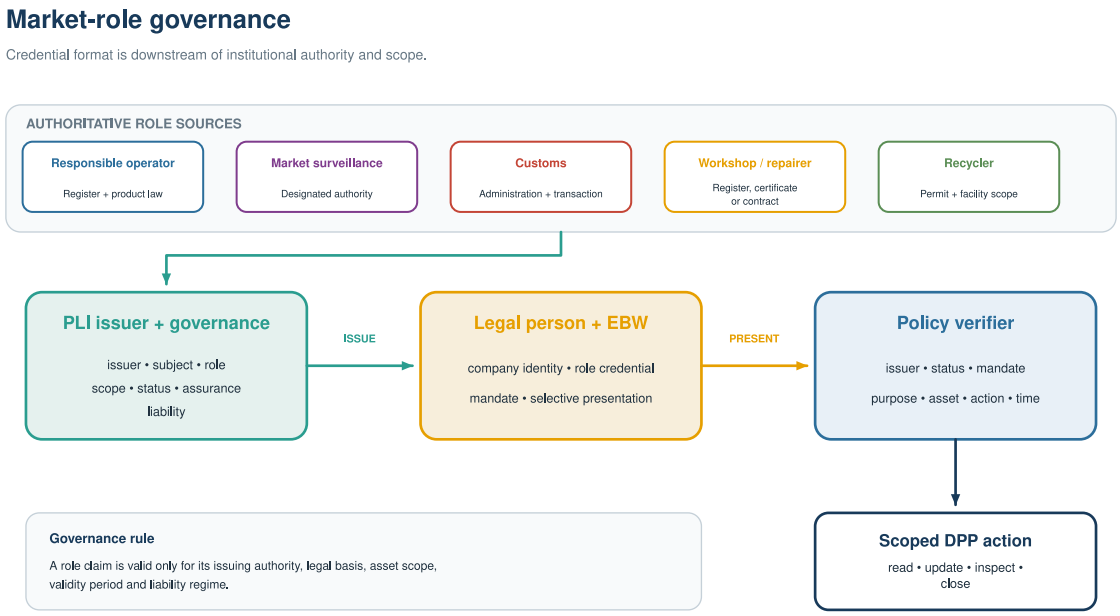

Figure 5: Market-role governance for product-linked identity credentials. *Spherity research.*

Table 4 maps representative market roles to issuers, scope and high-risk actions.

Table 4: Product-linked identity governance by market role

Role	Potential authoritative source	Scope that must be expressed	High-risk action
Responsible economic operator	Company register plus Registry/product-law evidence	Product group, identifiers, jurisdiction, responsibility basis	Create/register DPP
Market surveillance authority	Designated public authority	Office, jurisdiction, statutory function, case purpose	Read restricted compliance evidence
Customs	Customs administration and transaction system	Office/system, customs role, declaration or consignment	Verify identifier or hold goods
Workshop or repairer	Manufacturer, professional register, certification or contract	Product family, competence, territory, independent/authorised status	Read diagnostics or submit repair
Recycler	Environmental permitting authority	Facility, waste stream, chemistry, operations, jurisdiction	Declare treatment/end-of-life

Source: Spherity research; legal status and claim boundaries are documented in the source register.

The legal-person identity flow can now be stated precisely. First, an authoritative company source establishes the legal person and identifiers. Second, a role authority verifies sector-specific eligibility and issues a role credential. Third, a principal issues or activates a mandate for a

human, service or agent. Fourth, the presenter uses a wallet or equivalent key-management mechanism to create a selective presentation. Fifth, the verifier checks legal identity, issuer authority, credential status, mandate, role scope and transaction context. Sixth, a policy engine permits the minimum operation and records the decision. The process is reusable, but not identity-only.

7 The energy data-X reference use case

The energy data-X implementation offers a useful analogue because energy data exchange is already role intensive. Market participants operate under defined responsibilities, identifiers and contractual relationships. Data can be commercially sensitive and operationally consequential. The published use case combines an EBW-based identity and credential flow with a connector and runtime policy enforcement [9]. Its trust chain moves from an authentic source through data matching and an authorised issuer to an EBW, then through presentation and a connector to verification and an allow-or-deny decision.

The control plane jointly checks company identity, an EUID or equivalent company reference, energy-specific identifiers such as a market partner identifier, the asserted market role, issuer trust, credential validity and revocation, technical trust level and data-use policy. This composition matters. A company may be validly registered yet not hold the market role needed for a data transaction. A valid role credential may be presented by a workload that fails the technical assurance policy. A technically trusted connector may request data for a purpose not permitted by the provider.

The "imbalance settlement quality" scenario demonstrates multi-party exchange. A metering point operator supplies data to a supplier or balance responsible party; a forecasting service processes information; results return to the supplier or balance responsible party; and a flexibility provider may contribute operational options. Each participant sees and contributes only what its role and purpose require. The project reported test data and fine-grained authorisations. It should not be overstated as a completed deployment of every AI or production case, but it validates the feasibility of attribute- and role-based exchange.

For DPPs, the transferable pattern is a runtime join across four domains: enterprise identity, sector role, data policy and technical trust. A repair workshop requesting diagnostic history is analogous to an energy service provider requesting metering data. A recycler submitting destruction evidence is analogous to a market participant contributing settlement evidence. A market-surveillance authority requesting a confidential technical file is analogous to a regulated actor invoking statutory access. The schemas and issuers differ, but the control-plane sequence is stable.

There are also limits to the analogy. Energy markets often have mature role codification and participant registries. Product ecosystems contain a wider and less harmonised set of roles. The product itself changes hands and state over long lifecycles. Some DPP access must remain anonymous and public. Product carriers can be damaged or substituted. Therefore, energy data-X is a reference pattern, not a drop-in governance solution.

The principal design lesson is to keep authorisation close to the transaction. Pre-enrolment in a dataspace or possession of an EBW should not grant blanket access. The policy decision should include the specific DPP identifier, requested field or evidence package, action, purpose, jurisdiction, time and onward-use condition. A decision can return obligations, such as "disclose the safety certificate but not supplier identities," "allow viewing for 24 hours," or "permit an end-of-life update only after independent receipt evidence."

Table 5 gives an illustrative role- and evidence-specific access matrix.

Table 5: Illustrative access-control matrix

Evidence/action	**Public**	**Economic operator**	**Workshop**	**MSA/customs**	**Recycler**
Public identity and instructions	Read	Read/update	Read	Read	Read
Restricted composition detail	No	Read/update	Purpose-limited	Statutory read	Treatment-purpose read
Diagnostic/service history	Summary	Read	Work-order scope	Case scope	Safety-relevant subset
Register DPP	No	Scoped mandate	No	Verify only	No
Submit repair event	No	Approve/policy	Scoped role and mandate	Inspect	No
Submit end-of-life event	No	Receive status	No	Inspect	Facility and product scope

Source: Spherity research; legal status and claim boundaries are documented in the source register.

8 Data plane: from product records to verifiable evidence graphs

The data plane contains the information that describes a product or supports a decision: identifiers, material composition, certificates, declarations, test results, observations, repair events, ownership or custody events where lawful, software and configuration versions, safety incidents, performance indicators, treatment outcomes and derived claims. Its architecture should preserve evidence quality without forcing every participant into one database.

A conventional relational database and API remain appropriate for authoritative operational records. Signed JSON can provide portable integrity. Verifiable Credentials can express issuer-bound claims with status and selective presentation patterns. AAS can expose structured industrial asset information and submodels. Dataspace connectors can negotiate and enforce usage conditions. RDF or property graphs can integrate relationships across sources. These are complementary patterns, not mutually exclusive ideologies. The choice should follow the evidence transaction.

A verifiable evidence graph links claims to subjects, issuers, source artefacts, observations, methods, transformations, validation results, versions, policies and decisions. "Verifiable" does not mean that every node is cryptographically true. It means that integrity, issuer binding, status, provenance and validation context can be evaluated and that unsupported or contradictory claims are visible. JSON-LD and RDF support semantic links; OWL can express ontological relationships; SHACL supports closed-world validation of a submission against expected shapes; W3C Verifiable Credentials bind portable assertions to issuers and subjects; PROV-O records derivation, attribution and activity.

The distinction between open-world integration and closed-world validation is central. Supply-chain evidence is incomplete by nature: a graph should permit new suppliers, certificates and events to be added without redesigning one universal schema. A specific regulatory or operational decision, however, has a closed checklist. A battery conformity decision may require defined declarations, test evidence, issuer classes and freshness. SHACL or an equivalent rules layer can validate the relevant subgraph and produce a result. The graph preserves both the evolving evidence universe and the bounded decision snapshot.

Evidence paths are more useful than isolated documents. A recycled-content claim can link to incoming material batches, recycler credentials, mass-balance calculations, laboratory results, production lots, the responsible economic operator's declaration and the policy version used for validation. If one credential is revoked or one calculation changes, affected decisions can be identified. The graph can store a decision evidence package or cryptographic digest so a later auditor can reconstruct what was relied upon at the time.

Raw telemetry should generally remain in specialised time-series, historian or object stores. BESS systems may generate high-frequency cell, module, inverter and environment data. Copying every sample into a semantic graph is expensive and rarely useful. The graph should instead reference governed observation windows, quality metrics, extracted features, incident markers, model inputs and immutable hashes of source segments. This division keeps operational systems efficient while making decision-relevant evidence discoverable and auditable.

The data plane also needs confidentiality engineering. Public DPP fields can be served without identity. Restricted fields require field- or claim-level policy, encryption and auditable disclosure. Derived proofs can sometimes replace raw data: an authority or financier may need evidence that a threshold is met, not the full supplier formula. However, selective disclosure must not conceal the provenance needed for accountability. The system should record what was proven, by whom, under which method and against which policy.

AI use makes provenance more consequential. An industrial model may combine DPP data,

supplier attestations, sensor features and maintenance records. “Know Your Data” requires the organisation to identify source, licence, confidentiality, collection method, quality, transformations and permitted use. Data Risk Scoring can evaluate authenticity, completeness, freshness, sensitivity, jurisdiction, revocation exposure and model impact. A graph can connect an AI output to the evidence and model version used, supporting incident analysis and human oversight.

The evidence graph therefore serves as a policy-aware index of trust, not as a replacement for all enterprise systems. It makes relationships and validation explicit, supports reuse of verified claims, and allows control-plane decisions to request the smallest evidence subgraph required. Its success depends on shared vocabularies, identifier resolution, issuer governance, versioning and evidence-quality metrics.

8.1 Architectural alternatives and interoperability choices

The proposed evidence-graph pattern should be evaluated against simpler architectures. A central relational database offers strong transaction consistency, mature access control and efficient reporting within one authority domain. It can be entirely appropriate for a Registry or responsible operator. Its weakness is cross-organisational integration: evidence from many issuers is often copied, provenance is flattened, and schema change requires coordination. Federation can mitigate these issues, but cross-source relationships still need explicit modelling.

A document repository with signed PDFs or JSON packages preserves familiar evidence units and can be inexpensive to deploy. Qualified seals can provide strong organisation attribution. The model becomes difficult when a decision relies on selected claims from many evolving documents, when one certificate is revoked, or when a product transformation creates lineage. Search and validation often revert to manual work. Signed documents are therefore valuable evidence nodes, but an index of their meaning and relationships is still needed.

