Global Digital Product Passports

Regulation, Interoperability and Shared Evidence Infrastructure

Spherity Research Whitepaper

Dr. Carsten Stöcker
Spherity GmbH, Germany

Final version 1.0 | Prepared: 25 October 2026



Except where otherwise noted, this work is licensed under the Creative Commons Attribution 4.0 International License (CC BY 4.0). © 2026 Dr. Carsten Stöcker, Spherity GmbH.

Dataset 0.1.0: 23 October 2026 | Manuscript update: 25 October 2026 | Not peer reviewed

Research focus. How do fragmented DPP requirements connect through shared semantics, verifiable evidence and business identity—and where does interoperability remain unproven?

Abstract

A battery passport may provide a carbon-footprint value without showing whether its measurement method, issuer and supporting evidence are acceptable to the recipient. Digital Product Passport (DPP) interoperability therefore requires more than exchanging readable records. This paper examines how fragmented requirements connect through semantics, evidence and business identity, using a selected evidence atlas and comparative documentary analysis. The frozen baseline contains 203 entities, 224 assertions and 112 sources; a separately dated manuscript supplement updates the regulatory calendar, EU registry developments and CIRPASS-2 risk analysis. The findings distinguish overlapping functions and reported technical exchange from demonstrated semantic equivalence or institutional recognition. One externally reported Japan–Catena-X exchange supports a bounded result; the corpus does not establish worldwide interoperability. Computational checks establish reproducibility of the research artifact, while independent human review and new exchange experiments remain planned. The architectural proposition is: **Access-controlled, verifiable evidence graphs for physical products, virtual products and physical AI—built on open international standards and open-world semantics.** For example, a robot may need connected evidence about a replaceable battery, a software skill and the conditions under which their combination was assessed. The proposed infrastructure connects these records while preserving permissions, provenance, status and uncertainty. It does not make signatures proof of truth or a passport proof of safety. W3C and UNTP work connects product evidence with business identity; ODRL can express access and usage policies. Their composition remains a proposal requiring interoperable enforcement and scoped recognition. Four prospective scenarios explore different combinations of technical interoperability and institutional recognition. A dated implementation guide identifies near-term decisions and tests needed before this shared infrastructure can support both product compliance and AI-assisted operations.

Keywords. Digital Product Passport; ESPR; W3C; UNTP; business wallets; ODRL; evidence graph; access control; data spaces; physical AI

Contents

1 Introduction **4**
- 1.1 From a readable record to a defensible decision . . . 4
- 1.2 Research question and contribution . . . 4

2 Related work, method and evidence boundaries **5**
- 2.1 Related work and the unit of comparison . . . 5
- 2.2 Selection and source access . . . 7
- 2.3 Time, geography and manuscript updates . . . 8

3 A global regulatory calendar obligations, proposals and dependencies **11**
- 3.1 Reading the calendar without creating a universal deadline . . . 11
- 3.2 The EU product sequence fixed obligations and indicative adoption targets . . . 11
- 3.3 Global comparison and adjacent connected-product duties . . . 13

4 The European Product Act an evolving legislative package **15**
- 4.1 A package name is not a single enacted passport obligation . . . 15
- 4.2 Implications for convergence, with the evidentiary boundary intact . . . 15

5 Standards connections and candidate interoperability mechanisms **16**
- 5.1 Identification, carriers and resolution . . . 16
- 5.2 Semantics, profiles and industrial information models . . . 16
- 5.3 Evidence, assurance and provenance . . . 17
- 5.4 Business identity, delegated authority and access . . . 17
- 5.5 Publication, legal citation and institutional routes . . . 18
- 5.6 What the two AAS RDF papers establish . . . 18
- 5.7 International commitment and adoption in four distinct cases . . . 20
- 5.8 AAS as an initial experimental infrastructure . . . 22

6 The EU registry, shared semantics and a prospective lean dataspace **22**
- 6.1 What the registry does, and what its dates establish . . . 22
- 6.2 An operational qualification that changes the interpretation of launch . . . 23
- 6.3 Identity, registration evidence and the limits of a successful check . . . 23
- 6.4 A lean dataspace as a testable design proposal . . . 24

7 Access control business wallets and verifiable evidence graphs **27**
- 7.1 What the lifecycle catalogue establishes . . . 27
- 7.2 Identity, authority and action-specific permission . . . 27
- 7.3 W3C and DPP business wallet convergence . . . 27
- 7.4 Recognized entities and UNTP identity anchors . . . 28
- 7.5 ODRL policies and enforcement in data spaces . . . 28
- 7.6 A common policy layer for B2B and B2G operations . . . 29
- 7.7 From a wallet presentation to a verifiable evidence graph . . . 30
- 7.8 Authentic provenance can accompany false claims . . . 32
- 7.9 Confidentiality, status and cached decisions . . . 32
- 7.10 Continuity and the physical product boundary . . . 32
- 7.11 Local context, memory and accountable evaluation . . . 33

8 What interoperability and atlas checks establish **34**
- 8.1 A bounded external exchange report . . . 34
- 8.2 Completed research-artifact verification . . . 36

9 Evidence Graphs as Shared Infrastructure for Products and AI **37**
9.1 A shared infrastructure proposition 37
9.2 Open-world integration and bounded decisions 37
9.3 A continuum of evidence subjects 38
9.4 A humanoid-arm replacement and firmware update 40
9.5 AI first infrastructure and the risk of architectural displacement 40

10 Scenarios for Global DPP Convergence **41**
10.1 Two independent dimensions 41
10.2 Fragmented compliance limited exchange and limited recognition 43
10.3 Connected evidence exchange without portable recognition 43
10.4 Recognised networks accepted partners with constrained exchange 43
10.5 Federated evidence corridors bounded exchange and recognition 43
10.6 Value beyond ESPR and a measurable research programme 44

11 Limitations, disclosure and planned validation **45**
11.1 Limits of the evidence and author position 45
11.2 Tests required before stronger claims 46

12 Conclusion and implementation guide **47**
12.1 What the study supports 47
12.2 Practical implementation sequence 47

A Geographic coverage **49**

References **51**

1 Introduction

1.1 From a readable record to a defensible decision

Imagine a repairer considering a used electric-vehicle battery. A QR code opens a record with its identity, composition and carbon footprint. The record may be authentic yet insufficient for a second-life decision: which test supports its condition, when was it performed, who was competent to perform it, and may the repairer inspect the underlying evidence? Now imagine that an AI assistant recommends the reuse. The same questions remain, with an additional one: was the assistant authorised to make the recommendation or commit the business to it? These are illustrative decision problems, not experiments reported in this paper.

Digital Product Passports connect product information with lifecycle responsibilities and access conditions. The EU Ecodesign for Sustainable Products Regulation (ESPR) supplies a horizontal framework; the Batteries Regulation specifies a sectoral passport. Other jurisdictions use related identification, reporting and supply-chain instruments. Their functions may overlap without becoming the same legal object. A Chinese battery-coding rule, a European passport duty and a voluntary assurance programme must retain their distinct scopes and legal effects. [1, 2]

The paper uses one architectural anchor throughout: **Access-controlled, verifiable evidence graphs for physical products, virtual products and physical AI—built on open international standards and open-world semantics.**

An evidence graph links a claim to the product or service it concerns, the supporting records, the people or organisations responsible, and the conditions under which it can be used. Access control determines who can inspect or act on those links. Verification checks such properties as issuer binding, integrity, validity and status. Open-world semantics allows information from additional sources to extend the description without pretending the existing record is complete. An absence of evidence remains an unanswered question; it is not automatically evidence of absence.

This anchor connects the present study with Spherity's research on the industrial AI data plane: "Industrial AI needs evidence paths that preserve source, transformation, time, issuer, status, uncertainty, and validation context—not only retrieved text." That work proposes an architecture, not a direct performance benchmark between AAS and linked-data serialisations. Here, its relevance is the shared need for inspectable evidence in product decisions and AI-assisted decisions. Section 9 develops that proposition and the limits of the analogy. [3]

1.2 Research question and contribution

The research question is: How do fragmented DPP requirements converge through shared semantics, verifiable evidence and business identity—and where does interoperability remain unproven? Convergence is investigated rather than assumed. A cross-sectional, purposively selected corpus cannot establish a worldwide trend or attribute an improvement to a particular technology. The analysis asks which requirements address comparable functions, which versioned artifacts connect those functions, what exchange operations have supporting evidence, and what the research atlas itself has actually verified.

Three outcomes must be kept distinct. Functional correspondence means that requirements address a comparable problem. Demonstrated exchange means that identified systems perform a bounded operation. Recognised evidence or authority means that an institution or declared policy accepts the issuer, evidence or action for a particular purpose. A successful technical

transfer need not establish legal recognition; an accepted domestic certificate need not have a cross-system exchange path.

The contribution is a source-qualified analytical framework and a reproducible research artifact, coupled with a clearly labelled architecture proposal and prospective scenarios. Release 0.1.0 remains frozen at 23 October 2026. Targeted manuscript checks through 25 October form a separate supplement, including corrections and additions concerning earlier events. They do not retrospectively enlarge the original corpus or convert its assertions into independently reviewed findings. Sections 3–8 report documentary observations and completed checks, with the design proposals and unperformed tests in Sections 5–7 explicitly identified; Section 9 develops the shared infrastructure proposition; Section 10 presents scenarios; Section 11 specifies unperformed validation. [4,5] The AAS supplement analyses two full texts and distinguishes national standards, public programmes and prototypes from adoption prevalence and AI readiness. Its outlook remains a scenario, not an adoption survey. [6,7]

The expanded access-control analysis asks how a passport about a product and a wallet representing a business can work together. It distinguishes identity binding, recognition of a particular role, and permission to perform an action. Sections 7.3–7.7 connect the W3C and UNTP work with data-space services and a proposed ODRL policy profile; they retain the maturity and validation limits of each component.

2 Related work, method and evidence boundaries

2.1 Related work and the unit of comparison

DPP research already contains landscape reviews, product ontologies, architecture proposals and implemented applications. Psarommatis and May classify 225 studies across manufacturing, information modelling, architecture, governance and sustainability evidence. Lyse and Huang examine a narrower corpus of 32 framework studies, distinguishing design elaboration from validation maturity. Their reported limits on cross-organisational and lifecycle evaluation apply to their selected academic corpus, not every industrial deployment. Neither an inventory of initiatives nor identification of a validation gap is therefore a new contribution by itself. This paper instead examines the traceability and qualification of particular legal, technical and exchange claims. [8,9]

Ontology research makes the semantic problem concrete. Robal, Maigre and Haav derive requirements for a core ontology from ESPR. Hbeich and colleagues address semantic interoperability within and between heterogeneous DPP systems. Their publisher abstracts support these stated aims; they do not support an independent assessment here of implemented transformations or benchmark performance. A regulation-derived vocabulary can clarify concepts while leaving cross-instrument equivalence unresolved. Two records labelled carbon footprint may differ in product granularity, calculation boundary, measurement method, reference period or verification scope. A shared label is a candidate connection whose conditions require examination. [10,11]

Industrial interoperability research supplies a broader architectural context. Knothe and colleagues extend the Enterprise Interoperability Framework to address Internet of Things and dataspace artifacts and combinations of unified, integrated and federated approaches. This is the Enterprise Interoperability Framework associated with ISO 11354, rather than the similarly abbreviated European public-administration framework. The accessible abstract supports

the stated architectural contribution. It does not establish that arbitrary DPP implementations have exchanged equivalent information successfully. We therefore retain artifact versions, operation, participants, environment and reported result as distinct assessment fields. [12]

RePlanIT demonstrates that product knowledge graphs require evaluation appropriate to their purpose. Kurteva and colleagues report an ICT ontology, a laptop-passport graph, ontology checks, competency questions and end-user evaluation in a procurement setting. Their evaluation also discusses ontology alignment. These prior results preclude a claim that this paper introduces the first DPP knowledge graph. Our atlas has a different object: assertions about regulations, standards and ecosystem activity. Its source traceability does not inherit RePlanIT's application findings; its usefulness requires evaluation on evidence-retrieval and interpretation tasks. [13]

This targeted literature comparison supports positioning, not an exhaustive systematic review. Table 1 records the scope and access limits of selected work. The present atlas describes assertions about regulations, standards and ecosystem activity; it does not claim the first product-passport knowledge graph or inherit the evaluation results of product-level graphs.

The unit of comparison is a product–actor–action–information–condition tuple anchored to a provision or specified operation. Product identifies the covered class and granularity; actor identifies the responsible or participating role; action states what must or can be done; information identifies content or evidence; condition records territorial, temporal, procedural and acceptance limits. Explicit fields allow partial correspondence without asserting legal equivalence. Legal force, applicability, specification maturity, evidence independence and implementation result remain separate variables.

Table 1: Selected related work and the scope of the evidence atlas

Contribution	**Scope / evidence unit**	**Evaluation and mappings**	**Comparison boundary**
Landscape and framework reviews [8, 9]	225-study manufacturing review; separate 32-study framework review.	Taxonomies and design/validation assessment; findings attributed.	Literature-level regulatory context; provision coding unassessed here. Atlas adds claim and release tracing.
ESPR ontology requirements [10]	ESPR-based core-ontology requirements.	Implementation and transformation benchmarks unassessed.	Abstract-level assessment; temporal implementation unassessed.
Semantic and enterprise interoperability [11, 12]	DPP semantics and enterprise architecture.	Semantic and architectural contributions stated; exchange evaluation unassessed.	Abstracts inspected. Architectural connection differs from tested exchange.
RePlanIT [13]	ICT ontology, product graph and procurement case.	Reports competency questions, ontology checks, application evaluation and manual alignment.	Selected publisher sections inspected; temporal improvements identified as future work. Different object from the regulatory atlas.
Credential and provenance foundations [14, 15]	Protected claims, verifier roles and provenance relationships.	Specifications provide concepts and processing boundaries, not a DPP exchange experiment.	Primary texts consulted. Legal acceptance and general conformance not inferred.

Targeted positioning exercise; unassessed features are not presumed absent. Access limits accompany each reference.

2.2 Selection and source access

The study combines a selected scoping evidence atlas, comparative documentary analysis and verification of a research artifact. An initial discovery dossier was assembled before the research protocol was frozen. The protocol formalised subsequent extraction, classification, review limits and release construction; it was not prospectively registered or applied to an exhaustive original search. Consequently, the corpus supports transparent analysis of its included material, but not a claim of comprehensive global coverage or a systematic estimate of the prevalence of DPP requirements. [16]

The original discovery inventory contained 139 candidate sources. Of those, 106 were extracted into the seed and 33 remained pending; six additional source records were introduced during extraction, yielding 112 source records. Pending entries were not adjudicated as irrelevant. These numbers describe extraction from an existing inventory, not a reconstructed systematic-search flow. Subsequent searches should preserve their actual queries, platforms, dates, language restrictions and screening decisions rather than infer those details from the final bibliography. [4]

The basic evidence unit is a qualified assertion about an identified entity. Entities include legal instruments, provisions, requirements, standards, specifications, initiatives, implementations and geographical scopes. Sources are separate records linked to assertions. An assertion records its subject, relationship or literal value, source identifiers, locator, statement, evidence type, review state and limitations. This separates the existence of an entity from the strength of each claim made about it. A reference relationship, an input relationship and a reported test relationship remain different predicates even when they connect the same organisations or artifacts. [4]

Release 0.1.0 contains 203 entities and 224 assertions. Of the entities, 128 are substantive research records; the remainder provide geographic scope, sectors and analytical vocabulary. The release contains seven provision entities and nine requirement entities, so it is not yet a global clause-level crosswalk. Some operative conditions remain in descriptions and scope notes. The EU–China comparison in this paper therefore uses selected functions whose source locators can be stated, and treats unresolved or partly comparable fields explicitly rather than inferring equivalence from those summaries.

Source access is an independent variable. Thirty-two source records are marked opened, 65 dossier-only, four search-snippet and eleven unavailable. Two of the opened records support geographic reference data. An opened catalogue can substantiate a publication status without establishing that the complete normative standard was examined. A dossier-only record preserves a previously captured observation but does not imply a fresh full-text inspection. These distinctions matter most for material legal scope, deadlines, technical clauses and claimed implementation results. Table 2 reports the corpus denominators and review state. [17]

All 224 baseline assertions retain the status machine-assisted unreviewed. Parallel extraction and automated editorial review are not independent human coding. The planned review process prioritises material legal dates, territorial scope, mandatory versus conditional classifications, original-language interpretation and reported interoperability. It also requires a preselected stratified sample of the remaining assertions. The manuscript does not report reviewer agreement, accuracy percentages or adjudicated legal conclusions because those observations have not yet been obtained.

Table 2: Frozen corpus composition and review status

Measure	Count	Interpretation
Entities / substantive records	203 / 128	Includes geography and analytical vocabulary
Sourced assertions	224	Independent qualified human review pending
Source records	112	106 original candidates plus six additions
Source access	32 / 65 / 4 / 11	Opened / dossier-only / snippet / unavailable
Legal provisions / requirements	7 / 9	Not a worldwide clause-level crosswalk
Geographic scopes / country rows	52 / 44	EU joins are not national implementation findings
Qualified exchange claims	1	Externally reported demonstration; not reproduced

Denominators describe dataset release 0.1.0, not worldwide prevalence or the expanded manuscript bibliography. [4, 17]

2.3 Time, geography and manuscript updates

Dates are typed by their meaning. Adoption, publication, entry into force, applicability, technical availability, legal citation and programme milestones are not interchangeable. A conditional requirement retains the triggering act or decision; the dataset does not convert it into a fabricated calendar date. Observation time records when the research process captured a statement and remains distinct from the time at which the underlying rule or specification applies. The initial release preserves dated events and a snapshot of observations, rather than claiming a complete reconstructed legal history. [16]

Geography is similarly qualified. The atlas contains 52 geographic entities, including 44 country rows and global, regional, supranational, subnational and territorial scopes. EU-member-country display joins represent the scope of EU records; they are not independent assessments of national implementation. EU law is not automatically assigned to the EEA, the United Kingdom, Switzerland or the domestic jurisdiction of an exporter. Great Britain and Northern Ireland remain separate scope objects. Global initiatives are not mapped to a country merely because their secretariat or an active participant is located there.