W3C Verifiable Credentials, e.g. JSON-LD or CBOR-LD, provide portable, issuer-bound claims and status mechanisms. They support selective presentation patterns and wallet exchange. Their limitations are equally important: a credential schema does not establish issuer authority; cryptographic verification does not prove the claim; and the W3C model is not a full authorisation framework. Credentials work best when a governance framework defines issuer competence and a data plane links claims to source and decision context.

AAS provides a mature industrial representation for assets, submodels, properties and services. It is especially useful at the manufacturing and operational edge, where an asset already has an AAS and where domain submodels capture technical information. Making AAS the exclusive DPP or AI evidence architecture, however, risks stretching it beyond its strongest role. External attestations, legal-person credentials, cross-company provenance and policy decisions can be referenced from or adapted into AAS without forcing every source into one AAS shell concept.

A dataspace connector provides sovereign exchange, catalogue discovery, policy negotiation and enforcement between organisations. It can be a valuable policy enforcement point. DPP law does not generally require one connector technology, and public consumer access should not depend on dataspace membership. A portable control-plane profile should therefore support connector and non-connector access. Conformance should be measured at the evidence and policy interface.

The most robust design is compositional. Operational records remain in systems of record. Documents and credentials retain their native proof. AAS adapters expose industrial asset structures. The evidence graph records identities, semantic relationships, provenance and validation. The control plane evaluates portable role and mandate evidence. APIs and connectors deliver authorised projections. The Registry provides legally defined indexing and enforcement

integration. Each layer can evolve behind testable interfaces.

Interoperability must include semantics, security and governance for "open systems of authorized actors." Syntactic interoperability determines whether systems can exchange an identifier, credential or graph. Semantic interoperability determines whether they mean the same thing by "responsible economic operator," "state of health" or "recycled." Security interoperability determines algorithms, key assurance, status and presentation binding. Governance interoperability determines whose issuer and evidence are accepted, under which liability. Projects often solve the first and assume the other three.

Identifiers are the joins. A product may have a model, batch and item identifier; a battery may be transformed into a second-life asset; a legal person may have EUID, national registration, VAT and LEI identifiers; a facility and metering point have separate identifiers. The graph should not collapse them into one string. It should maintain typed equivalence and derivation relationships with authority and date. GS1 Digital Link [29] can resolve product identifiers to web resources; Registry entries provide DPP registration context; sector identifiers connect energy or waste processes.

To ensure interoperability, semantic profiles must be modular and grounded in open-world vocabularies and formats like RDF and JSON-LD. A common core can define product, legal person, evidence, issuer, credential, event, policy, decision and provenance. Product-group profiles add required fields and roles. Use-case profiles define a decision package. SHACL shapes or equivalent validation artefacts should be versioned and published with examples. Mappings to AAS, JSON APIs and credential schemas can be tested against the same competency questions.

Long-term verification needs special attention. Product passports and safety evidence may remain relevant for decades. Certificate chains expire, algorithms weaken, issuers cease operation and URLs change. Preservation should include evidence timestamps, trust-list snapshots or validation reports, algorithm metadata, migration procedures, persistent identifiers and content hashes. NIST's post-quantum standards [30] make cryptographic agility a present design requirement for evidence that must remain trustworthy into a post-quantum horizon, even though immediate migration priorities vary.

The choice among architectures should therefore be empirical. Reference tests can compare onboarding time, evidence-reuse rate, update propagation, revocation handling, query latency, confidentiality leakage, recovery, portability and audit reconstruction. The winning design may be hybrid. What matters is whether a relying party can make a lawful, explainable and reproducible decision across organisational boundaries.

9 CIRPASS-2 risks: a lifecycle control model

The CIRPASS-2 catalogue demonstrates that DPP risk is distributed across actors and phases. Creation risks concern the quantity and correctness of information, DPP reuse, false operators, denial of service and intercepted submissions. Storage risks concern deletion, service failure, alteration, carrier substitution, unauthorised access and leakage. Retrieval risks include carrier degradation, redirect-service failure, denial of service, interception, traffic analysis and strategic aggregation. Update risks involve inaccurate changes, compromised updaters and failures to reflect physical modifications. Deletion risks concern false or missing end-of-life reports.

No plane owns a phase exclusively. Creation combines control-plane proof of the responsible operator and data-plane validation of required fields. Storage combines resilient hosting, integrity and access policy. Retrieval combines resolver availability, secure transport, privacy protection and purpose-based access. Update combines mandate, role and product state. Deletion combines

recycler authority and corroborating treatment evidence. This cross-cutting structure argues against equating security with a signed payload.

Figure 6 summarises the lifecycle distribution of the 52 risks.

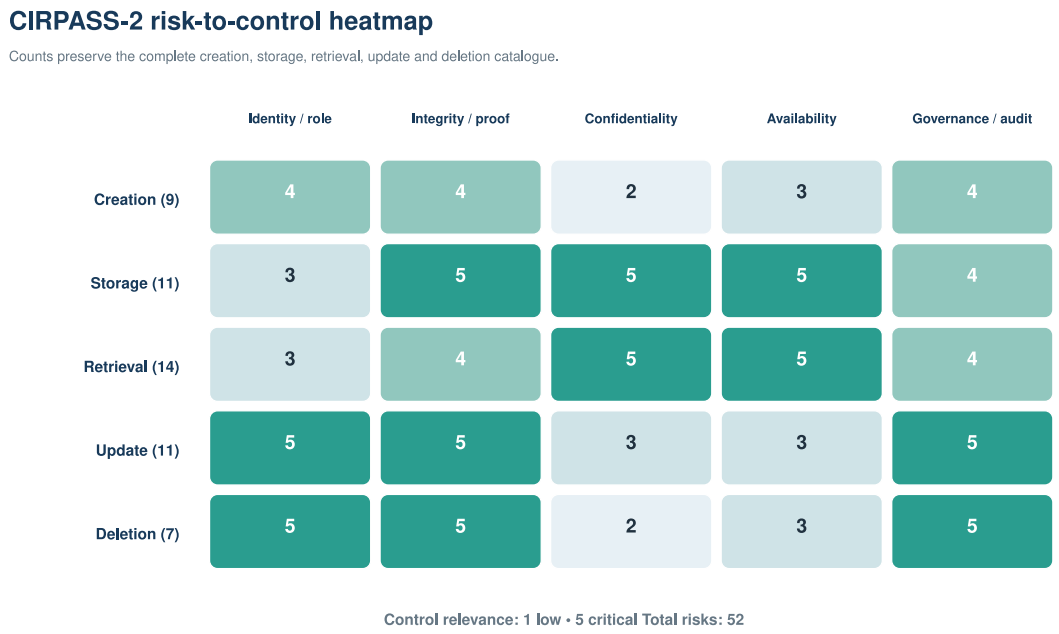

Figure 6: CIRPASS-2 lifecycle risks and primary control families. *Author's mapping of Roefs et al. [3].*

Creation controls should include verified enrolment, uniqueness and product-binding checks, rate limits, schema validation, completeness rules, issuer-authority checks and confidential transport. A signature binds a submitted object to a key or legal person, but does not prove that claims are factually correct. Incorrect information requires source evidence, plausibility checks, independent assessment where required, and liability. DPP cloning or reuse requires identifier uniqueness, Registry cross-checks and physical-to-digital binding.

Storage controls include replicated hosting, service-continuity and exit arrangements, integrity proofs, immutable versions, credential-status checking, encryption and independent backups. Provider insolvency is a governance risk as much as a technical risk. Persistence obligations should include data export, escrow or transfer mechanisms and tested recovery. Carrier substitution requires inspection and, for high-risk uses, stronger product binding than a printed label.

Retrieval creates confidentiality and intelligence risks that public-by-default designs often overlook. Even when an individual field seems harmless, large-scale aggregation may reveal supply-chain dependencies, strategic capabilities or sensitive equipment properties. Field classification, query-rate controls, purpose limitation, pseudonymous access where appropriate, monitoring and aggregation-resistant interfaces are therefore necessary. Security should not obstruct public rights; it should differentiate open access from high-risk bulk or restricted access.

Update controls require scoped mandates and event accountability. The updater should identify what changed, why, based on which observation, and how the event relates to the product. Policies should prevent history flooding while preserving material changes. Physical modifications that are not reflected digitally create a "twin drift" problem. Workshops, owners and third parties may have different duties and incentives. Detection can use maintenance records, inspections, device attestations and anomaly signals, but contractual and legal responsibility remains necessary.

End-of-life controls expose the weakness of self-asserted status. A recycler credential proves eligibility, not that a particular battery was treated. A robust destruction or recycling event should combine facility and role validity, custody or receipt evidence, timestamp, mass or serial reconciliation, treatment output, and where proportionate independent audit or authority reporting. The passport should not be simply erased: the product may be marked ended while an auditable minimum record is retained in accordance with law.

Appendix A maps all 52 risks to controls and residual risk. The highest priorities are false actors and product binding, confidential-data leakage and aggregation, unauthorised or inaccurate lifecycle updates, service continuity, and false end-of-life reporting. These priorities are contextual; a public low-risk product and a grid-connected BESS warrant different profiles. The general principle is assurance proportional to decision impact.

10 Traction-battery DBP use case

The traction-battery passport has a clear regulated product boundary: the individual EV battery placed on the market. Its lifecycle spans material sourcing, cell and module production, pack assembly, vehicle integration, use, maintenance, incident, removal, assessment, second-life preparation and recycling. Evidence originates from many parties, but the responsible economic operator for the finished battery remains accountable for the passport.

At creation, the control plane verifies the responsible operator and registration authority. Supplier evidence may arrive as signed declarations or credentials linked to batches, cells or modules. The data plane assembles the required passport fields and evidence links without necessarily exposing every upstream trade secret. Completeness and identifier uniqueness are checked before registration. The product identifier, carrier and Registry record establish resolution, while the responsible operator signs or seals the authoritative release.

During vehicle use, access views diverge. A consumer may see model, capacity, sustainability and safety information. An independent workshop may need diagnostic and repair information permitted by sectoral rules. A manufacturer-authorised workshop may receive additional procedures under a product-family role. A market-surveillance authority may request technical evidence. A potential second-life operator may need state-of-health, event and configuration information. The control plane evaluates role and purpose; the data plane provides an evidence package appropriate to the request.

Updates must distinguish observation from assertion. A battery-management system may generate measurements. An analytics service derives state-of-health. A workshop records a repair. The responsible operator or another authorised actor validates a passport update. The evidence graph links the resulting claim to the device, method, model version, calibration and actor. This makes a state-of-health number contestable and reproducible rather than a context-free field.

Transfer to second life changes the operational context, not necessarily the identity of the battery. A pack may be disassembled and modules recombined. The data model needs lineage: predecessor product identities, transformation event, responsible actor, test evidence and successor asset identities. Rules must specify when an original passport is updated, closed or linked to new passports. Graph relationships are well suited to this many-to-many transformation, while Registry entries preserve discoverable identity.

At recycling, the recycler's legal identity and permitted facility scope are checked. The treatment event is supported by receipt and reconciliation evidence. Restricted composition details can be released because the recycler's role and purpose satisfy policy. After treatment, an enduring

minimum audit record may remain even if operational access ends. This protects against the CIRPASS-2 risks of false destruction and unreported landfill.

Table 6 applies the two-plane model across the traction-battery lifecycle.

Table 6: Traction-battery passport lifecycle

Lifecycle stage	Control-plane decision	Data-plane evidence	Primary risk
Market placement	Responsible operator and registration mandate	Identifier, conformity, material and performance evidence	False operator or incomplete DPP
Vehicle integration/use	Owner/operator and service purpose	Configuration, incidents, state-of-health evidence	Over-disclosure or stale state
Repair	Workshop role and work order	Diagnostics, parts, method, signed repair event	Unauthorised or inaccurate update
Second life	Assessor/repurposer authority	Test, lineage, transformation and successor identities	Twin drift or broken lineage
Recycling	Permitted facility and treatment scope	Receipt, reconciliation, treatment and outputs	False destruction declaration

Source: Spherity research; legal status and claim boundaries are documented in the source register.

The traction-battery use case shows why access rights must be determined before data release rather than embedded as a static list in one passport. Roles, mandates and product state change. A workshop's authorisation may expire; a recycler permit may be suspended; an authority's purpose may be time-bounded. Runtime policy can adapt while preserving a stable product identity and evidence history.

11 BESS reference use case: system boundary and two-plane architecture

A battery energy storage system is a composite cyber-physical installation. It includes one or more battery products, racks or containers, thermal management, fire detection and suppression, inverters or power-conversion systems, a battery-management system, an energy-management system, supervisory control, communications, site and grid-connection configuration, warranties, service contracts and operational market roles. The regulated battery passport covers qualifying batteries, but not automatically this full system boundary.

The proposed BESS passport is therefore a system-level evidence dossier linked to component passports. It may be established voluntarily by an owner, operator, financier, insurer, system integrator or sector scheme. Its governance must identify a system passport owner, authoritative update actors and assurance level. It should not overwrite component passports. Instead, it references them and adds configuration, commissioning, operational, safety and service evidence that exists only at system level.

The control plane includes legal-person identities for owner, operator, asset manager, integrator, service workshop, battery and inverter manufacturer, distribution or transmission system operator, aggregator, flexibility service provider, insurer, authority and recycler. It includes asset-linked roles: who may dispatch the system, approve a firmware update, access safety logs, alter protection settings, attest availability, investigate an incident or submit a decommissioning event. Energy market-role credentials can be reused where applicable, following the energy data-X pattern.

Figure 7 applies the control-plane model to a BESS transaction.

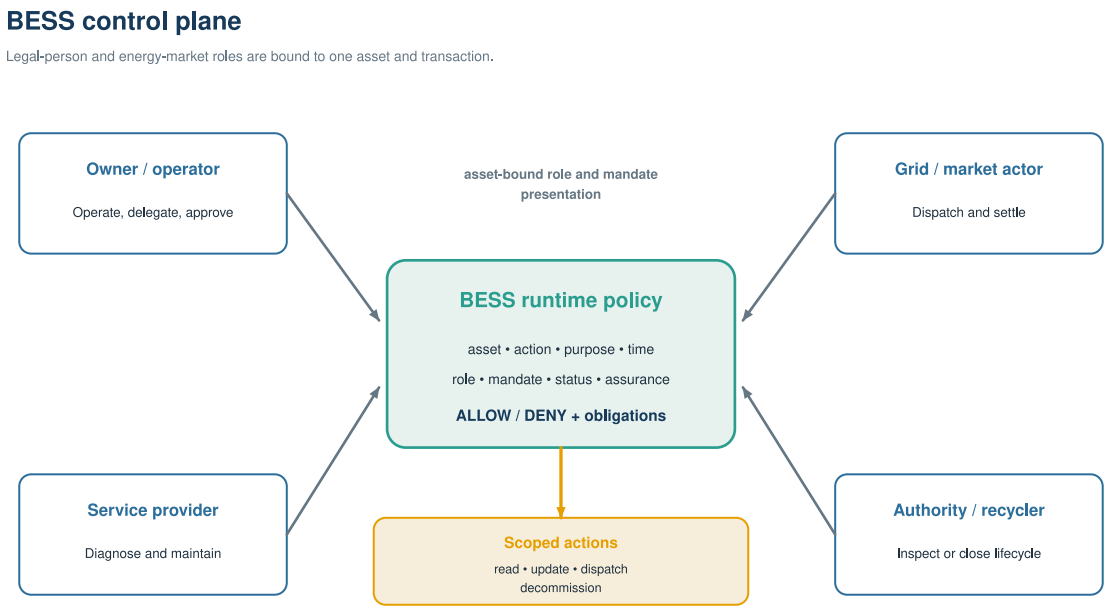

Figure 7: BESS control plane: legal persons, asset-linked roles, mandates and runtime policy. *Spherity research based on Gößling et al. [9].*

A runtime maintenance transaction illustrates the flow. The operator issues a work order and mandate to a service provider. The provider presents legal-person identity, technician or workload authority, product-family competence and work-order scope. The policy engine checks credential status, site and asset binding, maintenance window, requested diagnostic fields and cybersecurity posture. It grants time-limited access to selected telemetry features and technical documents. The resulting service event is signed, linked to replaced components and incorporated into the evidence graph.

The data plane links component DBPs, serialised configuration, grid-connection agreements, commissioning tests, environmental and safety permits, protection settings, software bills of materials where applicable, firmware versions, vulnerability and patch status, warranties, operational envelopes, state-of-health features, maintenance and incident evidence, market-service commitments and end-of-life plans. High-frequency telemetry remains in a historian; the graph references decision-relevant windows and hashes.

Figure 8 shows the corresponding evidence-graph data plane.

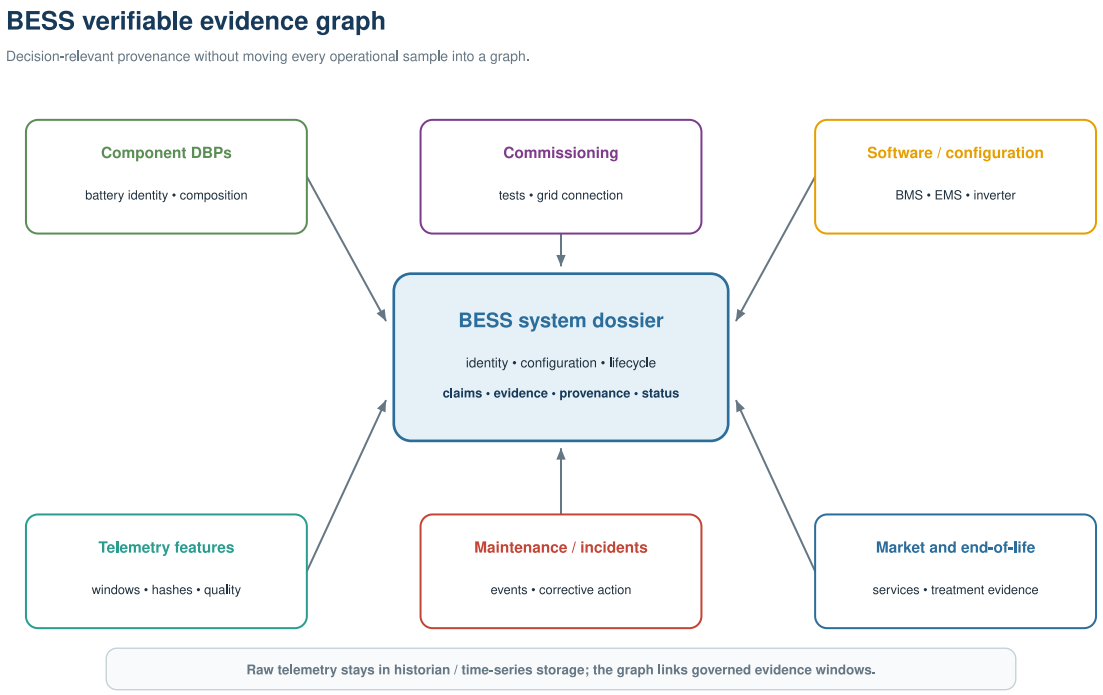

Figure 8: BESS data plane as a verifiable evidence graph linked to operational stores. *Spherity research based on Stöcker [10].*

Three decision packages demonstrate value. For financing or insurance, the system can present verified ownership or control, component provenance, commissioning, maintenance compliance, degradation trend and unresolved incidents. For grid or flexibility participation, it can present market role, connection eligibility, dispatch capability, metering quality and current constraints. For safety oversight, it can present configuration, alarm history, relevant thermal events, corrective actions and authority reports. Each package is a governed projection, not a copy of the full system record.

Cybersecurity duties must remain conceptually separate. The CRA governs products with digital elements and NIS2 governs cybersecurity risk-management obligations for covered entities. A BESS evidence dossier may carry conformity, vulnerability and operator-control evidence, but a valid product certificate does not prove that an operator complies with NIS2, and an NIS2 programme does not establish product conformity. Control-plane policies should request evidence appropriate to the decision.

Table 7 defines the BESS system boundary and passport treatment.

Table 7: BESS system boundary

Layer	Typical elements	Passport treatment
Battery product	Cell/module/pack, BMS, regulated battery attributes	Mandatory DBP where Article 77 scope applies
Power conversion	Inverter, transformer, protection	Linked component evidence; separate product obligations may apply
System integration	Rack/container, thermal/fire systems, site configuration	Voluntary system-level dossier and configuration lineage
Operations	EMS/SCADA, historian, dispatch, maintenance	Operational evidence and governed telemetry features

Continued on next page

Table 7 continued

Layer	Typical elements	Passport treatment
Market/grid context	Connection, metering, aggregator and flexibility roles	Market-role credentials and decision-specific presentations

Source: Spherity research; legal status and claim boundaries are documented in the source register.

The BESS case also tests AI integration. A predictive-maintenance model consumes telemetry features, maintenance evidence and environmental context. An evidence graph records input windows, data-quality scores, model and software version, output, human review and resulting work order. An AI agent may negotiate flexibility or schedule maintenance under a bounded mandate. The control plane constrains what the agent may access and commit; the data plane records the evidence and consequences. This is a concrete bridge from trusted data to trusted industrial AI.

12 DPP Registry and EBW convergence

The DPP Registry and the proposed EBW solve different but complementary problems. The Registry indexes product-passport identifiers and registration metadata, supports verification and enforcement, and enables links to customs. The EBW proposal addresses legal-person identity, attributes, mandates, trusted presentations, signatures or seals and secure exchange. Convergence should therefore mean interoperable trust and user journeys, not institutional merger or centralisation of all product data.

The current Registry enrolment process is appropriate as an operational baseline. It relies on EU Login, organisation information, legal identifiers, a Commission-generated declaration and qualified signing or sealing. The process creates an accountable administrator and verified organisation. Its limitations are repeatability and freshness. The same legal person may need to repeat related checks across product groups, authorities, customs services and other regulatory portals. Representation changes may require document workflows. Machine-to-machine authorisation is not the primary design centre.

Figure 9 distinguishes the current enrolment path from the proposed target state.