Figure 1 is generated from the frozen geographic view. Direct country coverage takes precedence over an EU-scope-only display join when both exist, so the categories describe the construction of this selected corpus. Grey geography includes countries without a country-level extraction and areas outside the selected review; it does not establish absence of law or activity. The accessible coverage table retains small and territorial scopes that the world geometry cannot adequately represent. The separately versioned ecosystem filter overlay used by the interactive application is not silently treated as scientific evidence in the paper figures. [4, 18]

Version 0.4 adds a dated manuscript supplement rather than changing release 0.1.0. Each added source records its observation date and access limitations. The legal calendar separates binding application dates, indicative adoption targets, conditional dependencies and implementation observations. The CIRPASS-2 report was checked in full against the file checksum published by its repository. A fresh machine-assisted source check is not independent legal review. The landscape map therefore retains the frozen geographic coverage; updated dates appear in Figure 2 and Table 3. [5]

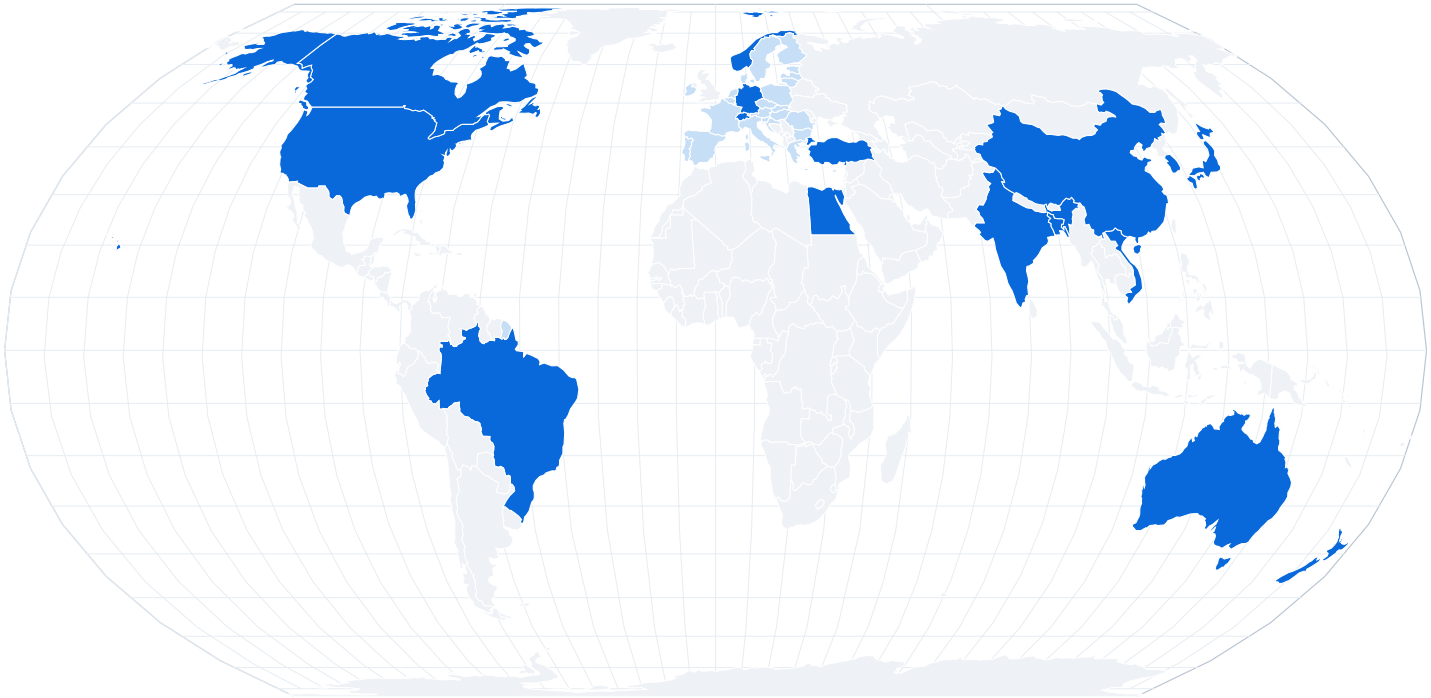
The evidence labels used throughout are documentary finding, completed artifact check, architectural proposition, scenario and planned validation. They describe different kinds of claims,

not a single ranking. A proposal can be well motivated without having measured benefits; a completed software test can pass without validating the interpretation of a legal clause. Stable identifiers, source locators and a release manifest support reconstruction of the research record. The AAS amendment additionally separates formal international-standard status, national adoption projects, standards participation, pilots, production reports and AI evaluation; none serves as a proxy for the others. [6] The four-country follow-up checks the responsible institution, procedural stage, policy or programme scope, implementation unit and reported outcome separately. Memberships, reference-model counts and national-standard status are not converted into deployment counts. The targeted search does not exhaust government procurement, funding awards or commercial installations. [7]

Global DPP landscape: evidence coverage

Selected legal, standards and ecosystem records | Release 0.1.0 | Evidence cut-off: 23 October 2026

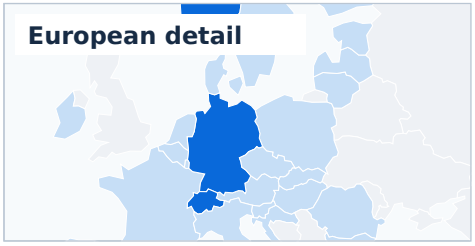
A GEOGRAPHIC COVERAGE



Country-level extraction

- 17 countries with direct records
- 26 countries: EU-scope joins only
- No country-level record / not assessed

44 country rows; 1 has no country-level record.



B TRANSNATIONAL SCOPE

Global standards and ecosystems

W3C DPP & Business Wallet TF
Active task force; vocabulary work evolving.

ISO/IEC JTC 5
Active international DPP committee.

UN Transparency Protocol
0.7.0 maintained pilot release.

Global Battery Alliance
Active battery passport programme.

RAIN-DPP-001
Published non-normative guidance.

European scope

CEN-CENELEC JTC 24
Europe: horizontal DPP standards.

CIRPASS-2
EU: research and implementation pilots.

Examples are not assigned to countries or treated as domestic legal obligations.

Coverage is not a legal-readiness ranking. Small states and territorial scopes require the accompanying table.

Figure 1: Selected DPP evidence coverage in release 0.1.0, 23 October 2026. Of 44 country rows, 42 have geometry; Malta and Singapore remain in the accompanying table. UK data has separate Great Britain and Northern Ireland scopes. Direct records and EU display joins do not establish national legal readiness; grey never means absence of law. Panel B shows transnational examples, not interoperability results. Sources: frozen release and Natural Earth v5.1.2. Human review pending. [18] Map geometry: Natural Earth, public domain; analytical overlay and layout by the author.

3 A global regulatory calendar obligations, proposals and dependencies

3.1 Reading the calendar without creating a universal deadline

DPP regulation develops through instruments that perform different jobs. A framework regulation can authorise later product requirements; a product measure can determine which information must be supplied; a registry measure can organise how a passport is registered. A proposal, a work programme and an operational announcement provide different kinds of evidence. Combining them into a single date labelled "DPP mandatory" would obscure the legal conditions that matter to manufacturers, importers and their customers. The calendar therefore records the instrument, product scope, legal status, relevant event and dependency separately. This approach permits comparisons across jurisdictions without assuming that a digital identifier, a reporting duty and a passport obligation are interchangeable.

Figure 1 remains the geographical view of release 0.1.0, with its 23 October 2026 evidence cutoff. It shows where that dataset contains evidence; it is neither a global legal census nor a ranking of regulatory readiness. Figure 2 supplements the baseline with legal and institutional observations retrieved on 25 October. An event newly identified during that update may itself precede the original cutoff. The distinction between event date and observation date is essential to a reproducible living paper: updating what researchers know must not be represented as a change in the law. The underlying release remains unchanged. [4]

3.2 The EU product sequence fixed obligations and indicative adoption targets

The EU Ecodesign for Sustainable Products Regulation (ESPR) establishes the framework, while product-specific delegated acts define requirements within it. The Commission's adopted 2025–2030 working plan identifies priority products and indicative adoption years: iron and steel in 2026; textiles, aluminium and tyres in 2027; furniture in 2028; and mattresses in 2029. It also schedules horizontal work on repairability and on electrical and electronic equipment. These are planning commitments, not automatically applicable product-passport deadlines. The Commission's sector pages narrow some windows, including the fourth quarter of 2026 for iron and steel and the fourth quarter of 2027 for apparel. They continue to describe future delegated acts. [1, 19] [20, 21]

The legal sequence matters. Adoption is followed by the relevant scrutiny and publication processes, entry into force and application. ESPR Article 4(4) normally provides at least eighteen months between entry into force of a product delegated act and its application, with specified exceptions. Article 72 governs legislative scrutiny. Accordingly, adding eighteen months to an indicative adoption quarter does not produce a binding compliance date. Table 3 separates the event actually scheduled from the product obligation that would follow. It also avoids treating energy-related products as one uniform DPP cohort: transitional measures under the earlier Ecodesign Directive and newer ESPR measures follow different routes. [1]

The Batteries Regulation supplies a contrasting fixed date. From 18 February 2027, Article 77 requires passports for light means of transport batteries, electric-vehicle batteries and industrial batteries with a capacity greater than 2 kWh that are placed on the market or put into service. The capacity threshold qualifies industrial batteries, not the entire list. This fixed passport date should also be distinguished from the dates and conditions governing individual information requirements. For construction products, the relevant passport-system delegated act is a trigger: the system becomes operational six months after its entry into force, while mandatory provision

follows after eighteen months. A Commission target for adopting that act cannot replace those conditional rules. [2, 22]

Table 3: Selected product measures and regulatory milestones, observed 25 October 2026

Product or measure	**Instrument and event**	**Date or planning window**	**Meaning and qualification**
Covered batteries	Regulation 2023/1542, Article 77; passport requirement	18 February 2027	Fixed date: LMT, EV and industrial batteries >2 kWh. Individual information requirements may have separate conditions. [2]
Iron and steel	ESPR product delegated act; adoption target	Q4 2026	Indicative adoption, not application. Final act and transition determine obligations. [19, 20]
Textiles and apparel	ESPR product delegated act; adoption target	2027; sector page Q4	Indicative; the wider timeline gives Q3–Q4. Scope and application remain dependent on the final act. [21]
Aluminium	ESPR product delegated act; adoption target	2027; indicative Q3–Q4	No fixed DPP application date established by the work plan. [19, 23]
Tyres	ESPR product delegated act; adoption target	2027; indicative Q3–Q4	No fixed DPP application date established by the work plan. [19, 23]
Furniture	ESPR product delegated act; adoption target	2028	Year denotes planned adoption, not a universal passport deadline. [19]
Mattresses	ESPR product delegated act; adoption target	2029	Outside the paper's twenty-four-month horizon. [19]
Horizontal repairability	ESPR horizontal measure; adoption target	2027	Includes repairability scoring work; product scope and requirements depend on the measure. [19]
Electrical and electronic equipment	Horizontal recycled-content and recyclability measure	2029 adoption target	Distinct from individual energy-related-product measures and their transitional routes. [19]
Construction products	Regulation 2024/3110; passport-system delegated act	Indicative Q2 2027 adoption	System operational six months, mandatory provision eighteen months, after the relevant act enters into force. [22, 23]
DPP service providers	ESPR service-provider requirements; delegated-act planning	2027; quarter unresolved	Commission materials give Q2/Q3 windows. These are inconsistent planning indications, not a verified adoption or application date. [23]
Machinery	Regulation 2023/1230; main application	20 January 2027	Adjacent safety regime; earlier provisions apply separately. This is not a DPP date. [24]

Continued on next page

Table 3 continued

Product or measure	Instrument and event	Date or planning window	Meaning and qualification
Products with digital elements	Cyber Resilience Act; main application	11 December 2027	Manufacturer reporting began 11 September 2026. Actor-specific exceptions matter; this is not a DPP date. [25, 26]

Selected comparison, not an exhaustive calendar. A target for adopting a delegated act is not a legal application date. Figure 2 uses the 25 October supplementary observation; Figure 1 remains release 0.1.0. No adopted steel product act was identified in the targeted official-source check.

3.3 Global comparison and adjacent connected-product duties

Outside the EU, the baseline contains pathways whose legal objects differ. China's power-battery measures combine identification, traceability and information responsibilities within a recycling and resource-management regime. India's Battery Pack Aadhaar document is recorded as a draft rather than an enacted passport mandate. Vietnamese sources connect product quality, digital information and traceability, but their effects require attention to implementing instruments and product scope. These examples justify function-by-function comparison, not a claim that every jurisdiction is adopting the EU model. Their inclusion here preserves the baseline's access qualifications, including machine-assisted interpretation of Chinese material and incomplete direct access to some Indian and Vietnamese legal documents. This update does not claim an exhaustive new legal review of those jurisdictions. [27, 28] [29, 30]

The EU–China battery comparison makes the functional difference concrete. China's Order 73, effective 1 April 2026, requires unique coding and marking and lifecycle reporting to a national traceability framework. Its Article 12 establishes a digital-identity system while reserving detailed measures for separate provisions. EU Article 77 instead directly specifies an electronic battery-passport obligation for defined battery categories from its application date. Both approaches address continuity of identity and lifecycle information, but comparable functions do not establish equivalent access rights, information models or evidence requirements. The reviewed Chinese material does not establish that a complete EU-equivalent passport service was operational on the order's effective date. This is a qualified legal comparison, separate from the Japan–Catena-X reported exchange examined in Section 8. [2, 27]

Two adjacent EU instruments deserve a distinct watchlist because connected machinery and software-dependent products may carry several obligations at once. The Machinery Regulation's main application date is 20 January 2027. The Cyber Resilience Act's main obligations apply from 11 December 2027, while relevant manufacturer reporting obligations began on 11 September 2026; reporting arrangements for open-source software stewards have a different timetable. These dates concern machinery safety and cybersecurity. They are not additional DPP mandates. Their analytical relevance is the possible reuse of identifiers, organisational authority and evidence across compliance processes, which requires separate legal and technical assessment. [24, 25] [26]

Measured from 25 October 2026, the six-month horizon ends on 25 April 2027 and includes the fixed machinery and battery dates. The twelve-month horizon ends on 25 October 2027: it covers several planned preparatory and delegated-act milestones, but not the entirety of a fourth-quarter adoption window. The twenty-four-month horizon ends on 25 October 2028 and includes the CRA's main application date and part of the furniture planning year. Mattresses and the 2029 horizontal electrical-equipment measure fall outside it. These horizons organise observation and preparation; they predict neither adoption nor successful implementation. Future releases

should record an enacted measure, a postponed target or a verified service independently rather than advancing all related records together. [23]

A calendar of different legal events

Selected EU milestones | supplementary observation: 25 October 2026

REGISTRY AND PASSPORT | fixed date or dated announcement	
19 Jul 2026	**EU registry: statutory deadline** Deadline to establish the registry; not a service-completeness result.
20 Jul 2026	**Registry availability announced** Operational announcement; no live registration test in this paper.
18 Feb 2027	**Covered battery passports: application** LMT and EV batteries; industrial batteries above 2 kWh.

ADJACENT PRODUCT REGIMES | these are not DPP mandates	
20 Jan 2027	**Machinery Regulation: main application** Safety obligations; earlier provisions apply separately.
11 Dec 2027	**Cyber Resilience Act: main application** Manufacturer reporting began 11 September 2026.

ESPR PRODUCT MEASURES | indicative adoption targets	
Q4 2026	**Iron and steel** Planned delegated act; no final act identified in targeted review.
Q3-Q4 2027	**Aluminium and tyres** Planning window; final act determines application.
Q4 2027	**Textiles and apparel** Sector-page target; broader timeline also gives Q3-Q4.
2028 / 2029	**Furniture / mattresses** Planned adoption years, not passport application dates.

Adoption target is not an application date.

ESPR product acts normally allow at least 18 months from entry into force to application, with exceptions. Do not add 18 months to a planning target.

Figure 2: Selected EU milestones, observed 25 October 2026. Fixed legal dates, the registry announcement and indicative product-act adoption targets are separate event types. The battery scope is light means of transport (LMT), electric-vehicle (EV), and industrial batteries above 2 kWh. Machinery and cybersecurity dates are adjacent obligations, not DPP mandates. Adoption, entry into force and application are distinct; indicative quarters cannot establish binding compliance dates. The registry announcement does not prove all functions were operational. Source access and legal-review limits are retained in the dated supplement. [1, 31] [2, 19] [20, 21] [23, 24] [25, 26]

4 The European Product Act an evolving legislative package

4.1 A package name is not a single enacted passport obligation

The term European Product Act describes a wider reform agenda and should not be used as shorthand for a newly enacted, universal DPP law. The European Parliamentary Research Service's June 2026 briefing situated the initiative around three connected tracks: the New Legislative Framework for products, market surveillance and European standardisation. Those tracks address how requirements are organised, how compliance is supervised and how technical specifications support legislation. They provide institutional context for DPP implementation, but the briefing is preparatory analysis rather than evidence that a particular obligation has entered into force. [32]

By the observation date, the standardisation track had reached a distinct procedural stage. The Commission adopted COM(2026)780 final on 6 October 2026, proposing a regulation on European standardisation that would repeal Regulation (EU) No 1025/2012. EUR-Lex identifies procedure 2026/0307/COD; the European Parliament's Legislative Observatory records a preparatory phase in Parliament. This is a Commission legislative proposal under the ordinary legislative procedure, not an adopted replacement regulation. The Commission's implementation tracker separately identifies the standardisation update as proposed while continuing to list the product-framework and market-surveillance reforms as planned. Its earlier third-quarter target should not be mistaken for proof that those proposals were adopted. [33, 34] [35]

This correction illustrates why the knowledge graph needs both a package entity and separate instrument entities. A single package-level status would conceal progress in one track and uncertainty in another. Each component needs a dated procedure record, a relationship to the instruments it would amend or replace, and a distinction between proposed and applicable provisions. The standardisation proposal's identification here is a new research observation on 25 October of an event on 6 October. It must not be presented as a legal change that occurred after the frozen dataset's 23 October cutoff. The primary procedural record supports the status statement; this paper does not claim a comprehensive clause-by-clause assessment of the proposal.

4.2 Implications for convergence, with the evidentiary boundary intact

The package matters to the research question because interoperability depends partly on institutions that determine which technical rules and evidence are accepted. A shared term in two data models establishes a possible semantic correspondence. Successful transfer establishes that specified systems can exchange something under specified conditions. Regulatory acceptance is a further question: whether a competent actor can rely on that information for the relevant obligation. Product-framework and market-surveillance reforms may affect this third layer, while standardisation reform may affect the production and use of technical specifications. The existence of a proposal, however, establishes none of those outcomes by itself.

For the same reason, publication of a European standard, citation of its reference in the Official Journal and use of an implementation that conforms to it must remain separate events. The legal consequences of citation depend on the applicable legislation and the scope of the reference. A proposed change to standardisation governance does not itself demonstrate interoperability between a battery system, an apparel passport and an industrial asset representation. That would require inspectable mappings, versioned test materials, identity and authority checks, and evidence of how the receiving organisation treats the result. The relevant question is therefore

not whether the package contains the word digital, but whether its eventual provisions alter a demonstrable step in this chain.

The paper consequently treats the European Product Act as an institutional development to follow, alongside existing enacted DPP provisions. Its future relevance can be assessed through explicit observations: publication of the remaining proposals, changes to the standardisation proposal during negotiation, final enactment and application, and the appearance of sector requirements or implementation evidence that rely on them. None is assumed in the current findings. This keeps the discussion useful to readers planning systems while preserving the distinction between a plausible route towards convergence and a convergence outcome already established.

5 Standards connections and candidate interoperability mechanisms

5.1 Identification, carriers and resolution

A passport must be associated with the intended product before its information can be interpreted. Assigning an identifier, encoding it on a carrier, resolving it to a service and obtaining a permitted representation nevertheless remain different functions. GS1 Digital Link URI Syntax 1.7.0 addresses web representation of GS1 identifiers; resolution is specified separately. European horizontal standards distinguish identifiers from carriers. RAIN-DPP-001 version 1.0 provides guidance for representing EN 18219 identifier schemes on RAIN RFID, rather than creating another legal passport duty. [36, 37] [38, 39]

This division permits modular integration but constrains what can be inferred from a scan. Reading the same identifier through different carriers does not establish agreement about product granularity, measurement methods or permissions in the resolved payloads. A test must specify the operation: identifying a model differs from retrieving an individual battery's history. Carrier compatibility may be necessary for that operation while remaining insufficient for its regulatory use. A connection at one layer must not be promoted into an end-to-end result.

5.2 Semantics, profiles and industrial information models

Semantic correspondence requires more than matching field names. Carbon-footprint values become comparable only when their product reference, unit, boundary, method and temporal context are understood. These are analytical criteria here, rather than measurements of ecosystem performance. UNTP separates product information from its credential envelope and supports links to criteria and assessment evidence. Its documentation distinguishes the maintained 0.7.0 pilot release from working 0.8.0 schemas described as candidates for a future stable release. An unversioned reference to UNTP is consequently insufficient to identify the artifact used in a transformation. [40, 41]

CIRPASS-2's ontology documentation combines a cross-sector core with extensions and separates vocabularies from profiles and validation shapes. Its exploratory, non-normative status matters: it is not an official EU ontology and does not make a data model legally mandatory. CIRPASS-2 also lists AAS/RDF interoperability work and a reference architecture. The full AAS/RDF white paper and a separate representation benchmark are analysed in Section 5.6. Their reported conversions and experiments were not reproduced by this study. Repository-version labels and report-version identifiers are recorded separately because they identify different revision histories. [42, 43] [44]

The Asset Administration Shell contributes an industrial representation framework through IEC 63278-1 and IDTA specifications. DPP4.0 connects that framework with passport use cases; it does not make the entire AAS stack a complete regulatory content model. Catena-X CX-0143 specifies ecosystem roles and passport components, while EPCIS supplies an event-exchange foundation. These artifacts can support complementary functions without being substitutes. A correspondence claim must identify the submodel, event or requirement being mapped and the information lost or added. No comparative transformation benchmark was executed for release 0.1.0. [45, 46] [47, 48]

The practical implication is that vocabulary reuse and profile conformance need separate evidence. Two profiles can reuse a term while requiring different cardinalities or permitting different measurement methods. Conversely, different terms can express compatible information when a documented transformation preserves the distinctions needed by the recipient. The study therefore records intended alignment, reuse and reported exchange as different relationships. Establishing exact, partial or lossy correspondence remains a future empirical task, with versions and test fixtures fixed before evaluation.

5.3 Evidence, assurance and provenance

Sustainability claims should remain distinguishable from their supporting evidence. UNTP separates product information, conformity credentials, facility information and traceability events, enabling questions about who asserts and who assesses a claim. The Global Battery Alliance's 2026 trials provide a sectoral example involving decentralised exchange, assurance and prototype certification. Developmental methodologies and a planned certification launch should not be represented as universal regulatory acceptance. The atlas records these trial descriptions as ecosystem evidence; it does not reproduce their assessment procedures or establish equivalent outcomes across participants. [49, 50]

The relevant question is whether a recipient can use the evidence under a specified policy. An accessible assessment can concern the wrong product, period or criterion. Conversely, confidential documentation may support an accepted conclusion through an agreed assurance process without becoming public. Evidence scope, issuer, method and access therefore need separate representation. BatteryPass-Ready's updates illustrate executable checks for selected lifecycle APIs and profiles, but success against a particular suite would establish only the conditions that suite covers. It would not alone establish compliance with every applicable law. [51]

5.4 Business identity, delegated authority and access

Verifiable Credentials Data Model 2.0 supplies a published W3C foundation for expressing credentials and verification relationships. Its distinction between verification and reliance is central: proof integrity does not establish the truth or sufficiency of every claim. Business identity, authority to act, delegated scope and the recipient's acceptance policy remain separate questions. An authenticated connection cannot by itself establish an organisation's competence to assess a product or a representative's authority to disclose restricted information. [14]

The W3C VC DPP & Business Wallet task force sits within the Verifiable Credentials Working Group. The charter for 11 March 2026 to 31 March 2028 identifies DPP and business-wallet vocabularies as tentative deliverables, with CIRPASS-2 and UNTP product work and WE BUILD and UNTP identity work as inputs. Work must satisfy the charter conditions before becoming a normative deliverable. The repository and use-case documents remain work in progress;

the latter explicitly disclaims formal Working Group review and endorsement. These activities document coordination, not completed interoperability. Section 7 develops the operational implications. [52, 53] [54, 55]

WE BUILD's blueprint includes DPP and backend-to-backend scenarios. UNTP's Digital Identity Anchor connects a digital identifier with a registered identity. Their pilot and evolving specification status limits what can be inferred about deployment. Neither makes a business wallet universally mandatory for passports. Credential arrangements should be compared with registries, signed documents or APIs under the same acceptance policy. Recognized Entities is considered separately in Section 7.4. [56, 57]

5.5 Publication, legal citation and institutional routes

Standardisation status cannot be collapsed into technical capability. At the 23 October baseline cut-off, the dossier records eight published CEN-CENELEC horizontal DPP standards and six references cited in the EU Official Journal. EN 18239 and EN 18246 had been published, while citation remained pending. Publication, national adoption, OJ citation and product-obligation applicability are different events. The presumption associated with cited standards concerns covered requirements, rather than general certification of product compliance. Catalogue and register evidence supports these status distinctions; clause-level compatibility analysis still requires the normative texts. [58, 59] [60, 61] [62]

ISO/IEC AWI 25534-1 and 25534-2 were approved projects at stage 10.99, not published International Standards. China's project 20251568-T-469 was a recommended national-standard project under development, distinct from operative battery measures. Committees, related scopes and common terminology demonstrate organised work on similar problems; they do not establish equivalence among clauses or implementations. For the standards comparison, the corpus supports identifiable connections and candidate mechanisms across functions. It does not establish quantified semantic convergence, a completed universal profile, or the sufficiency of one standards ecosystem for every jurisdiction. [63, 64] [65]

Ecosystem filters should preserve both institutional scope and technical role. CEN-CENELEC JTC 24 develops the European horizontal DPP framework; ISO/IEC JTC 5 is the international DPP committee announced by DIN and DKE on 20 April 2026, with initial results expected from 2028. The committee prefix matters: these are complementary institutional routes, not interchangeable designations or evidence of completed harmonisation. National committees, W3C working groups, industrial AAS communities, UNTP, CIRPASS-2, GBA and RAIN also have different roles. AAS has a strong German industrial context but an international IEC standard; W3C work is globally scoped. A country label should never imply that a standard applies only in that country. [66, 67] [45]

5.6 What the two AAS RDF papers establish

Grimm and colleagues identify practical shortcomings in the RDF representation of AAS, including string-valued references, indirect graph paths, fragmented predicates and handling of ordered values. Their proposed policies preserve the AAS metamodel while improving its RDF representation through resource identifiers, direct links, stable namespaces and native RDF facilities. They write that "high structural complexity makes it more difficult for developers, or even AI agents, to formulate and maintain queries correctly" (PDF p. 9). This is a motivation for their work; the experiment does not measure AI-agent query accuracy. The supplied manuscript is accepted for SemIIM/ISWC 2026, scheduled for 26 October, rather than a published journal article or an officially adopted AAS revision. [68]

Quotation reproduced unchanged from Grimm et al., PDF p. 9; © 2026 the authors, CC BY 4.0. https://creativecommons.org/licenses/by/4.0/

Their benchmark uses more than 20,000 synthetic AAS instances, three SPARQL queries and three stores. Linked triple-pattern counts fall from 11 to 7, 11 to 8 and 20 to 10, while the graph grows from 2,003,324 to 2,374,037 triples, about 18.5%. Reported mean latency improves across the nine query/store combinations; the largest QLever improvement is partly sensitive to query-optimizer behaviour. A separate SEW case reports one query falling from 266 to 41 ms over 1.1 million assets and 703 million triples. That case adds application-specific links and flattened paths, so its gain cannot be attributed solely to the generic proposal. Table 4 retains the distinct evaluation boundaries. [68]

Bernier and colleagues' AAS/RDF Interoperability Approaches for DPP brings together contributions from 17 projects and 32 researchers. It describes AAS-to-RDF, RDF-to-AAS and bidirectional approaches and recommends clearer transformation profiles, resolvable semantics and expected round-trip behaviour. Its discussion states: "This distinction motivates further work to layer domain-specific modeling on top of this foundational representation" (p. 17). Representing the AAS metamodel in RDF therefore needs to be distinguished from expressing the industrial meaning of the data. The report also includes an AAS-for-Everything proposal, which is a legitimate architectural alternative to evaluate alongside the adapter approach advanced here. [69]

Quotation reproduced unchanged from Bernier et al., p. 17; © 2026 the authors, CC BY 4.0. https://creativecommons.org/licenses/by/4.0/

The second report documents existing official RDF vocabulary and SHACL support, together with conversion tools. It would be incorrect to claim that AAS has no semantic validation or that all conversion work remains hypothetical. The unresolved issue is whether a specified profile preserves the required meaning, ordering, identifiers and evidence across versions and independent implementations. The improved-representation repository separately identifies its proposed branch as unofficial; AAS adoption does not establish adoption of that branch. Neither paper supplies a representative international adoption study or an end-to-end AI-assurance benchmark. Their contribution is a useful experimental foundation and a concrete improvement agenda. [69, 70]

Table 4: Evidence and limits of the two AAS RDF papers

Source and object	Reported evidence	What remains unestablished
Grimm et al. Improved RDF representation Accepted workshop manuscript [68]	More than 20,000 synthetic AASs; three queries in three stores. Pattern counts: 11→7, 11→8, 20→10; triples increase 18.5%.	No measured AI accuracy, full lifecycle test or geographic adoption study. Query latency depends on workload and optimizer.
Grimm et al. Separate SEW industrial case [68]	1.1 million assets; 703 million triples. One query: 266→41 ms; patterns 15→6.	Application-specific shortcuts also contribute. This is not an independent benchmark of the generic profile or proof of global adoption.
Bernier et al. AAS/RDF interoperability white paper [69]	17 projects; 32 researchers; conversion approaches, examples and recommendations. Attached revision history reaches v1.3.	No comparative AI benchmark or representative adoption survey. Project progress is not an interoperability success rate.

Author-reported results; not reproduced here. The papers support constructive integration work and distinct research questions. The first manuscript's workshop is scheduled for 26 October 2026; the second is a collaborative white paper, not a normative standard.

5.7 International commitment and adoption in four distinct cases

AAS is formally international: IEC published IEC 63278-1:2023 on 14 December 2023. Its wider acceptance nevertheless requires separate assessment of standardisation commitment, public implementation support and sustained use. A national standard can exist without widespread deployment; a publicly supported prototype can have strategic relevance without establishing a national technology choice. Table 5 compares the institutional evidence for four jurisdictions. These are selected observations, not country rankings or estimates of market share. [45]

China has an assigned recommended national-standard project, 20243452-T-604, established on 3 December 2024 and listed as under approval at observation. It targets identical adoption of IEC 63278-1:2023. The record names TC124 and participants from domestic research, universities and industry, alongside Chinese operations of international suppliers. A university participant reports that SAC/TC124/SWG2 was established on 20–21 March 2025 with a remit spanning AAS structure, metamodel, cybersecurity, modelling examples and interfaces. This is organised standardisation work rather than an informal suggestion. Drafting participation is still not a count of adopters. [71, 72]

The Chinese policy context is also substantive but bounded. The national smart-manufacturing standards guide, issued on 7 March 2025, includes administration shells among development priorities for sensing and control equipment. It separately advances industrial AI, knowledge graphs, digital twins, cloud and edge systems. The relevant passage does not name IEC 63278 or select AAS as a universal model. We interpret the guide as policy support for a related field within a broad standards portfolio, not as an AAS rollout mandate or evidence of privileged architectural status. [73]

Completion is not guaranteed. Chinese rules allow standards plans to be adjusted or terminated; a project listing should therefore not be treated as an accomplished national adoption. However, no project-specific withdrawal or termination was found in this review, and the inspected status remains under approval. The specified 16-month development cycle runs to submission for approval, not to final publication. Its elapsed duration alone does not demonstrate delay or abandonment. The distinction is between genuine procedural uncertainty and an observed failure, for which this review found no evidence. [74, 75] [71]

The United States shows selective institutional cooperation. The CESMII/LNI report released on 22 April 2024 describes two prototypes linking AAS and Smart Manufacturing Profiles, records Microsoft and GE Digital participation, and identifies Catena-X as a contributor specifically to the battery demonstrator. The report frames DPP work partly around Europe-facing supply chains. This is meaningful technical engagement; it does not establish broad US production use. CESMII is a federally supported national institute: DOE renewed its support on 15 September 2023, but that announcement does not identify AAS-specific spending or select AAS as a national architecture. NIST's manufacturing digital-twin programme also pursues ISO 23247 reference implementations and an MTConnect laboratory interface. These technologies address partly complementary layers. Their coexistence supports a plural standards landscape, not an inference of AAS rejection. [76, 77] [78]

Japan has sustained technical participation. JEMIMA's July 2024 national-committee account describes Japanese contributions to IEC 63278-1 alongside German and French experts. RRI has also organised Japanese-language dissemination covering AAS, semantics, industrial AI and dataspaces. These sources establish institutional knowledge; they do not measure how widely AAS is known or used across Japanese industry. A corresponding JIS adoption was not established by the targeted search. The government-supported Japan–Catena-X demonstration discussed in Section 8 deliberately preserved different architectures through an intermediate

conversion layer. It demonstrates a bounded exchange, not selection of AAS as Japan's domestic information backbone. [79, 80] [81]

South Korea provides direct evidence of formal national adoption and public implementation support. KS X IEC 63278-1 was published on 31 July 2025 as an identical adoption of IEC 63278-1:2023. The Ministry of SMEs and Startups' call of 6 April 2026 supports AAS reference-model development. TIPA reported on 1 July 2026 that 50 models had been developed in 2024 and 115 in 2025; 335 additional models were targeted for 2026, giving a cumulative year-end goal of 500. Those are equipment or process templates, not factories. The programme includes validation and demonstrations and is explicitly linked to prospective manufacturing AI applications. It constitutes public support beyond an isolated pilot, while neither template utilisation nor measured AI benefit is established here. [82, 83] [84]

Catena-X is one channel of international influence, not a sufficient explanation for every activity. Its role is explicit in the US battery demonstrator and the Japanese interconnection project. South Korea's government described cooperation with Catena-X and Manufacturing-X when launching its bilateral dataspace forum on 14 October 2024, while envisaging a Korean platform suited to domestic circumstances. Such links can promote compatible interfaces without requiring all internal systems to use AAS. The sources do not establish that China's national project or all US, Japanese and Korean engagement is driven by Catena-X. [76, 81] [85]

The defensible conclusion is selective but institutionally meaningful international commitment, with uneven and incomplete evidence of production reach. A blanket description of the four cases as isolated experiments understates the Chinese standards work and Korean programme. Conversely, these observations do not establish broad uptake across all four ecosystems. No representative denominator for awareness, independent production sites or installed-base share was obtained. None of this evidence establishes adoption of the proposed improved RDF profile specifically, or successful AI assurance. Those are separate empirical questions.

Table 5: Institutional commitment and deployment evidence for AAS

Jurisdiction	**Documented commitment**	**Boundary of the evidence**
China	Recommended national project under approval; dedicated standards working group. Administration shells appear in a broader manufacturing-standards guide. [71, 72] [73]	Formal standardisation with bounded policy relevance. Publication, a national rollout and widespread production adoption are not established; termination is possible but not observed.
United States	CESMII/LNI prototypes and architecture integration; federal support for CESMII as an institute. NIST pursues additional, partly complementary standards. [76, 77] [78]	Selective institutional engagement. Institute funding does not measure AAS investment; prototype participation does not establish federal architecture selection or production prevalence.
Japan	IEC co-development and RRI dissemination. Government-supported Catena-X exchange preserves different architectures. [79, 80] [81]	Organised participation and a bounded exchange. JIS adoption was not verified in this review; domestic AAS penetration and wholesale architectural adoption remain unmeasured.

Continued on next page

Table 5 continued

Jurisdiction	Documented commitment	Boundary of the evidence
South Korea	National standard adopted 31 July 2025; MSS/TIPA reference-model programme, validation and demonstrations. [82, 83] [84]	National adoption and programme support. Reported prior-year models and the 500-model target are templates, not factory counts; sustained uptake and AI gains require evaluation.

Observed 25 October 2026. The categories distinguish commitment from reach; they do not assign an adoption score. Participant reports, programme announcements and catalogues retain their access and verification limits. None verifies uptake of the improved RDF profile.

5.8 AAS as an initial experimental infrastructure

For organisations with asset models and relevant toolchains, AAS is a credible first experimental infrastructure for DPP integration. Asset identities, modular submodels and existing interfaces provide concrete objects around which partners can test information exchange. The SEW case also shows that its role is not confined to laboratory demonstrations. Our recommendation concerns the first stage of a broader evidence architecture: keep useful operational AAS representations, publish a versioned semantic projection where needed, and connect it to product claims, domain concepts and assurance evidence. This is an architectural recommendation, not a finding that one representation is sufficient for every sector. [68, 69]

Expectations should be defined by acceptance tests. A receiving system should be able to identify the applicable product configuration, interpret the measurement and method, follow its provenance, check current issuer and evidence status, and enforce the permitted use. Export and migration paths must preserve these properties when an AAS server, graph store or AI interface changes. Stable identifiers, documented mappings and policy enforcement are therefore more consequential than selecting a serialization alone. AAS, RDF and JSON-LD each need engineering and governance; none independently supplies truth, authority or safe action. Section 11 specifies the comparison needed before stronger AI-readiness claims.

6 The EU registry, shared semantics and a prospective lean dataspace

6.1 What the registry does, and what its dates establish

The EU registry is a concrete point at which the paper's three concerns—shared semantics, verifiable evidence and business identity—meet. It is also a useful test of disciplined claims. ESPR Article 13 required the Commission to set up the registry by 19 July 2026. The Commission announced its availability on 20 July. Implementing Regulation (EU) 2026/1778 was adopted on 16 July, published on 17 July and, under its twenty-day entry-into-force rule, entered into force on 6 August. These dates describe a statutory deadline, a public announcement and the commencement of an implementing instrument. Their sequence alone proves neither a breach of the deadline nor completion of every operational function. [1, 86] [31]

The public Commission page presents an index for passports, organisation enrolment and a separate testing environment. It explains that detailed passport information remains with economic operators or their service providers. The registry holds identifiers, registration information and high-level metadata, with additional information dependent on the applicable legislation. It also describes a technical component containing models, structures and semantic definitions.

Thus, the registry is more than a directory of web addresses, but it is not described as a central repository of all product information. This paper inspected those public descriptions and links; it did not authenticate, register a passport or execute an API test. [87]

The implementing rules connect registration with semantic checks and specified registration-event records. They also establish a semantic repository containing product models, definitions, vocabularies, roles and model metadata, with public search and interfaces. Article 12 includes links between passport attributes and supporting evidence, and applies DCAT-AP to model metadata. That requirement should not be expanded into a claim that every passport field must use DCAT-AP. Nor does a statutory model repository imply that operators can register arbitrary private schemas or that every product model is already available. [86]

6.2 An operational qualification that changes the interpretation of launch

The Commission page links a user guide labelled version 1.03 and dated 16 September 2026. Its battery-registration instructions state that successful registration is unavailable while the relevant semantic catalogue or content remains under development; the validation-error section also identifies unavailable semantic validation. This is a dated documentary observation, not a live-system finding for 25 October. The guide may lag deployment. Nevertheless, its qualification prevents the launch announcement alone from supporting a claim of verified, complete battery-passport registration. An updated official account or a documented successful transaction would be needed to resolve that uncertainty. [88]

The distinction is substantive. An organisation may be able to establish an account before a product-specific model is finalised. An interface may accept a request before all required validation is available. A semantic repository may have a legal basis before its full contents are published. These are different implementation states, each with a different evidentiary burden. Treating "registry live" as a single maturity score would hide exactly the dependencies that the research question seeks to explain. The defensible observation is that public infrastructure and enrolment are offered, the legal architecture includes semantic validation, and the inspected guide records a product-specific limitation whose subsequent resolution was not independently tested.

6.3 Identity, registration evidence and the limits of a successful check

The registry's legal architecture also distinguishes the economic operator, other value-chain actors and authorised representation. Verification and access arrangements support attribution and permitted actions; responsibility does not disappear when a service provider performs a technical step. A proof of registration concerns the registration event. It should not be described as a blanket certificate that every underlying sustainability claim is true. The study must therefore identify what a proof establishes, who supplied it, which role authorises the action and which further substantive checks are still necessary. [86]

For example, a syntactically valid carbon-footprint value could have an identifiable issuer and an intact digital signature yet still use a calculation method inappropriate to the receiving requirement. Conversely, an independently assessed result may be difficult to reuse if its product reference, unit, reporting period or evidence link cannot be interpreted. These are analytical examples, not observations of a defect in the EU registry. They explain why a useful assessment separates content meaning, evidence integrity and the authority to issue or rely on a statement. A successful check at one layer cannot simply be promoted to a finding at the others.

Table 6 distinguishes the statutory registration record and semantic repository from two dataspace functions: a semantic hub or vocabulary service that maintains models and mappings, and a catalogue that makes data and service offerings discoverable. DSSC's blueprint describes the latter functions separately. A semantic asset explains meaning; a catalogue entry helps locate an offering. Neither by itself grants access or establishes legal acceptance. The proposed DPP arrangement would link these functions to authoritative EU assets without equating an ecosystem mapping with an official product model. [89]

Table 6: Registration, semantics and discovery: distinct functions and evidence

Function	Object and authority	What it can establish	Boundary
Statutory registry record	Identifiers and registration-event data governed by EU law. [86]	Association with a recorded registration event and its specified data.	Does not establish the truth of every product claim or centralise all passport content.
Statutory semantic repository	Commission-governed models, definitions, vocabularies and metadata; a component of the registry. [86]	An authoritative model against which relevant content can be interpreted and checked.	Legal provision does not prove every model is published or every validation service operational.
Dataspace semantic hub / vocabulary service	Governed models, vocabularies, profiles and mappings. DSSC architectural function. [89]	Helps interpret content and inspect versioned mappings.	Not automatically a source of legally authoritative EU models or recognition.
Dataspace discovery catalogue	Metadata describing data/service offerings and access routes. DSSC architectural function. [89]	Helps users locate relevant resources and declared models.	Discovery does not grant access, verify the content or establish acceptance.