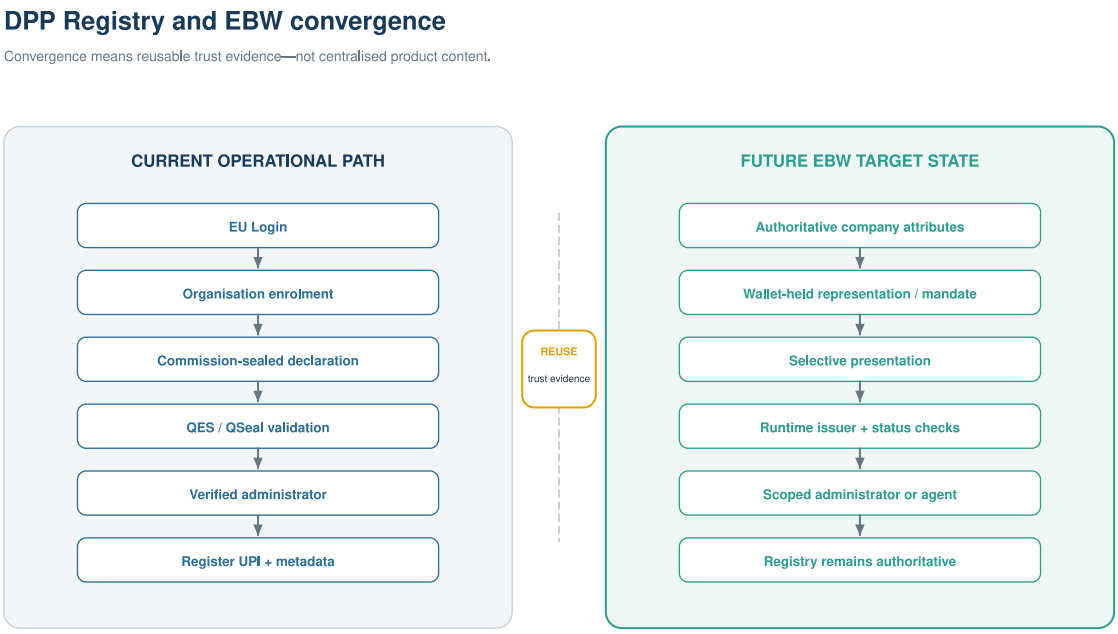

Figure 9: Current DPP Registry enrolment and a future EBW-enabled target state. *Spherity research based on the DPP Registry User Guide v1.01 [5] and COM(2025) 838 [16].*

A future EBW target state could supply reusable company and representation evidence. The Registry would request a presentation containing the minimum legal-person attributes, EUID or recognised identifier, representative mandate and assurance evidence. The wallet would obtain authoritative attributes from company and public registers or qualified issuers. The Registry would verify the presentation and bind the organisation to an account and DPP actions. Subsequent machine actions could use scoped organisational credentials and mandates rather than a human repeating a document upload.

The target state must preserve Registry authority. The Registry remains the authoritative system for DPP registration events and metadata in its legal scope. The EBW does not decide that a product is compliant, nor does it store the full DPP by default. It helps establish who is acting and what credentials or mandates the actor can present. Product-specific rules and Registry policy determine which evidence is accepted.

Convergence should include five interfaces. First, a legal-person resolution interface maps recognised identifiers and avoids duplicate organisations. Second, a representation interface expresses who may administer or register on behalf of the company. Third, a PLI interface binds the company to product responsibility, market role or facility scope. Fourth, a status interface supports expiry, suspension and revocation. Fifth, an audit interface records presentations and decisions in a privacy-preserving manner.

The transition should be staged. A compatibility phase keeps the signed-PDF path while accepting wallet presentations as an alternative. A reuse phase allows verified organisation attributes to be applied across product groups and relevant Commission services. A machine-action phase introduces scoped organisational credentials and delegated agents. A cross-border governance phase aligns assurance and liability across Member States and sectoral issuers. Each phase requires conformance tests and redress.

The legal-status distinction remains decisive. The EBW architecture described here is a target-

state proposal informed by COM(2025) 838 and the Council position, not a statement of enacted duties. The Parliament and Council may amend functions, governance, timelines and liability. System designers should therefore implement modular interfaces rather than hard-code one legislative outcome.

Table 8 compares the current Registry path with the future EBW-enabled target state.

Table 8: Current Registry path and future EBW target

Dimension	Current operational path	Future target-state proposal
Sign-in and organisation	EU Login plus organisation enrolment	EBW presentation of reusable legal-person attributes
Representation	Named representative and signed/sealed declaration	Machine-verifiable mandate or digital power of attorney
Validation	Document and certificate checks	Runtime issuer, status, scope and presentation checks
Product action	Verified administrator registers identifier	Scoped human or agent mandate registers/updates
Authority	Registry remains authoritative for registration	Registry remains authoritative; EBW supplies trust evidence

Source: Spherity research; legal status and claim boundaries are documented in the source register.

13 Simplification, competitiveness and the digital core of European industry

The macroeconomic case for convergence is evidence reuse. European companies repeatedly prove the same foundational facts, legal existence, registration, representation, permits, conformity, product identity, supplier evidence and reporting scope, to different authorities and business partners. Digitising each form separately does not remove duplication. A shared trust layer can allow one authoritative fact to be presented, verified and reused under purpose-specific policy.

Consider a battery placed on the market. The responsible operator may supply identifiers and conformity evidence to the DPP Registry, customs, a market-surveillance authority, a customer, a financier and a recycler. Today, the evidence may be re-keyed into portals, uploaded as PDFs and revalidated independently. In the proposed architecture, the company presents legal-person and mandate evidence from an EBW or equivalent mechanism; the Registry provides authoritative registration metadata; the DPP data plane provides product claims; and each relying party requests only the evidence package needed. The evidence is not "submitted once and open forever." It is reused with consent or legal authority, purpose, access control and an audit trail.

A second example is repair. A workshop verifies company identity and competence once with an authoritative issuer. For each job, it presents a product-linked role and work-order mandate. The DPP service releases permitted diagnostics and records a repair event. Warranty, safety, resale and later recycling processes can rely on the same event provenance. The workshop avoids multiple proprietary onboarding processes, while manufacturers and authorities retain policy control.

A third example is BESS operation. An owner, grid operator, aggregator, insurer and authority need overlapping but non-identical evidence. Shared identity and role credentials reduce repeated counterparty due diligence. Evidence graphs permit the same commissioning test, component passport or maintenance event to support several decisions without distributing the

complete operational record. Policy projections protect security-sensitive settings and commercial telemetry.

The evidence-reuse pattern is illustrated in Figure 10.

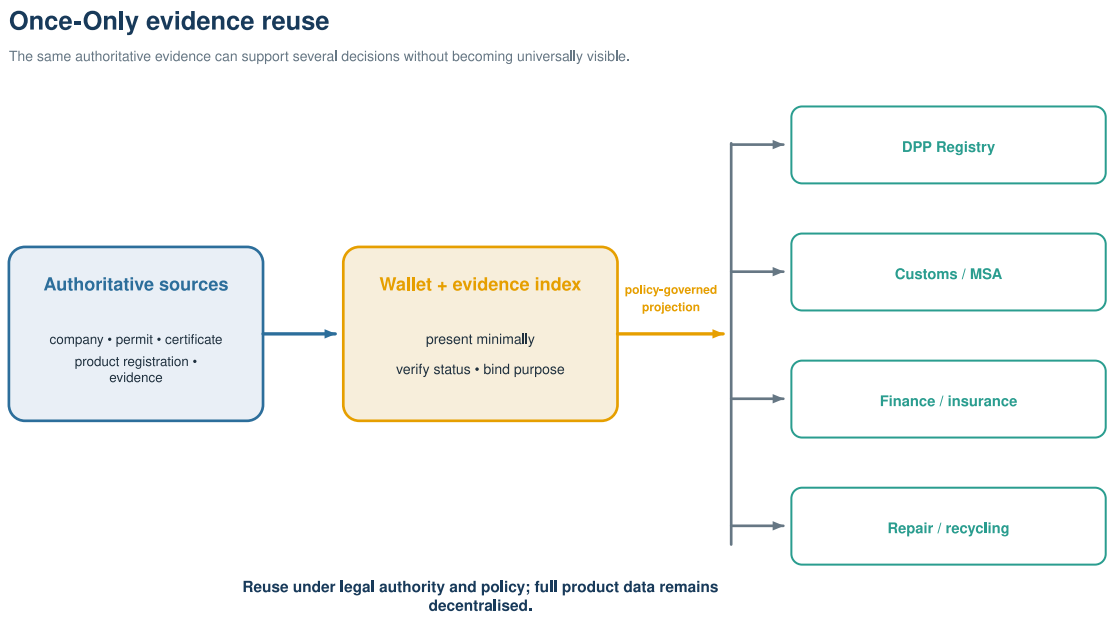

Figure 10: Once-Only evidence reuse across compliance and industrial decisions. *Spherity research based on Regulation (EU) 2018/1724 [31] and Implementing Regulation (EU) 2022/1463 [32].*

This architecture aligns with the Once-Only Principle [31, 32] but requires precision. Under the Single Digital Gateway and OOTS, cross-border evidence exchange is initiated at the user's request for covered procedures and remains governed by applicable law. DPP/EBW convergence should not be presented as unrestricted automatic data pooling. The design principle is "verify at source, reuse under authority, disclose minimally, record the decision." OOTS is a useful public-sector interoperability reference; DPP ecosystems extend the logic into business-to-business and product-linked evidence.

The Commission's simplification programme [33] targets administrative-burden reductions of 25% overall and 35% for SMEs. The EBW proposal's cost-benefit material presents large potential benefits and firm-level savings. Those figures are scenarios dependent on adoption, network effects, implementation cost and avoidance of duplicate systems. They should not be treated as realised savings. The economic hypothesis is nonetheless credible: standardised evidence and reusable identity reduce transaction costs where many parties verify the same facts.

Competitiveness gains arise [34] through faster market access, lower compliance integration cost, better access to finance, more reliable secondary materials, service innovation and reduced fraud. Single Market gains [35] arise when credentials and evidence can be verified across borders without abandoning national competence. Enforcement gains arise when authorities can query structured, current evidence and identify affected products. Industrial modernisation arises because the same evidence layer can support procurement, quality, maintenance, reporting and AI.

Risks accompany scale. A central identity or metadata layer can become a concentration target. Poorly designed access policy can create surveillance or strategic-intelligence exposure.

Proprietary trust frameworks can lock SMEs into intermediaries. Overly complex credentials can reproduce paperwork in machine-readable form. Governance must therefore require open standards, provider portability, proportional assurance, transparent fees, redress, data minimisation and independent conformance testing.

The "digital core" is consequently not one platform. It is a set of interoperable public and private capabilities: authoritative registers, identifiers, wallets and mandates, trust services, DPP Registry interfaces, decentralised evidence stores, semantic and credential standards, runtime policy, audit and secure AI consumption. Its value is measured by successful evidence reuse and decision quality, not by the number of credentials issued.

Table 9 identifies concrete evidence-reuse opportunities and their limits.

Table 9: Concrete evidence-reuse opportunities

Evidence	**Initial authoritative source**	**Reuse examples**	**Boundary**
Legal existence and identifiers	Company register/authoritative source	Registry, customs, MSA, contracting	Freshness and identifier matching still required
Representation or mandate	Company principal or authentic source	Registration, repair delegation, agent action	Must be object-, action- and time-scoped
Product registration	DPP Registry	Customs, marketplace, authority checks	Does not prove every product claim
Conformity/test evidence	Notified body, laboratory or responsible operator as applicable	Market access, finance, maintenance	Issuer competence and validity are decision-specific
Recycler permit and event	Permit authority plus facility evidence	Restricted access, treatment, circularity reporting	Eligibility does not prove a specific treatment event

Source: Spherity research; legal status and claim boundaries are documented in the source register.

13.1 Governance economics and the operating model

Shared infrastructure does not eliminate governance cost; it changes where the cost is paid. An issuer must verify organisations and roles, operate status services and handle disputes. Wallet and trust-service providers must secure keys, presentations and recovery. DPP hosts must preserve availability and data quality. Relying parties must maintain policies and evidence requirements. Authorities must supervise and update rules. The operating model should allocate fees and liability so that SMEs are not charged repeatedly for the same foundational verification.