The first two rows are statutory EU registry functions; the latter two are reference-architecture functions. Their integration in Figure 3 is proposed and has not been implemented or tested in this study.

6.4 A lean dataspace as a testable design proposal

Figure 3 develops a prospective architecture, not a diagram of an already integrated service. Here, a lean dataspace means a deliberately limited arrangement for discovering a resource, resolving its identifier, interpreting its declared model, checking relevant evidence and authority, and applying the conditions for access. It does not require centralising every participant's product data. The proposed catalogue would publish enough metadata to locate the appropriate resource and understand its scope. Authoritative registry records and semantic assets would remain identifiable as such; ecosystem mappings would carry their own authorship, versions and limits.

Section 7 specifies the proposed identity and policy connection: business wallets present actor credentials; recognised-entity assertions and identity anchors help evaluate their scope; a data-space service applies a declared policy to the requested evidence. An EU product registry, a semantic catalogue and a registrar directory contribute different information. No single entry in one of them establishes all three of product compliance, issuer competence and access entitlement.

The paper predicts that a lean dataspace will make DPP reuse across sectors and AI applications more economical by reusing discovery, model-governance and actor-status services across several workflows. The comparator is a competent bilateral API arrangement in which each

integration maintains its own discovery records, mappings and status checks. With the same evidence and acceptance policy, the proposed shared services should reduce repeated onboarding and maintenance effort without increasing disclosure, false acceptance or recovery failure. A study should predeclare those measures and thresholds: equal or higher total effort with no compensating control or continuity benefit would count against the prediction. This does not require a particular connector or branded platform. It is a comparative architectural hypothesis, not an ESPR requirement or an observed global outcome.

This design could reduce duplication where several applications need the same declaration or supporting record. The practical promise is that a participant could discover an existing, relevant item of evidence before requesting another copy or new declaration. Yet reuse would remain conditional. Access to metadata does not entail access to confidential evidence, possession of a credential does not establish a legal entitlement, and an identifier resolving today does not guarantee continuity after a provider ceases operating. The prospective design therefore needs explicit handling of authorisation, version change, supersession, revocation and persistence. These are proposed evaluation requirements, not claims that the present sources demonstrate their satisfaction.

A future evaluation should follow one bounded product claim from the applicable requirement through the product model, issuer and supporting evidence to a receiving organisation's decision. It should record the actual versions, the successful and unsuccessful checks, and whether the recipient accepts the information for the stated purpose. Negative cases would include an obsolete model, an unauthorised representative, a changed evidence record and an inaccessible supporting resource. No such experiment was conducted for this paper. Its contribution here is a documented distinction between legal functions, dated operational observations and a falsifiable architectural proposal: convergence is credible only when those layers can be connected with evidence.

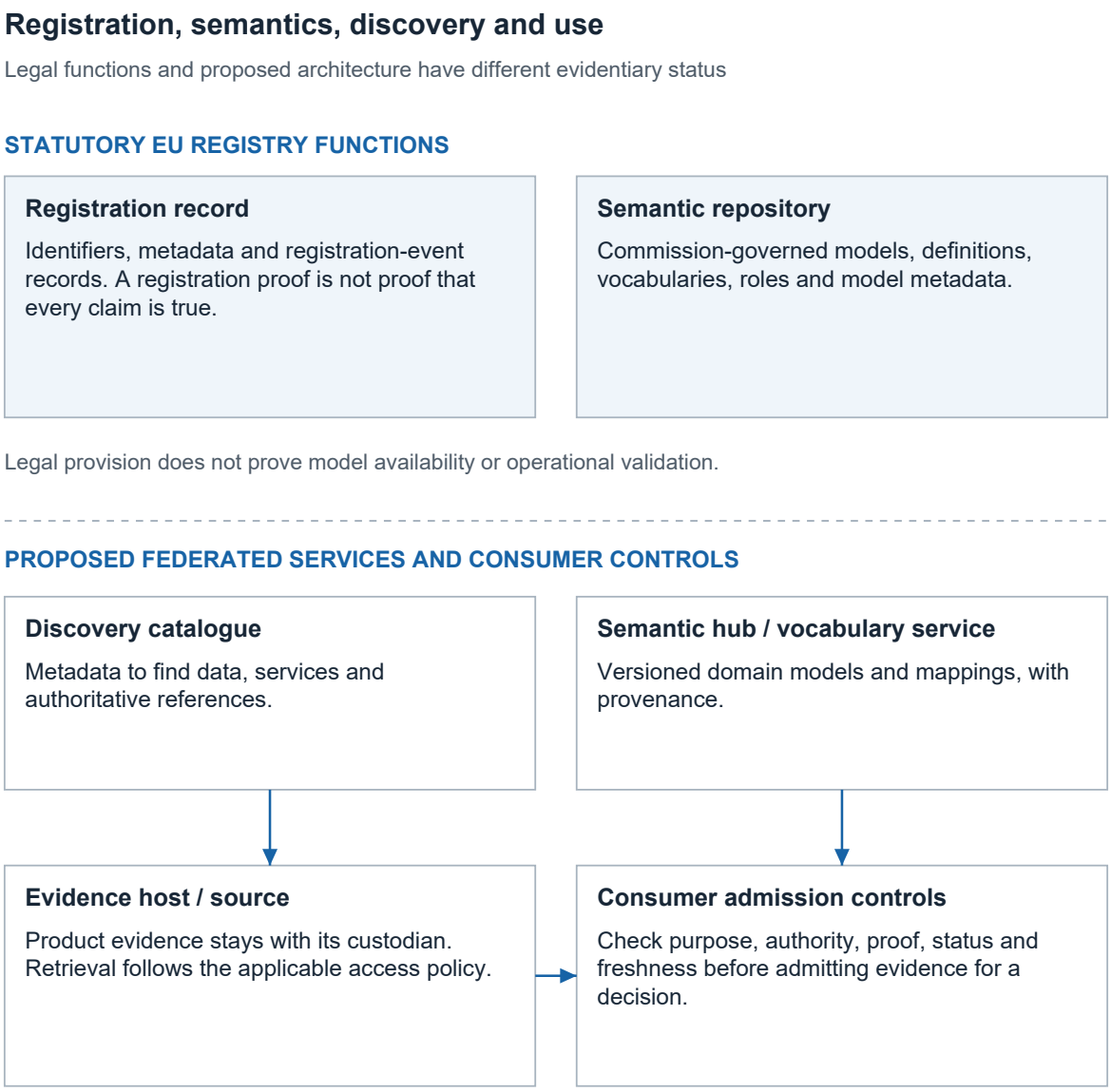


Figure 3: The upper pair represents two statutory functions within the EU registry architecture. The lower services and consumer controls are an author-proposed arrangement, not a required or implemented EU dataspace. A discovery catalogue publishes resource metadata; a semantic hub manages domain models and mappings; neither replaces the statutory semantic repository. Detailed evidence remains with its host. Arrows represent proposed information use, not verified integrations or recognition. The linked registry guide version 1.03 records semantic-validation limitations; this paper did not test whether those limitations persisted at observation. [86, 87] [88, 89]

7 Access control business wallets and verifiable evidence graphs

7.1 What the lifecycle catalogue establishes

Access control is a continuing decision about an actor, action and product context, not a property conferred permanently by issuing a passport. CIRPASS-2 provides a useful primary risk catalogue: its version 1.1 companion to D4.1, submitted and published on 5 June 2026, lists 52 numbered action/risk entries across creation (9), storage (11), retrieval (14), updates (11), and deletion (7). These counts describe the structure of an expert analysis; they are not observed incident frequencies, severity scores or demonstrated mitigation rates. Section 1.1 states that "many risks of abuse of the system cannot feasibly be mitigated using technical means alone" (printed p. 8; PDF p. 10). [90]

Quotation reproduced unchanged from Roefs et al., printed p. 8; © CIRPASS-2 Consortium, 2024–2027, CC BY 4.0. https://creativecommons.org/licenses/by/4.0/

The complete report was inspected for this amendment on 25 October 2026, separately from the frozen atlas. It distinguishes exploitation of technical faults from harmful behaviour possible even when the system operates as intended. Its mitigation catalogue includes proposed measures beyond those adopted in the reference architecture. Consequently, this paper uses it to identify questions and test cases, rather than treating every suggested control as an implemented safeguard or regulatory obligation. Table 7 makes this distinction explicit. [90]

7.2 Identity, authority and action-specific permission

An identity check establishes which account, key or organisation is represented under a specified scheme. Authority asks whether that represented party may perform this operation on this product now. Authentication alone does not establish a manufacturer role, a repair mandate or a recycler entitlement. A policy decision should bind the acting principal, representative or service, product scope, requested operation, purpose, evidence and current status. These are design requirements for the proposed architecture; the applicable law and institutional arrangements determine which roles and evidence are authoritative.

Reading, writing, deriving and acting should therefore be separate permissions. A repairer may read service instructions without seeing supplier prices; it may append a repair event without overwriting the original conformity claim. A permitted analytical service may compute an indicator without acquiring permission to redistribute its inputs. An autonomous agent may recommend a replacement without authority to order it or change the passport. The Spherity two-plane paper supplies this architectural interpretation, not independent confirmation of CIRPASS-2 outcomes. W3C likewise separates credential verification from the verifier's purpose-specific trust decisions. [14, 91]

7.3 W3C and DPP business wallet convergence

A DPP describes a product and its supporting claims; a business wallet can present credentials about the organisation and representative requesting or issuing those claims. Convergence means that these records can be interpreted together for a defined operation. It need not mean storing the entire product history inside a wallet. W3C VC Data Model 2.0, a Recommendation dated 15 May 2025, supplies a common credential model while leaving purpose-specific trust and authorisation to the receiving system. [14] VC Data Model 2.0 expressly requires an accompanying authorisation framework for role- or attribute-based control. [14]

The W3C task force provides a venue for developing compatible product and organisational vocabularies. The parent Working Group's charter names company certificates and powers of attorney among the business-wallet concerns. This gives the paper's proposed connection an institutional basis, but the tentative vocabulary work has not become a finished global wallet-to-passport standard. The charter's interoperability criteria require testing and independent implementations; participation or vocabulary similarity cannot substitute for those results. [52, 53]

UNTP's current Digital Wallets guidance supplies a more explicit architectural connection. It is wallet-agnostic and primarily uses resolver-based discovery of published credentials. Organisational wallets can complement that path by presenting identity, accreditation or role credentials for protected access. The guidance is labelled work in progress and suitable for pre-production pilots. It neither mandates a wallet provider nor converts every product into an active credential holder. Its relevance here is a documented design direction, not evidence of a completed cross-ecosystem deployment. [92]

7.4 Recognized entities and UNTP identity anchors

Who recognises this issuer, for which action and under which scheme? The W3C Recognized Entities v1.0 Working Draft of 6 September 2026 provides a model for communicating such assertions. Its product-conformity example connects an assessment issuer to accreditation information. Recognition is asserted by a credential issuer within an ecosystem; W3C does not thereby approve the company or certify its competence. The draft explicitly describes itself as experimental and unsuitable for production deployment. [93]

UNTP's versioned 0.7.0 Digital Identity Anchor binds a controlled decentralised identifier to an identity known to a registrar. Its requirements include verification of identifier control and a registration scope. The verifier must still accept the registrar and check the relevant scope. A corporate registration can establish a registered business identity without establishing laboratory accreditation or a mandate to update a particular battery record. The live work-in-progress DIA specification now describes DIA as a profile of the Recognized Entities model; the inspected 0.7.0 page does not make that alignment claim. This is documented specification convergence, with different versions and maturity states, rather than proof of legal or operational equivalence. [57, 94]

The developing UN/CEFACT Global Registry Information Directory (GRID) concerns discovery of authoritative registrars, rather than a central store of every company or product record. Its inspected project page is at Stage 5, Deliverable Acceptance Check. The directory's intended role should therefore be distinguished from a verified, universally deployed trust service. [95]

For the proposed evidence graph, a recognition assertion is another attributable, scoped and time-sensitive claim. A receiving organisation would follow the chain from assessment to assessor, recognition issuer and accepted governance rule, then decide whether that chain is sufficient for the requested purpose. Membership, accreditation, legal mutual recognition and access permission should remain distinct relationships. A machine-readable assertion can carry evidence of an existing arrangement; it cannot create that arrangement by itself.

7.5 ODRL policies and enforcement in data spaces

The Open Digital Rights Language (ODRL) Information Model and Vocabulary 2.2 became W3C Recommendations on 15 February 2018. They express permissions, prohibitions and duties concerning assets and actions, with parties and constraints such as time or purpose. A

passport evidence service could identify a restricted assessment as the asset, the provider and requester as parties, and the allowed operation and conditions in a policy. Shared profiles must fix the meaning of domain terms and the interpretation of constraints. ODRL is a policy language, not a credential verifier or an enforcement engine. [96, 97]

Data spaces can provide the surrounding exchange services. Eclipse Dataspace Protocol 2025-1, including errata release 2025-1-err2 of 11 September 2026, combines DCAT-based catalogue discovery and ODRL policy-bearing agreement negotiation with transfer-process coordination. Its authorisation-token semantics are outside the protocol's scope. Decentralized Claims Protocol 1.0.1 supplies a complementary credential-exchange mechanism; it does not itself confer legal recognition. These specifications demonstrate reuse of Web vocabularies across separately governed projects, not one W3C-operated infrastructure. [98, 99]

Eclipse Dataspace Components (EDC) provides an open-source implementation reference for ODRL-based policy evaluation in a connector. Its policy engine maps ODRL policies into an internal model and evaluates constraints through registered functions in defined execution scopes. Rules without a binding to the evaluated scope can be ignored. Implementers must therefore configure and test supported terms, scope bindings, unsupported-term handling and enforcement points. The v0.18.1 release of 25 September 2026 supplies a concrete version for follow-up evaluation. EDC demonstrates an implementation path; this paper does not claim universal ODRL-profile conformance or automatic enforcement of every downstream-use restriction. [100, 101]

Our proposed DPP profile would define product scope, purpose, permitted derivation, onward disclosure, retention and policy expiry, and specify how conflicts and missing evidence are handled. The service would verify the presented credentials, evaluate the policy against current context, and enforce the resulting decision at the resource boundary. A signed policy still requires executable rules and accountable operations. Once information has been disclosed, a usage restriction may require recipient controls, audit and contractual remedies; a policy label cannot prevent copying by itself. These are architectural requirements to test, not outcomes measured in this paper.

UNTP 0.7.0 already distinguishes public access from protected information and describes several authentication arrangements. The inspected access-control specification does not make ODRL mandatory. We propose ODRL as an explicit policy representation for a lean data space when participating implementations agree its profile. Public information should remain available according to its applicable rules; protected business evidence may require additional credentials. Catalogue discovery, semantic interpretation, identity recognition and policy enforcement remain separate functions. [102]

7.6 A common policy layer for B2B and B2G operations

ODRL's use in data spaces makes a common B2B and B2G policy layer a practical starting point. The same information model can describe a supplier's permission to share evidence and a public authority's legally grounded access. Here, universal means a reusable expression framework across domains, with explicit profiles for each operation. It does not mean that every actor acquires the same rights or that one policy engine already interoperates everywhere. ODRL provides read and modify actions; its former write action is deprecated. More precise operations, such as submitting a registry record or recording a verification result, require declared profile terms and agreed semantics. [97, 98]

For EU registration, ESPR Article 13(4) assigns the required registry upload to the economic operator placing the product on the market or putting it into service. Article 11 distinguishes

access rights from rights to introduce, modify or update passport data. Article 13(6) provides access for the Commission, national authorities and customs authorities to perform their duties. Article 15 provides for customs verification of identifiers and commodity codes and retrieval and use of relevant data. These provisions do not give every authority unrestricted permission to rewrite manufacturer claims. A supplier policy cannot override a public authority's lawful statutory access. [1]

A B2G profile should therefore distinguish a registration submission, a market surveillance authority's (MSA's) read operation, and a customs verification operation. A write operation should identify the exact record to be created or updated and the authority competent to do so. For example, the architecture could permit an authority to append its own attributable inspection result while preserving the manufacturer's declaration. That is a proposed operation whose legal basis, schema and responsible system must be established; it is not inferred from a generic authority credential. The EU registry implementing act separately addresses verified operators, roles, delegation and administration of national-authority access. [86]

Registration requirements can be mapped to machine-readable obligations and linked to the governing provision, deadline and proof of submission. Such a representation assists workflow control; it neither creates nor discharges the legal duty by itself. B2B confidentiality and B2G statutory powers may also produce different lawful grounds and conflict rules. An agreed ODRL profile must state how these are evaluated and which service enforces the decision. This allows one policy language to connect both settings while preserving their distinct responsibilities.

7.7 From a wallet presentation to a verifiable evidence graph

Figure 4 brings these relationships together as the paper's proposed integration. Consider an accredited recycler requesting a battery assessment. A product identifier first leads to the passport and available evidence references. UNTP's Identity Resolver locates resources; the client must separately verify their credentials. Where an information view is public, this design introduces no wallet requirement merely to discover it. [103]

For restricted evidence, suppose the recycler's business wallet presents its identity, current qualification and a representative's mandate. The provider checks cryptographic validity and status, accepts the qualification issuer under its governance rules, and matches the mandate to this product and operation. It evaluates an agreed ODRL profile and releases only the authorised evidence. This is an illustrative workflow: the paper has neither built nor independently tested the complete chain. Exact presentation protocols, identity mappings and enforcement behaviour would have to be fixed before an interoperability claim.

The evidence graph would retain the assessment's subject, method, version and provenance, together with references to the recognition evidence and decision record where disclosure and retention rules allow. Confidential credentials need not be copied into a public graph. An AI service using the assessment would require its own permitted purpose and action scope; the recycler's reading permission would not automatically authorise model training, permanent memory or a physical operation. This connects the wallet's actor evidence with the passport's product evidence while keeping their permissions distinct.

A useful experiment would involve two independently implemented wallet and evidence services, with the same declared policy profile. It should accept a correctly scoped request and reject an expired accreditation, revoked mandate, unknown recognition issuer, wrong product, unsupported policy term and unauthorised derived use. Record both false acceptance and unnecessary denial, status-check delay and the evidence retained for review. Passing that experiment would

establish a bounded result; mutual recognition across laws and sectors would require additional agreements and evidence.