A layered governance structure is appropriate. Union law and implementing acts define mandatory DPP outcomes. European and international standards define interoperable technical behaviour. Product-sector governance defines roles, evidence profiles and assurance. National authorities recognise permits and professional status where competence remains national. Ecosystem operators provide conformance testing, trust lists and incident coordination. Individual relying parties set transaction policy within legal bounds. This avoids both uncontrolled fragmentation and an unrealistic central authority for every industrial role.

Procurement can accelerate conformance. Public authorities and large buyers can require open interfaces, portable identifiers, evidence export, credential status, documented policy and independent test results. They should avoid specifying one vendor's wallet, connector or graph database. Procurement criteria can reward successful evidence reuse and revocation handling rather than decorative "blockchain" or "AI" labels.

SME adoption depends on assisted paths. A small manufacturer should not need to operate its own credential issuer, graph cluster and policy engine. Accredited or supervised service providers can offer managed DPP hosting, wallet custody options and evidence transformation. Portability is essential: the responsible operator must be able to move providers while preserving identifiers, evidence and audit. Transparent service boundaries also prevent outsourcing from obscuring legal responsibility.

Incident governance crosses the two planes. A compromised role issuer may require credential suspension; a corrupted DPP host may require evidence restoration; a resolver outage may require cached safe views; a leaked data set may require access investigation; a false recycler event may require product-status correction and enforcement. A coordinated incident protocol should identify notification duties, authoritative correction, status propagation, preservation of forensic evidence and communication to affected relying parties.

Success should be reported as an evidence-flow dashboard. Useful indicators include the percentage of DPP registrations using reused company evidence, average time to validate a cross-border role, number of authorities accepting a profile, share of restricted disclosures made by selective presentation, unresolved provenance gaps, policy-denial reasons, status-service latency, provider portability tests and confirmed administrative steps removed. These measures reveal whether convergence is simplifying work or merely adding a new credential layer.

The economic research design should compare counterfactuals. A pilot that measures only a wallet-enabled process may mistake digitisation benefits for wallet benefits. Studies should compare the existing process, a conventional portal/API improvement and a wallet-plus-evidence architecture. They should include integration, governance, training, exception handling and ongoing status costs. Benefits should be segmented by firm size, transaction frequency, cross-border activity and role complexity.

The macro thesis is consequently conditional. A reusable trust and evidence layer can modernise Europe's industrial core when it reaches sufficient adoption, offers credible liability and redress, and removes rather than duplicates legacy steps. Without these conditions, businesses may operate wallets, portals and PDFs in parallel. The implementation roadmap should include explicit retirement criteria for redundant reporting channels and legal recognition of machine-verifiable evidence.

14 Product continuum, AI Service Passports and Physical AI

Product policy increasingly spans a continuum rather than a binary distinction between physical goods and software. At one end is a passive physical product with a static information record. Next is a connected product whose state changes through software and operation. A hybrid product combines physical components with an embedded or associated AI agent. A virtual product may be a software service or autonomous agent without one persistent physical embodiment. The passport concept can organise evidence across this continuum, but the legal basis differs.

For a passive product, an AI-enabled DPP interface can make existing evidence easier to use. A board game could carry a DPP that identifies the edition, materials, safety information and rules. A conversational agent could explain rules, answer accessibility questions or guide setup. The agent should retrieve from a controlled rule corpus and cite the relevant version. The physical product remains the regulated object if product law applies; the agent is a service layer. The DPP should disclose that an AI interface is being used, the source corpus and limitations.

For a connected product, the DPP can link software version, cybersecurity support period, update

events and operating evidence. An AI assistant may diagnose or optimise the product. Access to operational data should depend on owner or operator authority, service role and purpose. The data plane records model inputs and recommendations; the control plane constrains actions. CRA conformity evidence and AI Act obligations may both be relevant, but they answer different legal questions.

For an AI-controlled physical system such as BESS, an agent may schedule dispatch, negotiate flexibility, optimise degradation or initiate maintenance. The agent requires a digital identity or workload credential and a power of attorney or machine-readable mandate from the legal person. The mandate should define assets, actions, financial or operational limits, counterparties, validity and escalation. Runtime policy prevents a general-purpose agent from converting read access into control authority.

An "AI Service Passport" is proposed here as a structured evidence object for an AI service or agent. It can identify provider, deployer or principal, model and service version, intended purpose, applicable AI Act role, risk classification where determined, evaluation evidence, data provenance summaries, cybersecurity and incident contacts, authorised tools, mandate, logging policy, material changes and status. It can link to conformity documentation without exposing protected model or training data. It is not asserted to be a DPP required by current ESPR or AI Act law.

Figure 11 positions the proposed passport patterns across the product–AI continuum.

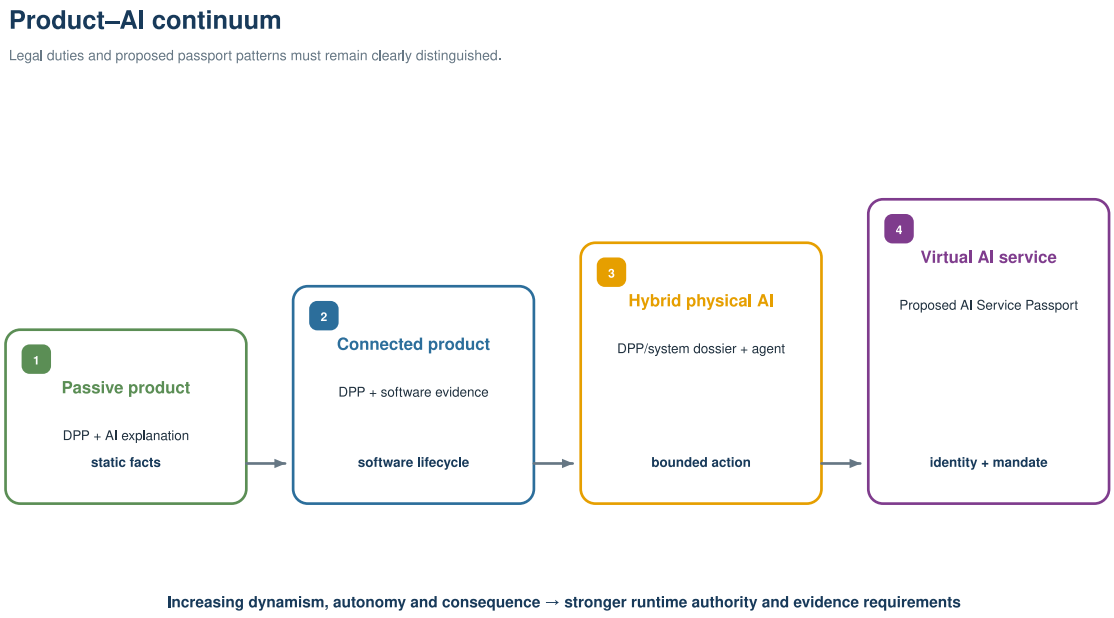

Figure 11: Product continuum from passive goods to connected systems, AI services and hybrid physical-agentic products. *Spherity research.*

Table 10 distinguishes the legal status and evidence focus of each passport pattern.

Table 10: Passport pattern across the product–AI continuum

Object	Passport or dossier	Control-plane focus	Data-plane focus	Legal status
Passive physical product	Product DPP where product law requires	Responsible operator and public/restricted view	Composition, instructions, conformity	Current/future product-specific duty
Connected product	DPP linked to software evidence	Owner, service and update authority	Version, support, incidents, operational evidence	DPP plus CRA/sector duties as applicable
Hybrid physical-agentic system	DPP/system dossier linked to AI Service Passport	Agent mandate, safety envelope, human oversight	Inputs, model version, actions and effects	Architectural proposal beyond existing duties
Virtual AI service or agent	AI Service Passport	Provider/deployer/principal, tools and mandate	Evaluation, provenance, logs, material changes	Architectural proposal; not an ESPR DPP

Source: Author's synthesis; legal status and claim boundaries are documented in the source register.

The value of the passport pattern is composability. A physical product DPP can link to an AI Service Passport for the agent that operates or explains it. The AI passport can link to product evidence needed for context. A transaction record can link the agent's mandate, input evidence, model version, output and human approval. When the model or product changes, versioned relationships preserve what applied at the time.

Trusted AI requires more than a model card. It requires trusted inputs, constrained authority and observable effects. A legally identified company may provide an AI service, but the service still needs technical identity and attested runtime properties. A valid AI passport does not prove every output correct. It makes responsibility, evidence, policy and change visible. An evidence graph can expose contradictions, expired sources and unsupported inferences before an action is executed.

Physical AI raises additional safety questions because software decisions alter the material world. Passport-linked policy can require two-person approval for high-impact actions, restrict control to certified operating envelopes, bind agents to a site and asset, and preserve an evidence snapshot. Emergency and offline modes require explicit design; dependence on remote identity or resolver services must not prevent safe operation.

This continuum turns the DPP into a general design pattern for accountable digital representations, but legal vocabulary should remain disciplined. Where product legislation mandates a DPP, the required object and responsible operator are determined by that law. Where the article proposes a system or AI passport, adoption may be contractual, voluntary, sectoral or future legislative. Convergence is an architectural possibility, not automatic legal equivalence.

15 Design principles, implementation roadmap and research agenda

The first design principle is plane separation with transaction-level binding. Identity and authorisation services should not be embedded inseparably in each product database, and data stores should not make role decisions based on unverifiable labels. The control plane returns a policy decision bound to requester, product, operation, evidence class, purpose and time. The data plane returns the authorised evidence projection and records the disclosure or update.

The second principle is authoritative issuance before credential portability. A role credential is valuable only when an accepted authority has verified the role and maintains status. Governance profiles should document issuers, legal basis, schema, assurance, scope, renewal, revocation, liability and audit. EU-wide interoperability can support several issuer types while relying parties express acceptable assurance.

The third principle is evidence over assertion. High-impact claims should link to source observations, methods, issuer competence, validity and transformation. Cryptographic proofs protect integrity and attribution; validation rules test structure and decision requirements; governance and audit address factual truth and misconduct. Systems should display missing, conflicting or expired evidence instead of collapsing uncertainty into a green badge.

The fourth principle is proportional disclosure. Public information should remain easy to access. Confidential, personal, security-sensitive or strategically aggregable evidence should be field classified. Policies should grant the least data and action needed, support selective presentation, limit bulk access and log sensitive decisions. GDPR principles apply where personal data is involved, but commercial confidentiality and national or infrastructure security require additional analysis.

The fifth principle is resilience and portability. Product lifecycles can exceed vendor lifetimes.

Hosting, identifier resolution, credential status and semantic resources require continuity plans, export formats, versioning and tested recovery. The system should degrade safely if an EBW, status service or network is unavailable. Long-lived evidence requires cryptographic agility, including preparation for post-quantum migration where risk and retention justify it.

The sixth principle is explicit system boundary. A battery passport, BESS dossier, vehicle record and AI Service Passport may be linked but are not interchangeable. Each needs an owner, lifecycle, update authority and retention rule. Transformations such as repurposing or aggregation should create lineage rather than silently rewriting identity.

Implementation can proceed in four increments. Foundation establishes identifiers, Registry integration, legal-person onboarding, public and restricted data classes, signing or sealing, resilient hosting and basic audit. Role governance adds issuer registries, PLI schemas, mandates, status and runtime policy for priority roles. Evidence integration adds graph relationships, validation reports, lifecycle events, decision packages and structured provenance. Agentic operation adds workload identity, agent power of attorney, AI Service Passports, tool and action policy, evidence snapshots and human oversight.

Evaluation should use measurable outcomes. Identity metrics include duplicate-organisation rate, verification time and false acceptance or rejection. Authorisation metrics include policy coverage, revocation latency, over-privilege and explanation quality. Data metrics include completeness, provenance coverage, freshness, contradiction rate and validation reproducibility. Operational metrics include resolver availability, recovery time and update latency. Economic metrics include onboarding effort, evidence-reuse rate, reporting cycle time and SME integration cost. AI metrics include traceable-input ratio, unsupported-claim detection and safe intervention.

The research agenda has six priorities. First, conduct cross-Member-State studies of market-role authority and mutual recognition for workshops, recyclers and inspectors. Second, test Registry–wallet convergence prototypes with real company and mandate changes. Third, compare evidence-graph, signed-document, AAS and relational approaches using common DPP decision tasks. Fourth, measure confidentiality leakage from metadata and large-scale queries. Fifth, validate BESS evidence packages against financing, safety and grid-operation decisions. Sixth, define and test bounded agent mandates and AI Service Passport profiles for industrial transactions.

Policy research should examine liability at plane boundaries. If an authorised issuer provides a false role, a wallet presents it correctly, a policy engine accepts it and a relying party acts, responsibility is distributed. Clear rules are needed for issuer diligence, verifier checks, software conformity, operator oversight and redress. Architecture can preserve evidence of each step; it cannot allocate liability by itself.

Standardisation research should align DPP harmonised standards with eIDAS/EBW profiles, W3C credentials and provenance, GS1 identifiers and Digital Link, AAS submodels and dataspace policy vocabularies. Alignment should focus on testable exchanges rather than one universal model. A conformance suite could test organisation enrolment, product registration, role presentation, restricted retrieval, authorised update, revocation and end-of-life evidence.

The expected outcome is a European industrial trust fabric that supports compliance and operations simultaneously. DPPs provide product-linked identity and governed evidence. The Registry provides discoverability and enforcement integration. EBWs can provide reusable legal-person, role and mandate presentations. Evidence graphs connect claims to their sources and decisions. When these capabilities interoperate, reporting simplification, trusted AI and circular-economy operations become different uses of one accountable evidence infrastructure.

16 Conclusion

The DPP's most important evolution is not from paper to QR code, nor from one database technology to another. It is the evolution from a static publication to a governed evidence interface. That interface must reliably connect a product identity, a legal person, a market role or mandate, a policy decision and a provenance-bearing evidence package.

Separating control and data planes makes responsibilities visible. The control plane authenticates organisations and representatives, validates role and mandate, evaluates purpose and policy, checks status and records decisions. The data plane integrates product facts, lifecycle events, source attestations, observations, transformations and validation. A signature participates in both planes by binding an issuer to evidence, but it neither creates authority nor proves truth.

The DPP Registry anchors registration and supports authorities and customs while detailed product content remains decentralised. The proposed EBW could make organisation and representation evidence reusable, but it was not enacted at the evidence cut-off and should not be treated as a universal role authority. Market-role governance remains sectoral. PLI credentials can make it machine verifiable when issuer authority, scope, status and liability are explicit.

Traction batteries demonstrate the regulated passport lifecycle. BESS demonstrates why a product passport must be linked to, but distinguished from, a system-level dossier. Energy data-X shows that fine-grained market-role authorisation is implementable. The CIRPASS-2 catalogue shows that security must cover incentives, continuity, confidentiality, update accountability and end-of-life evidence as well as cyberattack.

Verifiable evidence graphs provide a promising data-plane pattern because they preserve derivation, validation and version context across distributed sources. They should index decision-relevant evidence, not absorb all telemetry or replace every industrial model. Combined with bounded agent authority, they can support trusted industrial and physical AI.

Europe's strategic opportunity is to modernise compliance as reusable evidence infrastructure. The prize is fewer repeated proofs, faster cross-border verification, better enforcement, more reliable circular value chains and AI systems that can explain the evidence and authority behind their actions. The condition is disciplined governance: current law must be distinguished from proposal, identity from authorisation, integrity from truth, product from system, and technical interoperability from institutional trust.

Conflict of interest and positionality

The author is affiliated with Spherity GmbH and has contributed to publications and projects discussed in this article, including work on European Business Wallets, energy data-X and industrial evidence graphs. The CIRPASS-2 risk report acknowledges input from the author on authenticity and authorisation. These relationships create relevant domain access and potential intellectual interest. The article therefore labels implementation evidence, legal requirements and forward-looking proposals separately and relies on official primary sources for legal status.

Data and materials statement

The article is based on public legal acts, official institutional material, standards information, public papers and the attached CIRPASS-2 report. No personal data or confidential operational

data were used. The source register, BibTeX file, figures and complete risk-control mapping accompany the Word manuscript.

A Complete CIRPASS-2 52-risk control mapping

The wording is a concise faithful restatement of the 52 risks in CIRPASS-2 D4.1 v1.1. Control assignments are the author's synthesis. “Both” in the plane column means that governed authority and data/availability controls must operate together.

Table 11 provides the complete 52-risk mapping.

Table 11: CIRPASS-2 lifecycle risk-to-control mapping

Phase	ID	Threat type	Risk	Plane	Primary preventive/detective controls	Residual risk	Priority
Creation	1A	Non-technical	rEO provides too little information	Both	Verified rEO enrolment; product/identifier uniqueness; schema and completeness validation; signed submission; rate limiting; confidential transport.	Medium: requires operational monitoring, redress and periodic control testing.	Medium
Creation	2A	Non-technical	rEO provides too much information	Both	Verified rEO enrolment; product/identifier uniqueness; schema and completeness validation; signed submission; rate limiting; confidential transport.	Medium: requires operational monitoring, redress and periodic control testing.	Medium
Creation	3A	Non-technical	rEO provides incorrect information	Both	Verified rEO enrolment; product/identifier uniqueness; schema and completeness validation; signed submission; rate limiting; confidential transport.	Medium–high: factual misconduct or ecosystem-scale aggregation cannot be eliminated technically.	High
Creation	4A	Non-technical	rEO reuses its own DPP for another product	Both	Verified rEO enrolment; product/identifier uniqueness; schema and completeness validation; signed submission; rate limiting; confidential transport.	Medium: requires operational monitoring, redress and periodic control testing.	Medium
Creation	5A	Non-technical	rEO uses the DPP of another rEO	Both	Verified rEO enrolment; product/identifier uniqueness; schema and completeness validation; signed submission; rate limiting; confidential transport.	Medium: requires operational monitoring, redress and periodic control testing.	High
Creation	6A	Both	Fake rEO submits a bogus DPP	Both	Verified rEO enrolment; product/identifier uniqueness; schema and completeness validation; signed submission; rate limiting; confidential transport.	Medium: requires operational monitoring, redress and periodic control testing.	High
Creation	7A	Technical	Excessive DPP submissions cause denial of service	Both	Verified rEO enrolment; product/identifier uniqueness; schema and completeness validation; signed submission; rate limiting; confidential transport.	Medium: requires operational monitoring, redress and periodic control testing.	Medium
Creation	8A	Non-technical	rEO creates a product but no DPP	Both	Verified rEO enrolment; product/identifier uniqueness; schema and completeness validation; signed submission; rate limiting; confidential transport.	Medium: requires operational monitoring, redress and periodic control testing.	Medium
Creation	9A	Technical	Creation information is intercepted	Both	Verified rEO enrolment; product/identifier uniqueness; schema and completeness validation; signed submission; rate limiting; confidential transport.	Medium: requires operational monitoring, redress and periodic control testing.	Medium

Continued on next page

Table 11 continued

Phase	ID	Threat type	Risk	Plane	Primary preventive/detective controls	Residual risk	Priority
Storage	10A	Non-technical	Host deletes DPP information	Both	Integrity-protected versions; least-privilege host access; encryption; independent backup; portability/exit plan; monitored status and carrier binding.	Medium: requires operational monitoring, redress and periodic control testing.	Medium
Storage	11A	Technical	Host stops operating	Both	Integrity-protected versions; least-privilege host access; encryption; independent backup; portability/exit plan; monitored status and carrier binding.	Medium: requires operational monitoring, redress and periodic control testing.	High
Storage	12A	Technical	Cyberattack causes DPP loss	Both	Integrity-protected versions; least-privilege host access; encryption; independent backup; portability/exit plan; monitored status and carrier binding.	Medium: requires operational monitoring, redress and periodic control testing.	High
Storage	13A	Non-technical	Host alters DPP information	Both	Integrity-protected versions; least-privilege host access; encryption; independent backup; portability/exit plan; monitored status and carrier binding.	Medium: requires operational monitoring, redress and periodic control testing.	Medium
Storage	14A	Technical	Cyberattack alters DPP information	Both	Integrity-protected versions; least-privilege host access; encryption; independent backup; portability/exit plan; monitored status and carrier binding.	Medium: requires operational monitoring, redress and periodic control testing.	Medium
Storage	15A	Non-technical	Carrier is replaced or hidden to link to a different DPP	Both	Integrity-protected versions; least-privilege host access; encryption; independent backup; portability/exit plan; monitored status and carrier binding.	Medium: requires operational monitoring, redress and periodic control testing.	High
Storage	16A	Non-technical	Carrier is replaced or hidden to link to a malicious webpage	Both	Integrity-protected versions; least-privilege host access; encryption; independent backup; portability/exit plan; monitored status and carrier binding.	Medium: requires operational monitoring, redress and periodic control testing.	High
Storage	17A	Non-technical	Host accesses information it should not access	Both	Integrity-protected versions; least-privilege host access; encryption; independent backup; portability/exit plan; monitored status and carrier binding.	Medium: requires operational monitoring, redress and periodic control testing.	Medium
Storage	18A	Technical	Cyberattack steals DPP information	Both	Integrity-protected versions; least-privilege host access; encryption; independent backup; portability/exit plan; monitored status and carrier binding.	Medium: requires operational monitoring, redress and periodic control testing.	High
Storage	19A	Non-technical	Malicious actor pretends to have access rights	Both	Integrity-protected versions; least-privilege host access; encryption; independent backup; portability/exit plan; monitored status and carrier binding.	Medium: requires operational monitoring, redress and periodic control testing.	High