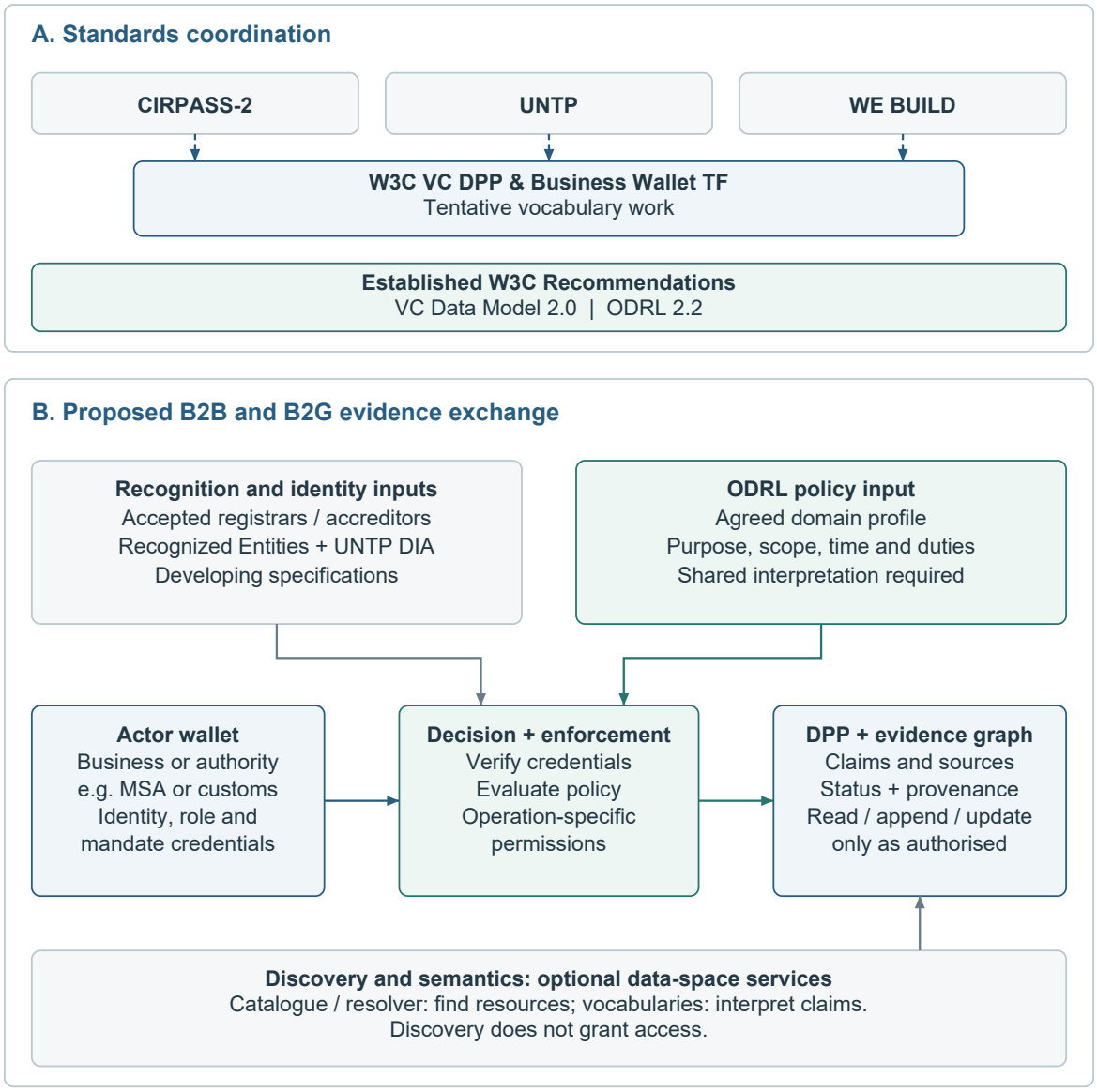


Figure 4: DPP and business-wallet relationships. Top: the W3C charter identifies CIRPASS-2, UNTP and WE BUILD inputs for tentative vocabulary work. Bottom: the author's proposed composition of actor credentials, scoped recognition, policy enforcement and product evidence. Recognized Entities and the aligned UNTP work-in-progress DIA remain developing specifications; ODRL and VC Data Model 2.0 have Recommendation status. Arrows describe intended information and control relationships, not a demonstrated integrated service or automatic legal recognition. Sources and maturity checked 25 October 2026. [52, 93] [92, 96] [98]

7.8 Authentic provenance can accompany false claims

A valid signature can bind a claim to its signer and expose later alteration; it cannot establish that a measurement was performed correctly or that a reported physical event occurred. CIRPASS-2 distinguishes inaccurate original content (3A), conflicting signed versions in the discussion of 13A, inaccurate updates by entitled actors (35A–36A), and unauthorised updates (38A). These are different failure mechanisms. Rejecting an unknown signer addresses only some of them. [90]

The proposed evidence path retains the originating source, product and measurement context, transformations, versions, responsible actors, and validation results. An update should append an attributable event, preserving superseded information where retention rules permit. Conflicting claims should remain identifiable until an authorised resolution process decides between them. Reviewable provenance supports investigation; it does not turn every documented assertion into a true assertion. Independent inspection, sanctions or accepted assurance procedures may still be needed. Tests should include a correctly signed but factually false statement, not only damaged signatures.

7.9 Confidentiality, status and cached decisions

The risk catalogue treats unauthorised disclosure and abuse of legitimate access separately. Risks 17A–20A address host access, extraction, impersonated entitlement and paid onward disclosure; 31A–34A address strategic inference from aggregated public information. Encryption and minimal disclosure can reduce exposure, but neither erases information already disclosed to an authorised recipient. A publicly retrievable field may become sensitive when linked with many other records. Discovery and indexing choices therefore need their own risk assessment alongside endpoint permissions. [90]

Permission also changes over time. A valid credential may be used outside its intended scope, after a mandate ends, or against an obsolete policy. The discussion of 38A explicitly raises excessive or outdated permissions, infrequent revocation checks, replay and compromised issuing authorities. Our proposed control design records the policy version, status-check time, credential validity and decision expiry. Caches should have documented freshness limits and safe handling of unavailable status services. Emergency suspension and issuer revocation require propagation tests. A cached positive decision must not silently become permanent authority. [90]

7.10 Continuity and the physical product boundary

Lifecycle reliability includes survival of hosts and resolvers, preservation of evidence, and correspondence with the physical product. CIRPASS-2 considers host discontinuity and loss (10A–12A), failed redirection (24A), carrier substitution (15A–16A), and mismatch between physical and recorded changes (40A–45A). For false destruction reports, its discussion of 46A and 49A includes retaining a state marker instead of immediately erasing the passport. Such proposals preserve investigatory evidence but do not prove that recycling occurred. Retention and deletion decisions still require the relevant legal and contractual basis. [90]

A continuity test should restore an independently retained copy, move a resolution service, and verify that identity, permissions and revision history remain coherent. A physical-event test requires evidence outside the digital record, such as an accountable inspection or accepted treatment record. These operations must be evaluated separately: restoring bytes cannot demonstrate product authenticity, and identifying a recycler cannot establish the truth of each

destruction claim. The paper makes no finding that the proposed controls have passed these tests.

7.11 Local context, memory and accountable evaluation

The same boundary applies when a passport feeds local analytical software or an AI assistant. An acquired document can supply evidence without supplying authority to execute its embedded instructions. Permission to retrieve a record should not automatically permit storing it indefinitely, merging it into another organisation's memory, or taking a downstream action. We propose that local context and retained memory inherit source restrictions, provenance and expiry, with renewed checks before reuse. This is an extension of the paper's design, not a risk class claimed to have been evaluated by CIRPASS-2.

The next study should exercise revoked mandates, stale caches, incorrect issuer roles, conflicting signed updates, leaked summaries, and unsupported end-of-life events against a declared policy. It should compare credential-based controls with appropriately authenticated registry or API alternatives under the same expected outcomes. Record false acceptance, false denial, detection delay, recovery behaviour and operator effort. These are planned measurements. Author involvement in the risk work must also remain visible: the report acknowledges Carsten Stöcker's input on authenticity and authorisation, which supports domain familiarity but does not constitute independent validation. [90]

Table 7: Selected lifecycle risks, proposed controls and unresolved tests

Risk and source evidence	Proposed control	Residual limitation	Planned test
False or mis-scoped actor: 6A, 19A, 38A, 49A; pp. 15, 17, 20–21.	Bind organisation, role, mandate, product and action; check current status.	Correct identity need not establish authority; issuer compromise remains possible.	Wrong role; expired mandate; revoked issuer; cross-product replay.
Signed incorrect content or conflicting versions: 3A, 13A, 35A–36A; pp. 14, 16, 19–20.	Preserve sources, signed revisions, independent validation and conflict history.	An attributable, authorised statement can still be false.	Validly signed false measurement; two inconsistent signed revisions.
Confidential-data leakage and public aggregation: 17A–20A, 31A–34A; pp. 17, 19.	Minimise disclosure; separate discovery from access; log purpose-bound decisions.	Legitimate recipients can disclose or infer more; public data cannot be recalled.	Restricted-field retrieval; aggregation inference; onward-sharing scenario.
Stale or replayed permission: residual risks under 38A; p. 20.	Limit validity; refresh status; bind requests to scope and policy version.	Availability and freshness trade off; revocation does not erase prior knowledge.	Revoke during session; replay after cache expiry; status-service outage.
Loss, resolver discontinuity and physical-digital mismatch: 10A–12A, 15A–16A, 24A, 40A–45A; pp. 15–18, 20–21.	Independent recovery; portable resolution; retain revision and event evidence.	Restored data does not verify its relation to the physical item.	Host exit; resolver migration; replaced carrier; unrecorded component change.
False end-of-life state: 46A–49A; p. 21.	Role-scoped event submission; preserve evidence and status history where lawful.	Authorised reporting still needs corroboration of physical treatment.	False destruction report; impersonated recycler; contested state correction.

Continued on next page

Table 7 continued

Risk and source evidence	Proposed control	Residual limitation	Planned test
Context or memory reuse: paper-proposed extension, not a CIRPASS-2 result.	Carry source restrictions, provenance and expiry into derived local records.	Copies and summaries can escape original access boundaries.	Expired evidence reused in memory; unauthorised derivation or downstream action.

Printed page numbers refer to CIRPASS-2 v1.1; add two for PDF page numbers. Risk identities are documentary evidence; the controls and tests are this paper's synthesis and proposed evaluation, not measured effectiveness. No full mapping of all 52 entries is claimed here. [90]

8 What interoperability and atlas checks establish

8.1 A bounded external exchange report

The release contains one qualified external report of cross-ecosystem exchange. NEDO and NTT DATA reported on 31 March 2025 that Japan's Battery Traceability Platform and Catena-X exchanged product carbon-footprint information in demonstration environments. Work ran from July 2024 to January 2025. An intermediate layer reconciled authentication, protocols and data models for reciprocal retrieval scenarios. The report also identified institutional and operational matters requiring further work. This is a bounded observation that separates a successful technical operation from wider conditions for sustained cross-border use. [81]

Our case analysis is documentary. We did not operate the demonstration, obtain its complete payload corpus or reproduce its results. Exact system versions and the artifacts needed for a repeatable benchmark remain unspecified in the evidence record. Its category is consortium-reported success, with environment and independence recorded separately. It should not be redescribed as an independent production evaluation. One carbon-footprint operation also cannot establish compatibility for all battery-passport attributes, lifecycle transitions or permissions. [4]

Analytically, the case motivates a more precise vocabulary for convergence. Compatible operation may be achieved through an intermediary that preserves differences between architectures, rather than by adopting one common schema. This raises questions the evidence cannot settle: which transformations preserve meaning, who maintains them as versions change, and who accepts the resulting evidence for a decision? These are follow-up questions, not negative findings about the demonstration. The reported result is most useful when its operational boundary remains visible.

Figure 5 separates ten dimensions. The source supports bounded reports of protocol, model and authentication conversion. Seven other dimensions have no qualified result coded in this seed. That label does not mean the implementers performed no tests, that a dimension failed, or that no other demonstrations exist. Model conversion is weaker evidence than a benchmark of semantic preservation, and authentication is weaker than recognised organisational authority. The denominator is one documentary case, not the worldwide population of DPP implementations. [4]

One reported exchange, ten distinct dimensions

Japan Battery Traceability Platform - Catena-X demonstration

Dimension	Corpus result	Scope of the evidence
Product identity	No result coded	Not assessed in this seed
Syntactic exchange	Reported	Protocol conversion reported
Semantic meaning	Reported	Model conversion reported, bounded
Evidence provenance	No result coded	Not assessed in this seed
Authentication	Reported	Authentication conversion reported
Business identity	No result coded	Not assessed in this seed
Delegated authority	No result coded	Not assessed in this seed
Access control	No result coded	Not assessed in this seed
Lifecycle continuity	No result coded	Not assessed in this seed
Legal acceptance	No result coded	Not assessed in this seed

Interpretation boundary

Consortium report; demonstration environment; versions unspecified.
No independent replication is reported by this study.

Figure 5: Evidence by dimension for the one qualified reported operation coded in release 0.1.0: reciprocal product carbon-footprint retrieval between the Japan Battery Traceability Platform and a Catena-X demonstration environment using an intermediary conversion layer. Assertion a-global-jp-cfp-exchange and the NEDO/NTT DATA announcement support bounded reports of protocol, model and authentication conversion. Model conversion does not establish comprehensive semantic equivalence; authentication does not establish recognised business identity or delegated authority. For the other seven dimensions, result=not_tested together with coding_status=not_assessed is displayed as No result coded. This does not assert that implementers performed no tests or that interoperability failed. Work ran July 2024-January 2025; exact execution dates and system versions are unspecified. This is a consortium report, not an independently reproduced result, general production claim or demonstration of legal recognition. Coding remains independently unreviewed. [4, 81]

8.2 Completed research-artifact verification

The release has undergone structural validation, regression testing and reconstruction checks. The validation package checks identifier uniqueness, complete entity and source references, appropriate jurisdiction and sector reference types, sources for substantive entities and dated events, date precision and conditional-trigger integrity, observation cut-offs, and consistency between reported and measured outcomes. Twenty-seven regression cases test these constraints, including rejection of missing references, unsupported coercion of conditional dates and confusion between absent evidence and a failed experiment. These checks passed in the archived release verification. [17]

Ten competency questions were executed against the release. They exercise the retrieval of source-qualified answers about the selected corpus and provide stable examples of intended use. Their expectations were defined within the research process. Successful execution establishes that the queries operate on the encoded data; it does not independently validate the legal interpretation or establish that the chosen questions represent every user's information needs. The distinction is essential because a logically consistent graph can reproduce an incorrectly coded assertion without generating a software error.

The release verification records 41 manifest-listed files and a byte-identical rebuild from the frozen inputs and scripts. A further checksum check during manuscript preparation found no changes to those files. Hash agreement establishes identity of the retained artifacts, not correctness of their contents or ownership of third-party texts. Source URL identifiers and source-access records should not be confused with archived copies of restricted standards or legal documents that were not actually retained. [104]

The accompanying explorer implements shared map, graph and table filters, record and assertion inspection, a static catalogue and shareable selections. Its local verification reports 24 interface-model tests and browser checks of filtering, source details, empty states, deep links and responsive layouts. The full graph presents 128 substantive nodes and 87 coded inter-record edges; literal assertions remain available through details. Those counts describe the chosen visual projection of the evidence model, not an additional set of independent observations. [105]

Table 8 distinguishes these completed checks from interpretation accuracy, user benefit and operational performance. The atlas preserves inspectable claims and a reproducible snapshot. It has no independently adjudicated accuracy estimate, no user study and no real correction replay across two substantive dataset releases. The version 0.4 manuscript supplement records new observations; it is not a substitute for that release-to-release experiment. [5]

Table 8: Completed checks and unperformed evaluation

Assessment	Observed state	Interpretation
Structural / regression checks	27 passed	Internal consistency, not legal accuracy
Competency questions	10 executed	Researcher-defined expected answers
Frozen release reconstruction	41 files; identical rebuild	Identity of retained artifacts
Explorer verification	24 model tests; browser flows checked	Functionality, not measured usability
Independent assertion review	0 of 224 reviewed	Planned qualified review
Mapping / authority experiments	Not performed	Designs proposed in Sections 10–11

Continued on next page

Table 8 continued

Assessment	Observed state	Interpretation
Real correction replay	Not performed	Separate from the manuscript supplement

Sources: archived release and interface verification. [17, 104] [105]

9 Evidence Graphs as Shared Infrastructure for Products and AI

9.1 A shared infrastructure proposition

Access-controlled, verifiable evidence graphs for physical products, virtual products and physical AI—built on open international standards and open-world semantics.

This proposition extends the paper's argument beyond the documentary findings of the atlas. Product passports and AI assurance systems repeatedly need to identify an object, attribute claims, preserve their sources, record change and establish who may use particular information for a particular decision. Reusing those functions could reduce repeated integration work across product and service lifecycles. Whether that reuse improves decisions, lowers costs or supports cross-border reliance remains a question for evaluation. The following synthesis draws on Spherity's related architecture research; these publications articulate the proposition and are not independent confirmation of its benefits. [91]

An evidence graph links claims to the observations, documents, transformations and responsible actors that support them. An assurance argument explains why selected evidence justifies confidence in a specified property under stated conditions. The graph can make that argument inspectable, including its limitations and missing premises. Verification of integrity or issuer binding does not establish factual truth, and a structurally complete record can still contain an unsuitable measurement or an unsupported inference. Assurance therefore depends on evidence quality, applicable requirements, assessment methods and the consequences of the intended use.

Access control adds another independent question: who may retrieve, change or rely on which view? Public information and commercially sensitive evidence can require different disclosure rules. The proposed separation between an evidence data plane and an organisational-authority control plane makes those responsibilities explicit. An authorised repairer may read a battery's service information without having permission to alter its declared characteristics; a manufacturer may issue a claim without that claim satisfying every recipient's acceptance policy. [91]

9.2 Open-world integration and bounded decisions

Open-world semantics accommodates incomplete knowledge. In OWL, a statement that cannot be inferred from the available ontology is not thereby established as false. This is useful when organisations contribute different parts of a product's history and new evidence arrives later. It is also incompatible with treating the absence of a recorded prohibition as sufficient permission for a consequential action. A decision must specify which evidence is required, which sources are recognised and how missing, stale or conflicting information affects the outcome. [106]

Bounded validation can operate within that wider evidence network. A decision profile might require an identified component, an applicable test, a current calibration and an authorised assessor for a defined configuration. SHACL can express conditions against which an RDF

data graph is checked. Passing those conditions establishes conformance to the selected shapes, not completeness of all relevant real-world knowledge. Domain rules, evidence acquisition and review remain necessary. The application must also record the profile version and evidence view used, so that a later change can be related to an earlier decision. [107]

Open international standards supply shared technical foundations; they do not guarantee universally agreed domain meanings or recognition of every issuer. Product terminology, measurement methods, authority and acceptance still require governed profiles and explicit mappings. Likewise, AAS, RDF/OWL and JSON-LD perform different roles. AAS can provide industrial source models; semantic models can link claims across sources; serializations can carry those models. The appropriate combination should be tested against actual tasks, including the cost of maintaining mappings. Related Spherity research explicitly does not report a direct AAS-versus-JSON-LD AI benchmark. [3]

9.3 A continuum of evidence subjects

Figure 6 presents three connected classes of evidence subject. Physical products have component identities, material and performance records, repair events and lifecycle responsibilities. Here, a passport can expose or reference evidence relevant to a product obligation or operational decision. The applicable legal duty remains tied to the relevant instrument, product scope and conditions; the broader architecture does not create additional statutory passport requirements.

Virtual products, as used here, include software packages, model-based services and other digital deliverables. Their relevant configuration may involve a model version, tools, dependencies, guardrails and deployment settings. A proposed AI Service Passport would connect that configuration to its provider or operator, intended purpose, evaluation evidence, incidents and current status. It is a research profile, not an established universal passport standard or a claim that current DPP law generally mandates AI-service passports. A service record can make assessment evidence discoverable while leaving permission for each consequential action to the receiving organisation. [108]

Physical AI combines these subjects: a robot's behaviour depends on installed components, control software, models, skills and operating context. Skills describe executable capabilities, while memories may preserve earlier observations or influence a subsequent plan. Such artifacts can require versioning and evidence dependencies without every memory being treated as a separately marketed product. The relevant assurance unit is the configured system in a defined task and environment. This is an architectural continuum, not a maturity ladder or a single legal category. [109, 110]

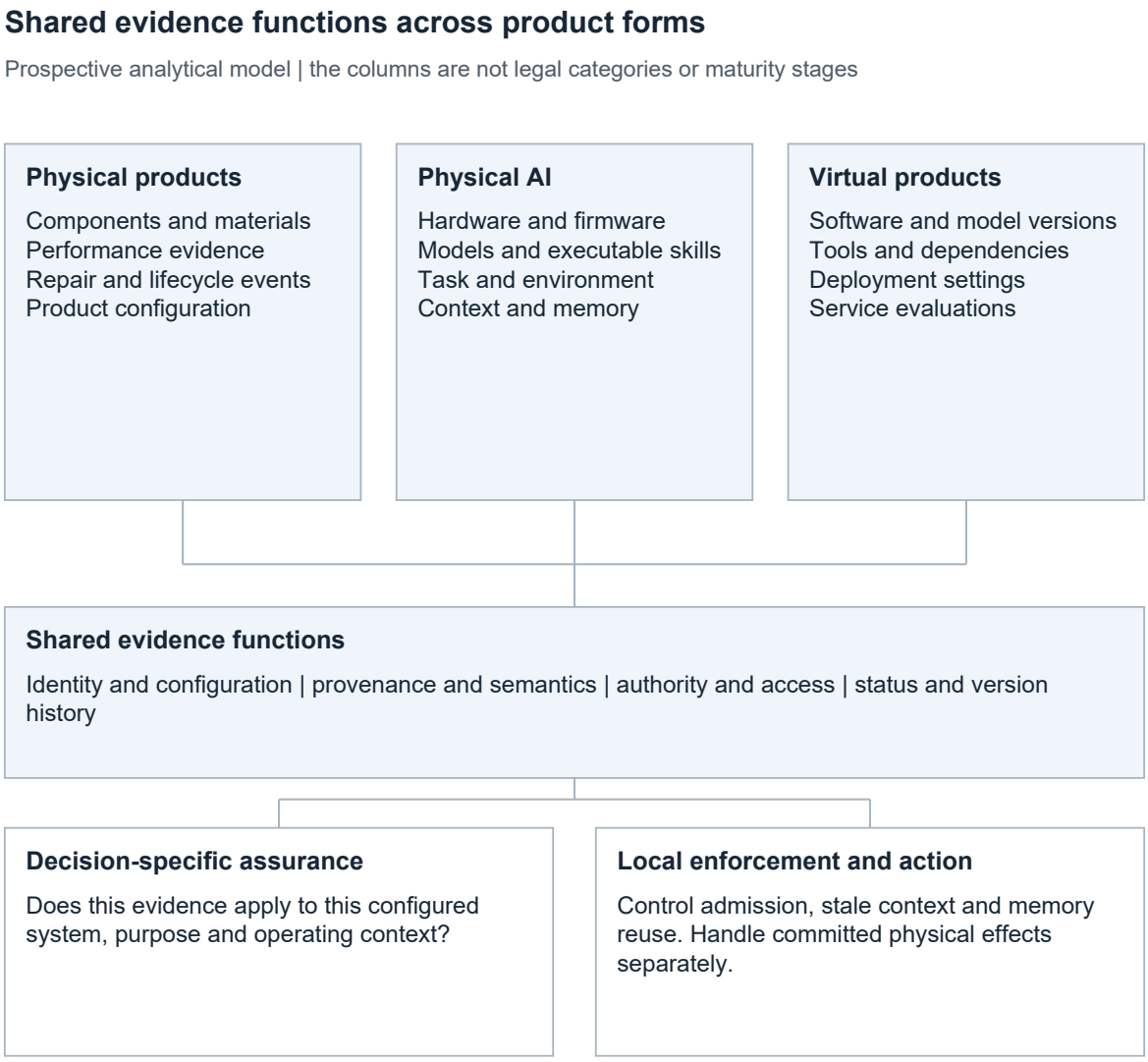


Figure 6: Author-proposed evidence model spanning physical products, physical AI and virtual products. Parallel columns express related evidence needs without implying identical legal duties or a maturity sequence. Versioned components, executable skills and memory can influence the configured system and its task-specific assurance case. Shared semantics and verifiable provenance do not establish authority, safe use or institutional acceptance. Local admission, action and recovery controls remain distinct from an external evidence graph. No cross-domain validation of this model was performed. [3, 91] [109, 110] [108, 111]

9.4 A humanoid-arm replacement and firmware update

Consider a humanoid robot whose arm module is replaced during maintenance and whose firmware is then updated. The replacement carries authentic component documentation, and the update has a valid supplier signature. Those checks establish useful facts about the supplied artifacts. They do not establish that earlier system tests cover the new combination of actuator, brake, sensor, firmware, tool, payload and task. The proposed evidence graph would connect the installed configuration to the claims and tests on which commissioning relied, then identify which dependencies changed. [109]

A qualified assessor could determine that some evidence remains applicable, that a parameter change requires a limited test, or that a wider integration assessment is necessary. The graph would preserve that decision, its scope and the responsible organisation. Its value would be measured through correct applicability judgments and change-impact identification, alongside the time required to reach them. Faster processing would be useful only if unsupported configurations are not accepted more often. Functional-safety engineering and deterministic protective functions retain their own qualified control paths; the graph supports assurance and change decisions.

Memory adds a further dependency. A grasping episode captured with the previous arm or tool may contain useful geometric observations while no longer supporting the same force recommendation. An incorrect success label may be withdrawn without discarding every informative segment. The receiving system needs an assessment covering the claim, reuse role and actual configuration. Copies distributed to multiple robots do not create independent observations. The related governed-memory research proposes Memory and Robot Bills of Materials for these relationships, with bounded protocol analysis rather than demonstrated robot-level behavioural benefit. [110]

Finally, an authority withdrawal or adverse finding must affect actual use. Removing an item from future retrieval does not remove its influence from retained context, a plan or a queued command. A protected admission boundary must relate current permission and applicable assurance to the exact operation. Already committed physical effects require an appropriate continuation or recovery procedure: a robot holding a load may need controlled stabilisation. Status publication, receiver enforcement and physical recovery are different events. Related runtime and revocation studies supply designs and bounded evaluations, not a general guarantee of safe physical stopping. [111, 112]

9.5 AI first infrastructure and the risk of architectural displacement

In this paper, AI-first infrastructure means that discovery, evidence retrieval and permission checks are designed for automated consumers as well as people. It requires more than converting asset records into another syntax. An AI system must handle incomplete and conflicting evidence, changes of configuration, current authority and uncertainty about whether a claim applies to its intended action. The two AAS/RDF papers advance representation and integration work; they do not evaluate this full decision path. [68, 69]

Strategic programmes indicate a broader competitive environment. The US AI Action Plan of 23 July 2025 prioritises AI infrastructure and international dissemination of packages spanning hardware, models, software, applications and standards. China's AI Plus Manufacturing notice, issued on 25 December 2025 and published in January 2026, addresses industrial agents, model and data engineering, agent discovery, identity and access mechanisms, and cloud-to-edge deployment. CESMII's i3X 1.0, announced on 18 June 2026, offers a complementary

API for contextual manufacturing information with AI-facing tooling. These are policy priorities and technical initiatives, not proof of AAS rejection or measured effects of investment on adoption. [113, 114] [115]

Our conditional strategic expectation at Spherity is that US and Chinese AI-first industrial ecosystems will combine several asset, context and domain models, with AAS serving selected industrial interfaces rather than becoming the dominant cross-domain evidence model. This is a forecast about architectural centrality, not a prediction of non-adoption. China's organised standards work and US institutional collaboration are meaningful counterweights: they could expand AAS's role. Section 5.7 also documents stronger Korean programme support and sustained Japanese participation. None of these observations settles future dominance, and no numerical probability is assigned.

The displacement scenario is that investment and developer attention move the organising layer for new applications towards systems that combine heterogeneous evidence without requiring every participant to adopt one asset model. Rigid AAS-centred implementations could then lose influence even while operational AAS systems continue supplying useful data. The competing scenario is that AAS profiles evolve into a widely used bridge for those applications. Broad, independently documented US and Chinese production use of AAS as the primary information model for cross-domain AI workflows, explicit AAS-specific procurement or deployment programmes, replicated AI task evaluations and low cross-vendor integration costs would weaken our expectation of a selective role. Technological change can shift the dominant interface without erasing the underlying industrial assets, models or obligations.

10 Scenarios for Global DPP Convergence

10.1 Two independent dimensions

The following scenarios organise prospective research rather than predict adoption. They ask how the shared-infrastructure proposition could develop when two independent conditions vary: demonstrated technical interoperability and institutional recognition. Technical interoperability concerns a bounded operation across identified implementations, including preservation of relevant meaning, evidence references, access conditions and status. Institutional recognition concerns whether participating organisations or competent bodies accept particular issuers, assessments, mandates and decisions for the stated purpose. Neither axis is measured globally by release 0.1.0.

Figure 7 shows four analytical combinations. The labels describe possible arrangements for a specified workflow, not countries or standards organisations. An ecosystem can occupy different combinations for different tasks: exchanging a public material identifier may be routine while accepting a protected safety assessment remains unresolved. Movement across the figure is neither automatic nor irreversible. A changed profile, incident or withdrawn recognition can alter a previously usable arrangement. No probabilities, adoption dates or country rankings are assigned.

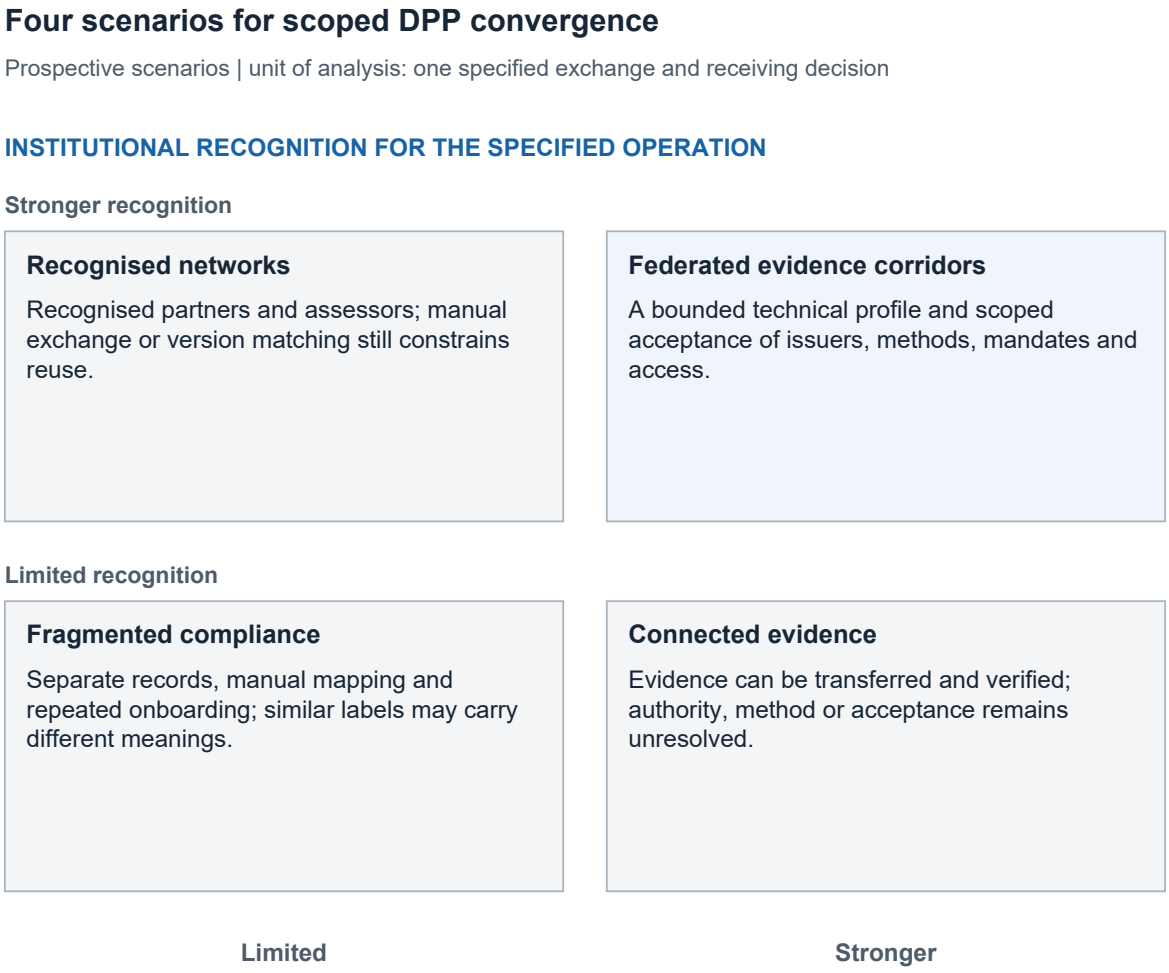


Figure 7: Prospective scenarios cross demonstrated technical interoperability with institutional recognition for a specified operation. Recognition concerns the relevant issuer, method, mandate, purpose and decision; it is not inferred from successful data transfer. The scenarios are analytical constructs, not measured placements of jurisdictions or ecosystems. A single ecosystem can occupy different scenarios for different workflows. There are no probabilities, trend arrows or assumed progression; release 0.1.0 does not measure either axis. [4, 91]

10.2 Fragmented compliance limited exchange and limited recognition

In the first scenario, organisations maintain separate passport records, documentary evidence and onboarding arrangements. Recipients reconcile identifiers, terminology and authority manually. Similar information requests produce repeated work, but common labels do not ensure that the underlying measurements or legal responsibilities match. A supplier serving several markets may therefore maintain related yet distinct compliance views.

An initial intervention would identify a narrow function that can be compared safely, such as linking a repair event to the correct battery and responsible operator. Useful indicators include the number of manual transformations, unresolved scope discrepancies, requests for the same evidence and time to identify an accountable issuer. These observations would establish the workflow's baseline. They would not justify assuming that every difference should disappear: some reflect substantive requirements or legitimate limits on disclosure.

10.3 Connected evidence exchange without portable recognition

In the second scenario, systems resolve identifiers, interpret selected payloads and verify cryptographic provenance, but recipients still disagree about issuer competence, assessment scope or permissible reliance. A supplier's test record may arrive intact and be machine-readable while a recipient requires a different method or a recognised assessor. A business credential may identify an organisation without establishing its authority to approve a configuration.

The potential benefit is narrower than full mutual acceptance: reliable transfer can reduce transcription and make outstanding recognition questions visible. Evaluation should measure successful exchanges alongside semantic exceptions, acceptance decisions and reasons for rejection. Particularly informative cases are technically valid records that should be refused because their authority, method or scope is unsuitable. The distinction follows the paper's separation between demonstrated exchange and recognised evidence; a signature check must not collapse the two.

10.4 Recognised networks accepted partners with constrained exchange

In the third scenario, participants recognise each other's roles and assessments through established governance, contracts or sector arrangements, while evidence remains difficult to exchange and update. Organisations may trust a named testing body yet rely on document portals and manual configuration matching. Changes then move more slowly than the underlying engineering work, and an accepted document can be applied to the wrong version.

The research opportunity is to preserve existing accountability while improving evidence structure, retrieval and change notification. A competent document-and-registry workflow is the appropriate baseline; it must not be artificially weakened to favour a graph. Measures include correct identification of applicable evidence, time to resolve a version mismatch, affected assessments found after a change and legitimate work delayed by incomplete records. Recognition already present in the network cannot be credited as a benefit created by the technical representation.

10.5 Federated evidence corridors bounded exchange and recognition

In the fourth scenario, participants agree a scoped exchange profile and rules for recognising the evidence and authority needed for a particular operation. A corridor could connect battery

repair, component replacement or an AI-assisted maintenance service across companies. It would define product and configuration boundaries, supported versions, issuer roles, accepted methods, access policy, current-status requirements and responsibility for adverse findings.

This arrangement could support reusable evidence without requiring one global database or universal ontology. Each recipient would retain its own decision and enforcement responsibilities. The corridor's claim must remain bounded: successful battery-repair exchange does not establish interoperability for robot commissioning or every jurisdiction. Research on cross-domain eligibility provides a candidate pattern for separating recognition, deterministic policy evaluation and protected execution, but production implementation and independent testing remain necessary. [116]

Indicators should combine positive and adverse cases: correctly completed operations, rejected scope violations, disclosure minimisation, withdrawal enforcement, unresolved remote work and the cost of maintaining mappings and governance. A corridor that achieves low error only by blocking most legitimate work would have a different operational value from one that preserves useful activity. Both security outcomes and availability costs therefore belong in the evaluation.

DPP and business-wallet convergence could strengthen this scenario if a common policy profile connects product evidence to recognised actors and enforceable permissions. A shared credential syntax without accepted recognition issuers would remain in the connected-evidence scenario. Agreed issuer lists without compatible policy interpretation would leave a recognised network with constrained exchange. Advancement therefore requires both institutional agreements and reproducible positive and negative access tests; the publication of a draft vocabulary alone changes neither axis.

10.6 Value beyond ESPR and a measurable research programme

The shared functions may matter wherever evidence must survive organisational and configuration changes. Candidate applications include repair and reuse, industrial commissioning, supplier qualification, warranty decisions, software maintenance and governed deployment of AI services. These are possible sources of value beyond a particular regulatory reporting duty. Their inclusion does not imply that the same law governs them, that passports are mandatory, or that an evidence graph is always the most economical solution.

The AAS outlook in Section 9.5 is a conditional overlay on these scenarios. A hybrid AAS-to-evidence-graph route could support connected evidence or a federated corridor if its transformations and authority rules are demonstrated. A universal AAS model and a direct semantic-model approach are competing hypotheses to test under equivalent requirements. Large AI programmes may accelerate either adaptation or displacement; the current evidence does not establish which outcome will prevail. The relevant unit remains a specified operation, rather than a forecast that an entire country will choose one stack. Institutional commitment and deployment reach must be tracked on separate axes: the four country cases are not measurements of either scenario axis, and public programmes can coexist with a continuing plurality of models.

Four proposed experiments would connect the scenarios to observable outcomes: a delegated agent reading and updating battery-repair evidence; a robot-arm replacement followed by firmware change; reuse of an assessed memory segment in a changed receiving configuration; and an AI-service update affecting a remote tool operation. Each experiment should freeze the subjects, versions, source material, decision rules and acceptance criteria before comparing approaches. The tests should include incorrect product scope, stale assessment, changed payload, revoked delegation, lost receipt and restart with pending work.

Evaluation should compare a competent source-linked document or API workflow with the proposed graph-supported workflow. Where AAS is relevant, an AAS-backed implementation and explicit graph mapping should receive equivalent information and engineering attention. Measure evidence-retrieval accuracy, configuration applicability, correctly detected adverse conditions, completed legitimate work, disclosure, latency and maintenance effort. Independent review should adjudicate whether the accepted evidence actually supports the decision; software conformance alone cannot supply that judgment.

These scenarios therefore translate convergence into a programme of bounded tests. The near-term question is whether shared representations and explicit authority rules improve a defined workflow while preserving its requirements. Broader claims about global acceptance, AI safety or environmental and economic benefit require their own evidence. The atlas can record the resulting operations, profiles and limitations in future releases, keeping prospective designs separate from reported and independently reproduced results.

11 Limitations, disclosure and planned validation

11.1 Limits of the evidence and author position

The selected corpus has several sources of bias. Discovery was purposive, with greater visibility for European instruments and internationally accessible initiative documentation. Language, indexing and access affect which non-European material could be inspected. The inclusion of both explicit DPP instruments and adjacent traceability rules broadens functional comparison but creates a classification burden that needs qualified review. The map's visually large countries and EU display joins must not be interpreted as a representative sample of legal systems or supply-chain adoption.

Source-access limitations constrain the strength of the findings. The majority of source records were not freshly opened in the frozen release, and catalogue access does not substitute for review of normative text. English paraphrases of Chinese, Japanese and Korean material need specialist checking before stronger legal or technical conclusions are published. The corpus also contains few provision and requirement entities relative to its broader inventory. Absence of a coded relationship may reflect incomplete extraction, inaccessible evidence or a deliberate scope choice rather than an actual incompatibility.

Implementation evidence is particularly sparse within the selected seed. One coded qualified demonstration does not imply that only one such demonstration exists globally. Unspecified system versions and unavailable public test artifacts limit reproduction and generalisation. Private production exchanges, unsuccessful tests and unpublished adaptations may be underrepresented. A future review should seek such evidence explicitly and retain negative or inconclusive results, rather than selecting only announcements of success.

The present research cannot attribute lower costs, improved environmental outcomes or reduced compliance risk to DPP technology. Those outcomes require different measures and study designs. Nor does it establish that verifiable credentials or business wallets are necessary for every passport architecture. Registries, signed documents, authenticated APIs and other institutional arrangements may satisfy particular functions. A fair comparison must hold the decision policy and required evidence constant before attributing an advantage to one technical approach.

The paper is prepared in the Spherity research context. The W3C directory lists the author as a facilitator of the VC DPP & Business Wallet task force; he participates in that work and is acknowledged by CIRPASS-2 for contributions concerning authenticity and authorisation in the risk report. These relationships supply relevant domain experience and are also potential

sources of interpretive bias. Neither participation nor acknowledgement amounts to institutional endorsement or independent validation of this paper. Self-cited Spherity papers are used as architectural contributions with their stated empirical limits. [53, 90]

Third-party quotations retain their original attribution and licence notices; no additional rights are claimed in them. Natural Earth map geometry remains in the public domain.