Continued on next page

Table 11 continued

Phase	ID	Threat type	Risk	Plane	Primary preventive/detective controls	Residual risk	Priority
Storage	20A	Non-technical	Malicious actor induces an authorised party to leak confidential information	Both	Integrity-protected versions; least-privilege host access; encryption; independent backup; portability/exit plan; monitored status and carrier binding.	Medium–high: factual misconduct or ecosystem-scale aggregation cannot be eliminated technically.	High
Retrieval	21A	Technical	Physical actor makes the carrier unusable	Both	Resilient resolver; secure transport; privacy-preserving access; field classification; role/purpose policy; bulk-query and anomaly controls.	Medium: requires operational monitoring, redress and periodic control testing.	Medium
Retrieval	22A	Non-technical	rEO attaches a low-quality carrier that degrades	Both	Resilient resolver; secure transport; privacy-preserving access; field classification; role/purpose policy; bulk-query and anomaly controls.	Medium: requires operational monitoring, redress and periodic control testing.	Medium
Retrieval	23A	Both	Handler destroys the carrier	Both	Resilient resolver; secure transport; privacy-preserving access; field classification; role/purpose policy; bulk-query and anomaly controls.	Medium: requires operational monitoring, redress and periodic control testing.	Medium
Retrieval	24A	Technical	Redirect service stops operating	Both	Resilient resolver; secure transport; privacy-preserving access; field classification; role/purpose policy; bulk-query and anomaly controls.	Medium: requires operational monitoring, redress and periodic control testing.	High
Retrieval	25A	Technical	Denial-of-service attack targets redirect service	Both	Resilient resolver; secure transport; privacy-preserving access; field classification; role/purpose policy; bulk-query and anomaly controls.	Medium: requires operational monitoring, redress and periodic control testing.	High
Retrieval	26A	Technical	Retrieved information is intercepted	Both	Resilient resolver; secure transport; privacy-preserving access; field classification; role/purpose policy; bulk-query and anomaly controls.	Medium: requires operational monitoring, redress and periodic control testing.	Medium
Retrieval	27A	Technical	Retrieved information is intercepted and modified	Both	Resilient resolver; secure transport; privacy-preserving access; field classification; role/purpose policy; bulk-query and anomaly controls.	Medium: requires operational monitoring, redress and periodic control testing.	Medium
Retrieval	28A	Technical	Man-in-the-middle attack occurs between host and requester	Both	Resilient resolver; secure transport; privacy-preserving access; field classification; role/purpose policy; bulk-query and anomaly controls.	Medium: requires operational monitoring, redress and periodic control testing.	High
Retrieval	29A	Technical	Actor monitors internet traffic	Both	Resilient resolver; secure transport; privacy-preserving access; field classification; role/purpose policy; bulk-query and anomaly controls.	Medium: requires operational monitoring, redress and periodic control testing.	Medium

Continued on next page

Table 11 continued

Phase	ID	Threat type	Risk	Plane	Primary preventive/detective controls	Residual risk	Priority
Retrieval	30A	Technical	Actor identifies end users	Both	Resilient resolver; secure transport; privacy-preserving access; field classification; role/purpose policy; bulk-query and anomaly controls.	Medium: requires operational monitoring, redress and periodic control testing.	Medium
Retrieval	31A	Non-technical	Actor aggregates supply-chain dependencies	Both	Resilient resolver; secure transport; privacy-preserving access; field classification; role/purpose policy; bulk-query and anomaly controls.	Medium–high: factual misconduct or ecosystem-scale aggregation cannot be eliminated technically.	High
Retrieval	32A	Non-technical	Actor aggregates product properties for sensitive equipment	Both	Resilient resolver; secure transport; privacy-preserving access; field classification; role/purpose policy; bulk-query and anomaly controls.	Medium–high: factual misconduct or ecosystem-scale aggregation cannot be eliminated technically.	High
Retrieval	33A	Non-technical	Actor uses dependencies for spear phishing	Both	Resilient resolver; secure transport; privacy-preserving access; field classification; role/purpose policy; bulk-query and anomaly controls.	Medium: requires operational monitoring, redress and periodic control testing.	Medium
Retrieval	34A	Non-technical	Actor maps strategic autonomy or product capability	Both	Resilient resolver; secure transport; privacy-preserving access; field classification; role/purpose policy; bulk-query and anomaly controls.	Medium–high: factual misconduct or ecosystem-scale aggregation cannot be eliminated technically.	High
Update	35A	Non-technical	rEO provides an incorrect update	Both	Scoped updater mandate; role/status verification; event provenance; versioning; plausibility checks; physical–digital consistency controls.	Medium–high: factual misconduct or ecosystem-scale aggregation cannot be eliminated technically.	High
Update	36A	Non-technical	Authorised actor provides an incorrect update	Both	Scoped updater mandate; role/status verification; event provenance; versioning; plausibility checks; physical–digital consistency controls.	Medium–high: factual misconduct or ecosystem-scale aggregation cannot be eliminated technically.	High
Update	37A	Non-technical	Excessive update frequency or history impairs usability	Both	Scoped updater mandate; role/status verification; event provenance; versioning; plausibility checks; physical–digital consistency controls.	Medium: requires operational monitoring, redress and periodic control testing.	Medium
Update	38A	Non-technical	Unauthorised actor pretends to have update rights	Both	Scoped updater mandate; role/status verification; event provenance; versioning; plausibility checks; physical–digital consistency controls.	Medium: requires operational monitoring, redress and periodic control testing.	High
Update	39A	Technical	Authorised updater is compromised	Both	Scoped updater mandate; role/status verification; event provenance; versioning; plausibility checks; physical–digital consistency controls.	Medium: requires operational monitoring, redress and periodic control testing.	High

Continued on next page

Table 11 continued

Phase	ID	Threat type	Risk	Plane	Primary preventive/detective controls	Residual risk	Priority
Update	40A	Non-technical	Intermediate operator changes product but neglects DPP update	Both	Scoped updater mandate; role/status verification; event provenance; versioning; plausibility checks; physical–digital consistency controls.	Medium: requires operational monitoring, redress and periodic control testing.	High
Update	41A	Non-technical	End user changes product without DPP update	Both	Scoped updater mandate; role/status verification; event provenance; versioning; plausibility checks; physical–digital consistency controls.	Medium: requires operational monitoring, redress and periodic control testing.	Medium
Update	42A	Non-technical	Third party changes product without DPP update	Both	Scoped updater mandate; role/status verification; event provenance; versioning; plausibility checks; physical–digital consistency controls.	Medium: requires operational monitoring, redress and periodic control testing.	Medium
Update	43A	Non-technical	Intermediate operator changes product and DPP inaccurately	Both	Scoped updater mandate; role/status verification; event provenance; versioning; plausibility checks; physical–digital consistency controls.	Medium: requires operational monitoring, redress and periodic control testing.	High
Update	44A	Non-technical	End user changes product and DPP inaccurately	Both	Scoped updater mandate; role/status verification; event provenance; versioning; plausibility checks; physical–digital consistency controls.	Medium: requires operational monitoring, redress and periodic control testing.	Medium
Update	45A	Non-technical	Third party changes product and DPP inaccurately	Both	Scoped updater mandate; role/status verification; event provenance; versioning; plausibility checks; physical–digital consistency controls.	Medium: requires operational monitoring, redress and periodic control testing.	Medium
Deletion	46A	Non-technical	Recycler falsely reports that product was destroyed	Both	Recycler/facility credential; custody, receipt and treatment evidence; reconciliation; authority/audit checks; close-not-erase retention policy.	Medium–high: factual misconduct or ecosystem-scale aggregation cannot be eliminated technically.	High
Deletion	47A	Non-technical	End user falsely reports that product was destroyed	Both	Recycler/facility credential; custody, receipt and treatment evidence; reconciliation; authority/audit checks; close-not-erase retention policy.	Medium–high: factual misconduct or ecosystem-scale aggregation cannot be eliminated technically.	Medium
Deletion	48A	Non-technical	Host destroys DPP while claiming recycling	Both	Recycler/facility credential; custody, receipt and treatment evidence; reconciliation; authority/audit checks; close-not-erase retention policy.	Medium: requires operational monitoring, redress and periodic control testing.	High
Deletion	49A	Non-technical	Fake recycler reports destruction	Both	Recycler/facility credential; custody, receipt and treatment evidence; reconciliation; authority/audit checks; close-not-erase retention policy.	Medium: requires operational monitoring, redress and periodic control testing.	High

Continued on next page

Table 11 continued

Phase	ID	Threat type	Risk	Plane	Primary preventive/detective controls	Residual risk	Priority
Deletion	50A	Non-technical	Recycler fails to notify destruction	Both	Recycler/facility credential; custody, receipt and treatment evidence; reconciliation; authority/audit checks; close-not-erase retention policy.	Medium: requires operational monitoring, redress and periodic control testing.	High
Deletion	51A	Non-technical	Product is lost and owner fails to notify	Both	Recycler/facility credential; custody, receipt and treatment evidence; reconciliation; authority/audit checks; close-not-erase retention policy.	Medium: requires operational monitoring, redress and periodic control testing.	Medium
Deletion	52A	Non-technical	Product goes to landfill but DPP is not closed	Both	Recycler/facility credential; custody, receipt and treatment evidence; reconciliation; authority/audit checks; close-not-erase retention policy.	Medium: requires operational monitoring, redress and periodic control testing.	High

Source: Risk identifiers and lifecycle grouping from Roefs et al. (2026); controls, residual risk and priority are the author's assessment.

B Minimum PLI credential and governance profile

Table 12 defines the minimum PLI credential and governance profile.

Table 12: PLI profile

Element	Minimum content	Purpose
Credential subject	Legal person and, where relevant, facility or organisational unit	Prevents role claims from floating free of an accountable organisation.
Role and vocabulary	Machine-readable role plus human-readable definition	Avoids ambiguous labels such as a universal "workshop" or "recycler".
Product/asset scope	Product group, family, item, BESS site or identifier pattern	Limits a valid role to the relevant product context.
Jurisdiction and competence	Territory, authority domain and legal/contractual basis	Supports cross-border policy without assuming full harmonisation.
Permitted actions	Read classes, update event types, registration, dispatch or end-of-life	Converts identity evidence into an authorisation input.
Issuer authority	Issuer identifier, trust-framework entry, assurance and audit	A credential from an unauthorised issuer is rejected.
Validity and status	Issuance, expiry, suspension/revocation endpoint and reason profile	Enables runtime freshness and incident response.
Mandate binding	Principal, delegate/agent, action scope, time, value limits and delegation	Separates company role from the authority of the presenter.
Liability and redress	Issuer, holder and verifier duties; dispute and appeal route	Makes institutional accountability explicit.

C BESS decision evidence packages

Table 13 specifies five decision-specific BESS evidence packages.

Table 13: BESS decision packages

Decision	Required evidence	Minimisation boundary	Control-plane conditions
Finance/insurance	Owner/operator mandate; asset identity; component DBPs; commissioning; warranty; maintenance compliance; degradation trend; unresolved safety/cyber incidents	Limited operational summary; exclude raw dispatch strategy and unnecessary supplier detail	Financier/insurer role, transaction purpose, NDA/usage obligation
Grid/flexibility	Market participant role; connection and metering identifiers; current capability; operational envelope; availability and constraint evidence	Time-bounded capability projection; retain high-resolution telemetry in historian	Market-role credential, asset mandate, technical trust and data-use policy
Maintenance	Work order; service role; manuals; diagnostic features; firmware/configuration; prior repair and safety events	Product-family and job-scoped disclosure; time-limited access	Service-provider identity, technician/workload mandate, site and maintenance window
Safety/authority	System configuration; alarm/incident timeline; component evidence; corrective action; test and inspection results	Statutory case projection with enhanced logging	Authority role, jurisdiction, case purpose and officer/system mandate
Decommissioning	Owner authority; component identities; custody; recycler permit; receipt, treatment and successor material evidence	Retain minimum immutable audit record after operational closure	Facility and waste-stream role, product binding and corroborated treatment event

D Evidence-quality and data-risk scoring rubric

Table 14 defines the four-level evidence-assurance rubric.