11.2 Tests required before stronger claims

The following programme is planned and has not been executed for this edition. First, qualified reviewers should independently assess material legal scope, dates, actor roles and conditional requirements, including original-language material where needed. The reviewed denominator, disagreements and adjudicated corrections should be published. A real correction should then be replayed into a second dataset release while preserving the earlier answers and their provenance.

Second, freeze two comparable public profiles and publish transformation fixtures. Vary units, measurement boundaries, product granularity, lifecycle stage, methods and evidence references. Record exact, partial, lossy and conflicting mappings. Compare against a competent conventional mapping under identical requirements. Third, test authority and access policy with legitimate requests, wrong issuers, missing delegation, expired status, overbroad scope, revoked access and stale caches. Compare credentials with registry, signed-document or API arrangements under the same decision policy.

The AAS comparison should include a competent native AAS workflow, the improved RDF projection, and a direct domain-graph or API alternative, using the same source records, models, decision policies and AI tasks. Include unfamiliar partner data, renamed elements, ordered lists, changing units, conflicting claims, revoked permission and unavailable evidence. Measure semantic loss, identifier stability, round-trip fidelity, update cost, provenance preservation, false acceptance, legitimate work completed and integration effort. Existing SHACL checks should be retained where applicable; proposed-profile extensions need their own versioned tests. A shorter SPARQL query is a useful intermediate result, not a substitute for accuracy on the downstream decision. Independent implementations and external review are required. [68, 69] Adoption monitoring should record programme budgets specifically attributable to AAS, actual template use, named production sites, operating duration, cross-vendor transactions and the model's role in AI workflows. Standards projects, training attendance and consortium membership remain separate indicators.

Fourth, test the lean-dataspace proposition with two independently operated implementations, a regulator or assessor access route, and a controlled change of provider. Measure onboarding effort, integration cost, policy errors, evidence retrieval and service discontinuity. Fifth, test the proposed product–AI continuum on a versioned robot configuration: revoke one skill or alter a component, then measure which dependent decisions and evidence paths are invalidated. A safety expert must define the relevant operating envelope; a graph query cannot replace a safety assessment.

Finally, test whether the research graph improves specific tasks against a source-linked table, using independently defined questions and blinded answer assessment where feasible. Report errors, time and traceability as separate outcomes. These experiments can establish bounded system behaviour and researcher utility. Legal mutual recognition, real-world safety and environmental benefit require their own institutional and empirical evidence.

12 Conclusion and implementation guide

12.1 What the study supports

The documented landscape contains overlapping product-information functions, distinct legal obligations and multiple institutional routes towards compatible implementations. Those connections are useful evidence of organised work, but they do not demonstrate worldwide semantic equivalence or mutual recognition. The selected Japan–Catena-X report shows why a successful bounded exchange and unresolved institutional questions can coexist. The atlas's completed checks establish reproducibility of a selected research snapshot, while all 224 baseline assertions remain pending independent qualified review.

The architectural anchor remains: **Access-controlled, verifiable evidence graphs for physical products, virtual products and physical AI—built on open international standards and open-world semantics.**

This is a proposition for shared infrastructure. For a battery, the graph can connect a footprint claim to its method and assessment. For an AI service, it can connect an operational claim to the version, evaluation and permitted action. For physical AI, it can connect components, software and skills to a bounded operating context. Product compliance and accountable AI can draw on the same evidence foundations while retaining different legal tests, safety controls and decision responsibilities. The metaphor of two sides of the same coin is useful at the infrastructure level; it does not establish equivalence between a DPP and AI assurance.

W3C's product and business-wallet work, UNTP identity anchors and ODRL policy expressions offer complementary building blocks for this proposition. The practical connection is between the evidence about an object, the authority of the actor, and the conditions governing a particular use. Their composition must preserve the distinction between verified provenance, accepted recognition and enforced permission. Version 1.0 finalises this paper's synthesis; it does not finalise the draft standards or convert its planned experiments into results.

12.2 Practical implementation sequence

Begin with one product and one consequential decision. Record the applicable instrument, responsible actor, exact scope, date type and evidence needed by the recipient. Give every claim a subject, issuer, method, validity interval and source. Keep the public passport view separate from restricted evidence. Use stable identifiers and versioned vocabularies; document mappings and information loss. Preserve industrial source systems, including AAS where useful, through explicit adapters rather than rebuilding all information to fit one exchange format.

For AAS adopters, retain industrial value while requiring portable semantic exports, attributable evidence and enforceable permissions. Track China's eventual publication and implementation guidance, the transition from US prototypes to sustained production, Japanese cross-architecture exchanges, and actual use of Korea's reference models after its end-2026 target. These are different adoption signals. National standards and public programmes warrant engagement; they do not independently establish broad deployment or AI readiness. Our expectation of heterogeneous AI infrastructure should guide portability and testing, not be presented as evidence that major markets have rejected AAS.

Next, implement permissions and status as operating controls. Identify the business, representative and permitted action; check policy at retrieval and use; test expiry, revocation, delegation and cached copies. Establish an assessor or regulator route that works under the relevant law. Test the exchange with a second implementation, including failure cases, and retain the evidence

of what passed. Treat adoption announcements, successful signatures and registry registration as inputs to assurance, not substitutes for the applicable decision.

For a wallet-enabled implementation, pin the credential and identity-anchor versions, accepted registrars and recognition issuers, and the ODRL profile with its supported actions and constraints. Test policy interpretation with another implementation before relying on it. Over six months, prepare one protected-evidence workflow and adverse test set; over twelve months, compare decisions and revocation behaviour across implementations; over twenty-four months, assess actual portability and scoped recognition. These are proposed work packages, not forecasts that W3C or UNTP drafts will have reached a particular status.

Table 9 gives dated observation horizons from 25 October 2026. The dates are review checkpoints, not forecasts of universal adoption. At six months, prepare for enacted near-term obligations and inspect the status of the steel measure. At twelve months, review draft product measures and operational readiness, while recognising that Q4 2027 targets may fall after the checkpoint. At twenty-four months, reassess furniture developments, actual transformations and scoped recognition arrangements. Keep 2029 measures outside that horizon. [5]

Value beyond ESPR compliance should be demonstrated with a baseline: less duplicate evidence collection, faster repairs or supplier qualification, better recall targeting, or fewer unsupported AI decisions. Measure these outcomes against a competent existing process and retain adverse results. The next decisive step is not a larger graph. It is reviewed requirements, reproducible exchanges and explicit evidence of when a recipient can rely on a claim.

Table 9: What to watch and do over six, twelve and twenty-four months

Checkpoint	Watch / expect conditionally	Implementer action
6 months 25 April 2027	Battery passports: fixed 18 February 2027. Machinery: adjacent fixed 20 January 2027. Verify outcome of steel Q4 2026 target and registry semantic availability.	Prioritise covered products; prepare correct evidence and permissions; exercise registration and recovery in the relevant environment.
12 months 25 October 2027	Construction and service-provider act progress; textiles, aluminium and tyres targets in 2027. Q4 targets may complete after this checkpoint. Track Product Act negotiations.	Pin profiles and standards versions; test two implementations, delegation and status; retain conditionality until final acts establish application.
24 months 25 October 2028	CRA main application from 11 December 2027. Furniture target in 2028 may fall later than this checkpoint. Check international standards outputs and scoped recognition agreements.	Reassess adapters and evidence reuse; test provider exit and changes; measure operational value. Do not assume mutual recognition from a standards publication.

Watchpoints use the 25 October 2026 observation date. Planned adoption is not guaranteed; mattresses and the 2029 EEE measure lie beyond this horizon. [19, 23] [25, 67]

A Geographic coverage

This table provides the accessible geographic counterpart to Figure 1. Counts identify substantive records within each scope. The same records can occur in more than one row, especially through EU display joins, so rows must not be summed to estimate unique records or mandates. A country polygon indicates that the cartographic geometry can represent the country row, not that the country has been independently assessed. Great Britain and Northern Ireland are kept as separate scopes. [4, 18]

Table A1: Geographic rows retained in release 0.1.0

Geographic scope	Scope type	Direct records	EU joins	Polygon
Austria	country	0	27	Yes
Australia	country	1	0	Yes
Bangladesh	country	4	0	Yes
Belgium	country	0	27	Yes
Bulgaria	country	0	27	Yes
Brazil	country	1	0	Yes
Paraná	subnational	1	0	No
Canada	country	1	0	Yes
Switzerland	country	1	0	Yes
China	country	5	0	Yes
Cyprus	country	0	27	Yes
Czechia	country	0	27	Yes
Germany	country	5	27	Yes
Denmark	country	0	27	Yes
Estonia	country	0	27	Yes
Egypt	country	2	0	Yes
Spain	country	0	27	Yes
European Union	supranational	38	0	No
Europe	region	10	0	No
Finland	country	0	27	Yes
France	country	0	27	Yes
United Kingdom	country	0	0	Yes
Great Britain	territory	1	0	No
Northern Ireland	territory	1	0	No
Global scope	global	40	0	No
Greece	country	0	27	Yes
Croatia	country	0	27	Yes
Hungary	country	0	27	Yes
Ireland	country	0	27	Yes

Continued on next page

Table A1 continued

Geographic scope	Scope type	Direct records	EU joins	Polygon
India	country	3	0	Yes
Italy	country	0	27	Yes
Japan	country	5	0	Yes
Republic of Korea	country	2	0	Yes
Busan	subnational	1	0	No
Lithuania	country	0	27	Yes
Luxembourg	country	0	27	Yes
Latvia	country	0	27	Yes
Malta	country	0	27	No
Netherlands	country	0	27	Yes
Norway	country	1	0	Yes
New Zealand	country	1	0	Yes
Poland	country	0	27	Yes
Portugal	country	0	27	Yes
Romania	country	0	27	Yes
Sweden	country	0	27	Yes
Singapore	country	1	0	No
Slovenia	country	0	27	Yes
Slovakia	country	0	27	Yes
Türkiye	country	1	0	Yes
United States	country	1	0	Yes
California	subnational	1	0	No
Viet Nam	country	2	0	Yes

Source: frozen geographic view and Figure 1 coverage table. No polygon is assigned to global, regional or territorial rows. [18]

References

Numeric references identify the cited source or companion research artifact. Baseline access states describe release 0.1.0 and do not imply independent human review. Later literature checks are dated separately. The URLs below identify authoritative records; access to a catalogue does not imply access to the full normative standard.

[1] European Union. 2024. Regulation (EU) 2024/1781, consolidated text. Locator: Articles 4(1), 4(4), 13, 72 and 79. Supplementary official indexed legal text, including Articles 4 and 13; direct text requests challenged. Frozen access status unchanged. Observed 2026-10-25. https://eur-lex.europa.eu/eli/reg/2024/1781/2024-06-28/eng

[2] European Union. 2023. Regulation (EU) 2023/1542, Batteries Regulation. Locator: Article 77; fixed passport date corroborated by current Commission timeline, without fresh complete consolidated-law review. Frozen access state: unavailable. Direct opening returned a JavaScript challenge. Dossier identifies consolidated text dated 13 August 2026; consolidation was not independently reopened. Observed 2026-10-23. https://eur-lex.europa.eu/eli/reg/2023/1542/ojn

[3] Carsten Stöcker. 2026. 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. Published 9 July 2026; page updated 7 September 2026. Research perspective; indexable summary inspected. Architectural proposal, not a direct AAS-versus-JSON-LD benchmark. Observed 2026-10-25. https://spherity.github.io/spherity-research/evidence-graphs-industrial-ai-data-plane.html

[4] Spherity Research. 2026. Global DPP evidence dataset, release 0.1.0. Companion research artifact: dpp-research/releases/0.1.0/dataset.json and manifest.json. Retained locally; no public DOI asserted. Locator: Release 0.1.0, cutoff 23 October 2026. Frozen machine-assisted evidence baseline; no independent human-reviewed findings. Observed 2026-10-25.

[5] Spherity Research. 2026. Global DPP whitepaper version 0.4 manuscript supplement. Source-qualified legal calendar, verified CIRPASS-2 risk analysis, figure provenance and amendment ledger; observed through 25 October 2026. Separate from frozen dataset release 0.1.0. Machine-assisted; independent human review pending.

[6] Spherity Research. 2026. Version 0.5 AAS evidence amendment and citation audit. Targeted full-text analysis of two supplied papers and primary-source international checks, observed 25 October 2026. Supplements version 0.4; frozen dataset release 0.1.0 unchanged. Source notes, claim boundaries and final reference-order audit retained with the manuscript.

[7] Spherity Research. 2026. Version 0.6 assessment of AAS institutional commitment and deployment evidence. Targeted primary-source follow-up for China, the United States, Japan and South Korea, observed 25 October 2026. Source notes and claim boundaries retained with the manuscript. No representative adoption survey; frozen dataset 0.1.0 unchanged.

[8] Foivos Psarommatis; Gokan May. 2026. A Comprehensive Review of Digital Product Passports in Sustainable Manufacturing: Current State, Challenges, and Future Directions. Circular Economy and Sustainability, 6, article 207. Locator: Abstract; Methodology; Results / Study Types. Publisher abstract, methodology and selected results inspected; underlying studies not re-reviewed. Observed 2026-10-24. https://link.springer.com/article/10.1007/s43615-026-00927-x

[9] Stig Morten Lyse; Lizhen Huang. 2026. Digital Product Passports: A Systematic Literature Review on Framework Design and Validation. Digital, 6(2), 43. Locator: Sections 2.2, 2.5, 3.1, 3.4, 4.6. Direct request returned 429; indexed publisher full-text passages inspected, not independently recoded. Observed 2026-10-24. https://www.mdpi.com/2673-6470/6/2/43

[10] Tarmo Robal; Riina Maigre; Hele-Mai Haav. 2026. Ontology Requirements for Digital Product Passports based on the Ecodesign for Sustainable Products Regulation. Procedia Computer Science, 277, 356–365. Locator: Publisher abstract; institutional bibliographic record. Indexed publisher abstract; details corroborated by TalTech and ETIS records. Full text not assessed. Observed 2026-10-24. https://www.sciencedirect.com/science/article/pii/S1877050926001936

[11] Elio Hbeich; Carolynn Bernier; Seth Van Hooland; Tarmo Robal; Riina Maigre. 2026. Achieving Semantic Interoperability for Digital Product Passports. Procedia Computer Science, 277, 2981–2992. Locator: Publisher abstract; institutional statement of authorship. Indexed publisher abstract; authors corroborated by TalTech and ETIS records. Full text not assessed. Observed 2026-10-24. https://www.sciencedirect.com/science/article/pii/S1877050926004552

[12] Thomas Knothe; Patrick Gering; Gernot Böge; Jason Fox; Niko D'Agostino; Coenraad van Deventer. 2025. Evaluation of the Enterprise Interoperability Framework (EIF) for Creating an Interoperable European Digital Passport System. Enterprise Interoperability XI, Proceedings of the I-ESA Conferences, 12, 177–189. Locator: Abstract; publisher citation metadata. Publisher preview and Fraunhofer abstract inspected; subscription chapter not read. Observed 2026-10-24. https://link.springer.com/chapter/10.1007/978-3-031-93995-2_15

[13] Anelia Kurteva; Carlo van der Valk; Kathleen McMahon; Alessandro Bozzon; Ruud Balkenende. 2025. RePlanIT Ontology for Digital Product Passports of ICT: Laptops and Data Servers. Semantic Web, 16(5), article 22104968251361274. Locator: Sections 5, 5.1, 5.4 and 6. Indexed publisher Introduction and Sections 5, 5.1, 5.4 and 6 inspected; institutional metadata corroborated; evaluation not reproduced. Observed 2026-10-24. https://journals.sagepub.com/doi/10.1177/22104968251361274

[14] World Wide Web Consortium. 2025. Verifiable Credentials Data Model v2.0. W3C Recommendation, 15 May 2025. Locator: Sections 1.1, 5.1, 5.2 and 5.9. Primary specification consulted; supplementary observation does not update frozen access state. Observed 2026-10-24. https://www.w3.org/TR/2025/REC-vc-data-model-2.0-20250515/

[15] World Wide Web Consortium. 2013. PROV-O: The PROV Ontology. W3C Recommendation, 30 April 2013. Locator: Abstract; Section 3.1. Primary abstract and starting-point term descriptions inspected; no atlas conformance claim. Observed 2026-10-24. https://www.w3.org/TR/2013/REC-prov-o-20130430/

[16] Spherity Research. 2026. Global DPP Atlas research protocol and evidence schema version 0.1.0. Companion release 0.1.0: research-protocol.md and graph-schema.md. Protocol frozen 23 October 2026 after initial discovery.

[17] Spherity Research. 2026. Global DPP Atlas validation report and competency query results. Companion release 0.1.0: validation-report.json and competency-questions.json. Computational verification; no independent human review.

[18] Spherity Research. 2026. Selected global DPP evidence coverage and transnational institutions. Figure package derived from release 0.1.0. Natural Earth 1:110m country geometry, repository v5.1.2, public domain. Figure provenance and 52-row coverage table supplied with the research package. https://www.naturalearthdata.com/about/terms-of-use/

[19] European Commission. 2025. Ecodesign for Sustainable Products and Energy Labelling Working Plan 2025–2030, COM(2025)187 final. Locator: Sections 2.1 and 2.2.1; adopted 16 April 2025. Official indexed text; direct full-text requests met an anti-bot challenge; schedule corroborated with Commission material. Observed 2026-10-25. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025DC0187

[20] European Commission. 2026. Iron & Steel: Digital Product Passport. Locator: Indicative Q4 2026 delegated-act adoption. Official indexed text; no final adopted steel delegated act identified in the targeted check. Observed 2026-10-25. https://single-market-economy.ec.europa.eu/single-market/digital-product-passport/iron-steel_en

[21] European Commission. 2026. Textile apparel: Digital Product Passport. Locator: Indicative Q4 2027 delegated-act adoption. Official indexed text; planned product requirements, not an adopted final delegated act. Observed 2026-10-25. https://single-market-economy.ec.europa.eu/single-market/digital-product-passport/textile-apparel_en

[22] European Union. 2024. Regulation (EU) 2024/3110, Construction Products Regulation. Locator: Articles 22(7), 75 and 80; conditional trigger corroborated by official indexed legislative text. Frozen access state: search_snippet. Direct opening returned a JavaScript challenge. Indexed Article 80 conditional timing and Article 96 application were rechecked. Product-family transitions remain dossier-derived. Observed 2026-10-23. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32024R3110

[23] European Commission. 2026. Digital Product Passport: indicative timeline. Locator: Indicative timeline, 2026–2029. Official indexed timeline; indicative dates are not application rules; inconsistent service-provider quarters not resolved. Observed 2026-10-25. https://single-market-economy.ec.europa.eu/single-market/digital-product-passport_en

[24] European Commission. 2026. Machinery: Regulation (EU) 2023/1230. Locator: Application from 20 January 2027. Official indexed overview; main application date corroborated with EUR-Lex summary; earlier exceptions not exhaustively reviewed. Observed 2026-10-25. https://single-market-economy.ec.europa.eu/sectors/mechanical-engineering/machinery_en

[25] European Commission. 2026. Cyber Resilience Act implementation. Locator: Main obligations from 11 December 2027. Official indexed implementation timeline; not a new full review of Regulation (EU) 2024/2847. Observed 2026-10-25. https://digital-strategy.ec.europa.eu/en/factpages/cyber-resilience-act-implementation

[26] European Commission. 2026. Cyber Resilience Act reporting obligations. Locator: Manufacturer reporting 11 September 2026; steward reporting 11 December 2027. Official indexed text; manufacturer and open-source software steward reporting schedules distinguished. Observed 2026-10-25. https://digital-strategy.ec.europa.eu/en/policies/cra-reporting

[27] Ministry of Industry and Information Technology, China. 2025. Interim Measures for recycling and comprehensive utilisation of waste NEV power batteries, Order 73. Locator: Articles 4, 9-12, 24, 32 and 50. Frozen access state: opened. English paraphrases are machine-assisted; no named legal translator has reviewed them. Observed 2026-10-23. https://www.miit.gov.cn/gyhxxhb/jgsj/cyzcyfgs/bmgz/jdcjxl/art/2026/art_392462fdc40c415ea4a4129cac3028c2.html