Table 14: Four-level evidence assurance rubric

Dimension	Level 0	Level 1	Level 2	Level 3
Issuer authority	Unknown or self-asserted	Known party; authority not proven	Accepted issuer profile	Authoritative source or supervised issuer
Integrity/status	No verifiable binding	Signature without status	Verified proof and current status	Verified proof, status, timestamp and validation record
Provenance	No source	Source named	Method and derivation linked	Reproducible evidence path and immutable snapshot
Completeness	Required elements absent	Material gaps	Decision profile satisfied	Satisfied plus independent cross-check
Freshness	Unknown	Potentially stale	Within policy interval	Continuous/event-driven status where proportionate
Contradiction	Unresolved conflict	Conflict flagged	Conflict resolved/documented	Automated impact analysis and redress trail
Confidentiality	Unclassified or excessive	Coarse restriction	Field-level policy and minimisation	Selective proof, usage control and monitored aggregation
Operational impact	No impact analysis	Qualitative impact	Decision-specific risk score	Threshold, escalation and human oversight tested

E Legal-status and claim ledger

Table 15 records the legal-status formulation discipline used in the article.

Table 15: Claim discipline

Claim	Category	Permitted formulation	Primary evidence
DPP Registry operational date	Operational fact	20 July 2026	Commission announcement and Implementing Regulation (EU) 2026/1778
Registry content	Operational/legal interpretation	Identifiers, registration data and metadata; complete DPP remains decentralised	Commission Registry portal and User Guide v1.01
DBP scope/date	Binding law with future application	Article 77 duty from 18 February 2027 for specified batteries	Regulation (EU) 2023/1542
EBW status	Legislative proposal	COM(2025) 838; Council general approach; Parliament work ongoing	Commission proposal, Council release and EP tracker
Harmonised DPP standards	OJEU citation	Six cited at cut-off	Implementing Decision (EU) 2026/1736
BESS passport	Architectural proposal	Voluntary system dossier linked to component DBPs	This article and energy data-X reference use case
AI Service Passport	Architectural proposal	Evidence and mandate object for AI service/agent	This article and Stöcker (2026)
EBW benefit figures	Scenario estimate	Adoption- and network-effect dependent; not realised savings	COM(2025) 838 cost-benefit material

References and source corpus

[1] European Parliament, and Council, "Regulation (EU) 2024/1781 establishing a framework for ecodesign requirements for sustainable products," 2024. *EU Regulation; status at 31 July 2026: Enacted.* https://eur-lex.europa.eu/eli/reg/2024/1781/oj/eng

[2] European Parliament, and Council, "Regulation (EU) 2023/1542 concerning batteries and waste batteries," 2023. *EU Regulation; status at 31 July 2026: Enacted.* https://eur-lex.europa.eu/eli/reg/2023/1542/oj/eng

[3] Roefs, David, and others, "CIRPASS-2 D4.1: Risks and Mitigations, version 1.1," 2026. *Research report; status at 31 July 2026: Published.* https://zenodo.org/records/20670585

[4] European Commission, "Digital Product Passport Registry now live," 2026. *Official announcement; status at 31 July 2026: Operational.* https://single-market-economy.ec.europa.eu/news/digital-product-passport-registry-now-live-2026-07-20_en

[5] European Commission, "DPP Registry User Guide for Economic Operators, version 1.01," 2026. *Official user guide; status at 31 July 2026: Operational guidance.* https://single-market-economy.ec.europa.eu/document/download/079a45e2-469f-4eec-b1e5-32e8e05d1357_en?filename=dpp_registry_user_guide_for_economic_operators.pdf

[6] Stöcker, Carsten, "The 2×2 Matrix: DPPs and the paradigm shift toward dynamic, AI-driven supply chains," 2024. *Concept article; status at 31 July 2026: Published.* https://medium.com/spherity/the-2x2-matrix-dpps-and-the-paradigm-shift-toward-dynamic-ai-driven-supply-chains-c8a4541ab1b5

[7] Stöcker, Carsten, "Digital identity, real-world impact: The industrial upside of the European Business Wallet," 2025. *Concept article; status at 31 July 2026: Published.* https://medium.com/spherity/digital-identity-real-world-impact-the-industrial-upside-of-the-european-business-wallet-eubw-d9e0c4e96aae

[8] Stöcker, Carsten, "The European Business Wallet: A strategic pillar for digital identity and industrial transformation," 2025. *Concept article; status at 31 July 2026: Published.* https://medium.com/spherity/the-european-business-wallet-a-strategic-pillar-for-digital-identity-and-industrial-3f9983f7b299

[9] Gößling, Jan-Niklas, and Hoffmann, René, and Kießling, Axel, and Rohrbach, Daniel, and Stöcker, Carsten, "The energy data-X data ecosystem: Cross-sector and BESS data exchange enabled by the European Business Wallet and market role credentials," 2026. *Journal article; status at 31 July 2026: Published reference use case.*

[10] Stöcker, Carsten, "Evidence Graphs for Industrial AI: Data-plane architectures for global supply chains, Industry 4.0, critical infrastructure, and B2G data exchange from a German perspective," 2026. *Research paper; status at 31 July 2026: Perspective draft.*

[11] Industrial Digital Twin Association, "Asset Administration Shell specifications," 2026. *Industry specification; status at 31 July 2026: Published.* https://industrialdigitaltwin.org/en/content-hub/asspecifications

[12] European Commission, "Commission Implementing Regulation (EU) 2026/1778 laying down implementation arrangements for the DPP Registry," 2026. *Implementing Regulation; status at 31 July 2026: Enacted/operational.* https://eur-lex.europa.eu/eli/reg_impl/2026/1778/oj/eng

[13] European Commission, "Digital Product Passport for batteries," 2026. *Official portal; status at 31 July 2026: Implementation guidance.* https://single-market-economy.ec.europa.eu/single-market/digital-product-passport/batteries_en

[14] European Parliament, and Council, "Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 as regards the European Digital Identity Framework," 2024. *EU Regulation; status at 31 July 2026: Enacted.* https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng

[15] European Parliament, and Council, "Directive (EU) 2025/25 as regards further expanding and upgrading the use of digital tools and processes in company law," 2025. *EU Directive; status at 31 July 2026: Enacted; transposition/application pending.* https://eur-lex.europa.eu/eli/dir/2025/25/oj/eng

[16] European Commission, "Proposal for a Regulation establishing European Business Wallets, COM(2025) 838 final," 2025. *Legislative proposal; status at 31 July 2026: Proposed.* https://ec.europa.eu/transparency/documents-register/api/files/COM(2025)838_0/090166e5258f2ef0

[17] Council of the European Union, "European business wallets: Council adopts negotiating position," 2026. *Council position; status at 31 July 2026: Legislative negotiation.* https://www.consilium.europa.eu/en/press/press-releases/2026/06/09/european-business-wallets-council-adopts-negotiating-position/

[18] European Parliament, "Legislative Train: European Business Wallet," 2026. *Procedure tracker; status at 31 July 2026: Ongoing.* https://www.europarl.europa.eu/legislative-train/theme-internal-market-and-consumer-protection-imco/file-european-business-wallet

[19] European Commission, "Commission Implementing Decision (EU) 2026/1736 on harmonised DPP standards," 2026. *Implementing Decision; status at 31 July 2026: Enacted.* https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ%3AL_202601736

[20] CEN, and CENELEC, "European standards for Digital Product Passports," 2026. *Standards-body overview; status at 31 July 2026: Published.* https://www.cencenelec.eu/news-events/news/2026/en-in-the-spotlight/2026-07-15-dpp/

[21] W3C, "Verifiable Credentials Data Model v2.0," 2025. *W3C Recommendation; status at 31 July 2026: Standard.* https://www.w3.org/TR/vc-data-model-2.0/

[22] W3C, "Verifiable Credential Data Integrity 1.0," 2025. *W3C Recommendation; status at 31 July 2026: Standard.* https://www.w3.org/TR/vc-data-integrity/

[23] W3C, "Decentralized Identifiers (DIDs) v1.0," 2022. *W3C Recommendation; status at 31 July 2026: Standard.* https://www.w3.org/TR/did-core/

[24] W3C, "JSON-LD 1.1," 2020. *W3C Recommendation; status at 31 July 2026: Standard.* https://www.w3.org/TR/json-ld11/

[25] W3C, "Shapes Constraint Language (SHACL)," 2017. *W3C Recommendation; status at 31 July 2026: Standard.* https://www.w3.org/TR/shacl/

[26] W3C, "PROV-O: The PROV Ontology," 2013. *W3C Recommendation; status at 31 July 2026: Standard.* https://www.w3.org/TR/prov-o/

[27] NIST, "SP 800-207: Zero Trust Architecture," 2020. *Technical guideline; status at 31 July 2026: Published.* https://doi.org/10.6028/NIST.SP.800-207

[28] European Parliament, and Council, "Regulation (EU) 2016/679 (General Data Protection Regulation)," 2016. *EU Regulation; status at 31 July 2026: Enacted.* https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

[29] GS1, "GS1 Digital Link," 2026. *Industry standard; status at 31 July 2026: Published.* https://www.gs1.org/standards/gs1-digital-link

[30] NIST, "FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard," 2024. *Cryptographic standard; status at 31 July 2026: Published.* https://csrc.nist.gov/pubs/fips/203/final

[31] European Parliament, and Council, "Regulation (EU) 2018/1724 establishing a Single Digital Gateway," 2018. *EU Regulation; status at 31 July 2026: Enacted.* https://eur-lex.europa.eu/eli/reg/2018/1724/oj/eng

[32] European Commission, "Commission Implementing Regulation (EU) 2022/1463 on the Once-Only Technical System," 2022. *Implementing Regulation; status at 31 July 2026: Enacted.* https://eur-lex.europa.eu/eli/reg_impl/2022/1463/oj/eng

[33] European Commission, "Simplification, implementation and enforcement," 2026. *Official policy page; status at 31 July 2026: Policy.* https://commission.europa.eu/law/law-making-process/better-regulation/simplification-implementation-and-enforcement/simplification_en

[34] European Commission, "A Competitiveness Compass for the EU," 2025. *Commission communication; status at 31 July 2026: Policy.* https://commission.europa.eu/topics/competitiveness/competitiveness-compass_en

[35] European Commission, "The Single Market: our European home market in an uncertain world, COM(2025) 500," 2025. *Commission communication; status at 31 July 2026: Policy.* https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52025DC0500

[36] European Commission, "DPP Registry," 2026. *Official portal; status at 31 July 2026: Operational.* https://single-market-economy.ec.europa.eu/single-market/digital-product-passport/dpp-registry_en

[37] European Parliament, and Council, "Regulation (EU) 2019/1020 on market surveillance and compliance of products," 2019. *EU Regulation; status at 31 July 2026: Enacted.* https://eur-lex.europa.eu/eli/reg/2019/1020/oj/eng

[38] European Parliament, and Council, "Regulation (EU) No 952/2013 laying down the Union Customs Code," 2013. *EU Regulation; status at 31 July 2026: Enacted.* https://eur-lex.europa.eu/eli/reg/2013/952/oj/eng

[39] European Parliament, and Council, "Directive (EU) 2022/2555 on measures for a high common level of cybersecurity (NIS2)," 2022. *EU Directive; status at 31 July 2026: Enacted.* https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

[40] European Parliament, and Council, "Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements," 2024. *EU Regulation; status at 31 July 2026: Enacted; staged application.* https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

[41] European Parliament, and Council, "Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence," 2024. *EU Regulation; status at 31 July 2026: Enacted; staged application.* https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

[42] W3C, and OGC, "Semantic Sensor Network Ontology," 2017. *W3C Recommendation; status at 31 July 2026: Standard.* https://www.w3.org/TR/vocab-ssn/