[28] MoRTH, India. 2025. Draft Guidelines for Implementation of Battery Pack Aadhaar System. Locator: Frozen release 0.1.0 source and associated dossier. Frozen access state: dossier_only. Prior dossier relied on search-indexed official draft; direct PDF extraction was blocked or timed out. Observed 2026-10-23. https://morth.gov.in/sites/default/files/Battery%20Pack%20Aadhaar%20Guideline_30122025_0.pdf

[29] Government of Vietnam. 2025. Consolidated Law on Product and Goods Quality, 156/VBHN-VPQH. Locator: Frozen release 0.1.0 source and associated dossier. Frozen access state: dossier_only. Observed 2026-10-23. https://datafiles.chinhphu.vn/cpp/files/vbpq/2025/9/156-vbhn-vpqh.pdf

[30] Ministry of Science and Technology, Vietnam. 2026. Decree 37: Digital technologies in quality management and traceability. Locator: Frozen release 0.1.0 source and associated dossier. Frozen access state: opened. Official explanation; decree full text was not rechecked. Displayed publication date is 2026-01-24; URL contains an August timestamp. Observed 2026-10-23. https://mst.gov.vn/nghi-dinh-37-ung-dung-cong-nghe-so-trong-quan-ly-chat-luong-va-truy-xuat-nguon-goc-197260812204117614.htm

[31] European Commission. 2026. The Digital Product Passport Registry is now live. Locator: Commission announcement, 20 July 2026. Supplementary official indexed announcement; no live service test. Observed 2026-10-25. https://single-market-economy.ec.europa.eu/news/digital-product-passport-registry-now-live-2026-07-20_en

[32] European Parliamentary Research Service. 2026. European product act: pre-initiative briefing. Locator: New Legislative Framework, market surveillance and standardisation tracks. Official institutional analysis dated 17 June 2026; used for package context, not current legal status. Observed 2026-10-25. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI%282026%29789349

[33] EUR-Lex / European Union. 2026. Procedure 2026/0307/COD: COM(2026)780 final, European standardisation. Locator: Commission adoption of legislative proposal on 6 October 2026. Official indexed procedural record; direct opening unavailable. Proposal identity and date verified; no full proposal clause analysis. Observed 2026-10-25. https://eur-lex.europa.eu/procedure/EN/2026_307

[34] European Parliament, Legislative Observatory. 2026. 2026/0307(COD): Standardisation Regulation. Locator: Status and key event 6 October 2026, COM(2026)0780. Official indexed procedure; latest retrieved state is preparatory phase in Parliament. Observed 2026-10-25. https://oeil.europarl.europa.eu/oeil/en/procedure-file?reference=2026%2F0307%28COD%29

[35] European Commission. 2026. Competitiveness implementation tracker. Locator: Proposed standardisation update; planned product-framework and market-surveillance reforms. Official indexed tracker; elapsed Q3 target retained as a planning record, not assumed completed. Observed 2026-10-25. https://commission.europa.eu/priorities-2024-2029/competitiveness/implementation-tracker_en

[36] GS1. GS1 Digital Link URI Syntax 1.7.0. Baseline access: opened. Observed 2026-10-23. https://ref.gs1.org/standards/digital-link/uri-syntax/

[37] CEN-CENELEC. EN 18219:2026 catalogue. Baseline access: dossier-only. https://standards.cencenelec.eu/ords/f?cs=14DC1F74D7E9F9DD3EA30959F19526334&p=205:110:::::FSP_PROJECT:79954

[38] CEN-CENELEC. EN 18220:2026 catalogue. Baseline access: dossier-only. https://standards.cencenelec.eu/ords/f?cs=1EEB1FD069281C804EC0A5EEDB8295A77&p=205:110:::::FSP_PROJECT:80081

[39] RAIN Alliance. RAIN DPP identifier encoding guidance. Baseline access: opened. Observed 2026-10-23. https://docs.therainalliance.org/dpp/

[40] UNECE / UN/CEFACT. UNTP DPP working specification. Baseline access: opened. Observed 2026-10-23. https://untp.unece.org/docs/specification/product-passport/

[41] UNECE / UN/CEFACT. UNTP documentation versions. Baseline access: opened. Observed 2026-10-23. https://untp.unece.org/versions/

[42] CIRPASS-2. CIRPASS-2 DPP ontologies documentation. Baseline access: unavailable. https://cirpass-2.github.io/ontologies-docs/

[43] CIRPASS-2. CIRPASS-2 project outputs. Baseline access: opened. Observed 2026-10-23. https://cirpass2.eu/project-results/

[44] CIRPASS-2 / Zenodo. CIRPASS-2 D4.1 Reference Architecture. Baseline access: dossier-only. https://zenodo.org/records/20720002

[45] International Electrotechnical Commission. 2023. IEC 63278-1:2023: Asset Administration Shell for industrial applications—Part 1: Asset Administration Shell structure. Edition 1.0, published 14 December 2023. Formal international-standard status does not establish deployment prevalence or the normative status of every AAS extension. Official catalogue opened; full paid standard not accessed in this check. Observed 2026-10-25. https://webstore.iec.ch/en/publication/65628

[46] Industrial Digital Twin Association. DPP4.0 using the Asset Administration Shell. Baseline access: dossier-only. https://industrialdigitaltwin.org/dpp4-0

[47] Catena-X. Catena-X CX-0143 DPP standard. Baseline access: dossier-only. https://catenax-ev.github.io/docs/Io/standards/CX-0143-UseCaseCircularEconomyDigitalProductPassportStandard/introduction

[48] GS1. EPCIS Standard 2.0. Baseline access: dossier-only. https://ref.gs1.org/standards/epcis/

[49] UNECE / UN/CEFACT. UNTP technical specifications. Baseline access: dossier-only. https://untp.unece.org/docs/specification/

[50] Global Battery Alliance. GBA 2026 battery passport trials. Baseline access: unavailable. https://www.s2.globalbattery.org/2026-battery-passport-pilots/

[51] Battery Pass. BatteryPass-Ready test environment update. Baseline access: unavailable. https://thebatterypass.eu/news/batterypass-ready-test-environment-update-new-features-for-improved-battery-passport-preparation/

[52] World Wide Web Consortium. 2026. Verifiable Credentials Working Group Charter. Charter period 11 March 2026 to 31 March 2028. Locator: Tentative deliverables; success criteria. Primary source inspected for the version 1.0 manuscript supplement; frozen release 0.1.0 remains unchanged. Observed 2026-10-25. https://www.w3.org/2026/03/vc-wg-charter.html

[53] World Wide Web Consortium. 2026. VC DPP & Business Wallet task force. Official group directory. Locator: Parent group; facilitators. Primary source inspected for the version 1.0 manuscript supplement; frozen release 0.1.0 remains unchanged. Observed 2026-10-25. https://www.w3.org/groups/tf/vc-dbw/

[54] W3C VC DPP & Business Wallet task force. 2026. VC DPP and Business Wallet document repository. Working repository; document maturity varies. Locator: Document index. Primary source inspected for the version 1.0 manuscript supplement; frozen release 0.1.0 remains unchanged. Observed 2026-10-25. https://w3c.github.io/vc-dpp-bw/

[55] W3C VC DPP & Business Wallet task force. 2026. Vocabulary use cases and requirements. Task-force work in progress; not formally reviewed or endorsed by the Working Group. Locator: Authored status; organisational identity and delegation use cases. Primary source inspected for the version 1.0 manuscript supplement; frozen release 0.1.0 remains unchanged. Observed 2026-10-25. https://w3c.github.io/vc-dpp-bw/ucr/

[56] WE BUILD Consortium. WE BUILD D4.1 architecture blueprint. Baseline access: dossier-only. https://webuild-consortium.github.io/wp4-architecture/blueprint/blueprint.html

[57] UN/CEFACT. 2026. Digital Identity Anchor. UNTP work in progress; pre-production pilot guidance. Locator: Relationship to W3C Recognized Entities; identity binding. Primary source inspected for the version 1.0 manuscript supplement; frozen release 0.1.0 remains unchanged. Observed 2026-10-25. https://untp.unece.org/docs/specification/DigitalIdentityAnchor/

[58] CEN-CENELEC. DPP horizontal standards overview. Baseline access: opened. Observed 2026-10-23. https://www.cencenelec.eu/news-events/news/2026/en-in-the-spotlight/2026-07-15-dpp/

[59] CEN-CENELEC. EN 18239:2026 catalogue. Baseline access: unavailable. https://standards.cencenelec.eu/ords/f?cs=1C97AB3E731BCF82E3BD2A04D9D8DC8CD&p=205:110:::::FSP_PROJECT:81494

[60] CEN-CENELEC. EN 18246:2026 catalogue. Baseline access: unavailable. https://standards.cencenelec.eu/ords/f?cs=1C627F97280D3E45FBBBED053BCCA88A9&p=205:110:::::FSP_PROJECT:81495

[61] European Union. Commission Implementing Decision (EU) 2026/1736. Baseline access: unavailable. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32026D1736

[62] European Commission. DPP harmonised standards register. Baseline access: opened. Observed 2026-10-23. https://single-market-economy.ec.europa.eu/single-market/goods/european-standards/harmonised-standards/digital-product-passport-dpp_en

[63] ISO. ISO/IEC AWI 25534-1 catalogue. Baseline access: opened. Observed 2026-10-23. https://www.iso.org/standard/90652.html

[64] ISO. ISO/IEC AWI 25534-2 catalogue. Baseline access: opened. Observed 2026-10-23. https://www.iso.org/fr/standard/95289.html?browse=tc

[65] SAMR / SAC. National standard project 20251568-T-469: DPP — General requirements. Baseline access: opened. Observed 2026-10-23. https://std.samr.gov.cn/gb/search/gbDetailed?id=1CB92886179AEDB9E06397BE0A0A064B

[66] CEN-CENELEC. 2026. CEN/CLC/JTC 24 Digital Product Passport framework and system. Business Plan, 6 March 2024. Horizontal framework and system; sector-specific product content excluded. Observed 2026-10-25. https://standards.cencenelec.eu/BPCEN/3342699.pdf

[67] DIN and DKE / VDE. 2026. Global Standards for the Digital Product Passport. Primary announcement, 20 April 2026, of ISO/IEC JTC 5 Digital Product Passport; first results expected from 2028, not a publication guarantee. Observed 2026-10-25. https://www.vde.com/en/press/press-releases/din-dke-jtc-5-product-passport

[68] Grimm, S.; Rimaz, H.; Wenzel, K.; Schoesau, M.; Li, W.; Zanini, P.; Neumann, A.; Coelho, S. G. 2026. An Improved RDF Representation of the Asset Administration Shell. Accepted manuscript, SemIIM/ISWC 2026 (scheduled 26 October 2026), 12 pp. User-supplied full PDF reviewed; URL is the public co-author announcement, not a DOI. Accessed 25 October 2026. Observed 2026-10-25. https://www.linkedin.com/posts/mhrimaz_an-improved-rdf-representation-of-the-aas-activity-7505301601750872064-l-x7

[69] Carolynn Bernier; Wan Li; Jesper Kuiper; et al. 2026. AAS/RDF Interoperability Approaches for DPP. Collaborative technical white paper, 21 pp. Revision history v1.3, 24 May 2026; matching archive deposited 26 May. Summary box retains v1.0. Version-specific DOI 10.5281/zenodo.20396377; attached-file MD5 matches the repository. No normative-standard status inferred. Locator: Sections 3–7; quote p. 17; recommendations p. 19. Full user-supplied PDF inspected; exact archive checksum and primary project listing verified. Observed 2026-10-25. https://zenodo.org/records/20396377

[70] Mohammad Hossein Rimaz. 2026. py-aas-rdf: representation, experimental branch and semantic-lifting design notes. Repository README reviewed 25 October 2026; mutable source. Proposed experimental representation expressly not yet official. Observed 2026-10-25. https://github.com/mhrimaz/py-aas-rdf

[71] State Administration for Market Regulation / Standardization Administration of China. 2024. National standard project 20243452-T-604: Asset Administration Shell for industrial applications—Part 1: Asset Administration Shell structure. Recommended national-standard project established 3 December 2024; under approval at observation, proposing identical adoption of IEC 63278-1:2023. No national deployment measurement. Locator: Project status and basic information; adoption section (采标情况). Official project record opened in full. Observed 2026-10-25. https://std.samr.gov.cn/gb/search/gbDetailed?id=28F53BF293F6A8D3E06397BE0A0AF10B

[72] Qingdao Binhai University. 2025. Participation in drafting the national standard for Asset Administration Shells for industrial applications [English translation of Chinese title]. Participant report dated 21 March 2025; describes establishment of SAC/TC124/SWG2 on 20–21 March and a remit covering multiple AAS specifications. The stated policy connection is the participant's account. Primary participant account inspected in full; machine-assisted interpretation of Chinese text. Not an independent measure of uptake. Observed 2026-10-25. https://qdbhu.edu.cn/News/Detail/14842

[73] Ministry of Industry and Information Technology / Standardization Administration of China. 2025. National Smart Manufacturing Standards System Construction Guide (2024 edition) [English translation]. Issued 7 March 2025 as document 60; official notice published 22 April 2025. Administration shells appear within a broader standards portfolio; the relevant passage does not identify IEC 63278 or a universal AI architecture. Locator: Printed p. 13; pp. 20–23. Official PDF and issuing notice inspected; machine-assisted interpretation of Chinese text. Observed 2026-10-25. https://www.miit.gov.cn/cms_files/filemanager/1226211233/attach/20253/694cbeb17a9b45b580c3602a6345723b.pdf

[74] State Administration for Market Regulation. 2022. Measures for the Administration of National Standards [English translation of Chinese title]. Order No. 59, dated 9 September 2022; effective 1 March 2023. Articles 25 and 29 provide for extension or termination of projects; Article 36 distinguishes mandatory and recommended standards. Locator: Articles 25, 29, 32 and 36. Official full text inspected; machine-assisted interpretation of Chinese primary text. Observed 2026-10-25. https://www.sac.gov.cn/xw/tzgg/art/2022/art_9c1b5873a12446f28e5a1117b375b28b.html

[75] State Administration for Market Regulation, Standards Technical Management Department. 2025. Notice on strict management of national-standard development cycles [English translation of Chinese title]. Notice dated 26 December 2024, published 3 January 2025. The development cycle ends at submission for approval; freezing and formal termination are separate procedural steps. Locator: Sections I–IV. Official full text inspected; machine-assisted interpretation of Chinese primary text. Observed 2026-10-25. https://www.samr.gov.cn/bzjss/tzgg/art/2025/art_6158ef3700f44a27bcd49f6cebec4930.html

[76] CESMII; Plattform Industrie 4.0; Labs Network Industrie 4.0; ZVEI and contributing organisations. 2024. US-German Digital Product Passport Demonstration. Issuer publication date 22 April 2024; ten-page project report. Describes prototypes and their participants; no national production-adoption measure. Catena-X contribution is specified for the battery example. Locator: Printed pp. 2–3, 6–7 and 10. Primary PDF, all 10 pages extracted and reviewed; issuer landing page opened. Observed 2026-10-25. https://lni40.de/wp-content/uploads/2024/04/US-German-DPP-PCF.pdf

[77] U.S. Department of Energy, Advanced Materials and Manufacturing Technologies Office. 2023. Department of Energy Continues Commitment to Smart Manufacturing Innovation by Renewing UCLA's Collaborative Ecosystems Smart Manufacturing Innovation Institute. Announcement dated 15 September 2023. Federal support concerns CESMII as an institute; no AAS-specific funding allocation or national architecture selection is established. Full primary announcement opened. Observed 2026-10-25. https://www.energy.gov/cmei/ammto/articles/department-energy-continues-commitment-smart-manufacturing-innovation-renewing

[78] National Institute of Standards and Technology. 2026. Digital Twins for Advanced Manufacturing. Created 15 April 2024; updated 20 July 2026. Programme research and laboratory implementation; scope does not constitute a complete national technology strategy. Full primary programme page opened; status ongoing as displayed on access date. Observed 2026-10-25. https://www.nist.gov/programs-projects/digital-twins-advanced-manufacturing

[79] Takuya Iijima; JEMIMA IEC TC65 Japanese National Committee. 2024. Overview of IEC 63278-1 Asset Administration Shell structure [Japanese], JEMIMA Report Vol. 61 No. 3. July 2024 issue, verified from the primary committee index. Participant account of Japanese contribution to IEC development; not a representative adoption study. Locator: 2024 Vol. 61 No. 3 entry and introduction; printed p. 17 in original issue. Primary national-committee index and full article introduction opened; the linked issue is explicitly labelled July 2024. Full PDF was indexed in previous review; direct PDF access limited by size. Observed 2026-10-25. https://www.jemima.or.jp/international-standardization/jncactivities/JNC-iectc65.html

[80] Robot Revolution & Industrial IoT Initiative (RRI), WG1/AG1. 2025. Release of the Japanese translation of the German Standardization Roadmap Industrie 4.0 Progress Report. Japanese translation issued to members in July 2025 and subsequently announced publicly. Evidence of organised dissemination; no Japanese government adoption of the German roadmap inferred. Primary release announcement opened; registration-gated translated report not downloaded. Observed 2026-10-25. https://www.jmfrri.gr.jp/library/library-6743/

[81] NEDO and NTT DATA Group. Demonstration of interconnection between the Battery Traceability Platform and Catena-X. Baseline access: opened. Observed 2026-10-23. https://www.nedo.go.jp/news/press/AA5_101831.html

[82] Korean Standards Association; Korean Agency for Technology and Standards. 2025. KS X IEC 63278-1: Asset Administration Shell for industrial applications—Part 1: Asset Administration Shell structure. Published 31 July 2025; IDT to IEC 63278-1:2023; KATS notice 2025-0177. National-standard adoption does not establish mandatory use or production penetration. Locator: Publication date, international-standard correspondence, announcing authority and history table. Primary catalogue metadata and scope opened in full; normative text not purchased or inspected. Observed 2026-10-25. https://www.kssn.net/search/stddetail.do?itemNo=K001010153517

[83] Ministry of SMEs and Startups, Republic of Korea. 2026. 2026 Manufacturing Data Standardization Programme: Call for reference-model development organisations, No. 2026-247 [Korean]. Ministry call dated 6 April 2026; applications through 24 April. Concerns manufacturing-data reference models, demonstrations and implementation support. Primary ministry notice opened; linked PDF download failed in web tool. Official Bizinfo summary independently opened for AAS eligibility, activities and funding ceiling. Observed 2026-10-25. https://www.mss.go.kr/site/smba/ex/bbs/View.do?bcIdx=1067009&cbIdx=310

[84] Korea Technology and Information Promotion Agency for SMEs (TIPA). 2026. Accelerating international-standard-based manufacturing-data model development to support SME manufacturing AI transformation [Korean]. Release dated 1 July 2026. Model-development counts are templates, not installed factories; the cumulative 500-model goal for end-2026 remains a target at the observation date. Full primary article body recovered in search index; direct open redirected to the agency English homepage. No independent programme evaluation or completed 2026 deliverable audit inspected. Observed 2026-10-25. https://www.tipa.or.kr/s040102/view/page/3/id/17527

[85] Ministry of Trade, Industry and Energy, Republic of Korea. 2024. Korea and Germany launch 1st Industrie 4.0 & Dataspace Forum. Ministry announcement dated 14 October 2024. Bilateral dataspace cooperation; standard sharing and mutual recognition are work objectives, not demonstrated completed outcomes. Primary ministry article indexed body inspected. Observed 2026-10-25. https://english.motie.go.kr/eng/article/EATCLdfa319ada/2070/view?bbsCdN=2&pageIndex=1

[86] European Commission. 2026. Commission Implementing Regulation (EU) 2026/1778. Locator: Articles 3, 4-6, 8, 9, 12, 19 and 24; OJ 17 July 2026. Supplementary official indexed legal text; direct requests challenged. Frozen dossier-only access state unchanged. Observed 2026-10-25. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32026R1778

[87] European Commission. 2026. The DPP Registry. Locator: Index, decentralised product data, technical semantic element, organisation enrolment and test environment. Public page opened; enrolment, testing and guide links inspected. No authenticated platform use or API test. Observed 2026-10-25. https://single-market-economy.ec.europa.eu/single-market/digital-product-passport/dpp-registry_en

[88] European Commission. 2026. DPP Registry User Guide for Economic Operators, version 1.03. Locator: Sections 6.2.1 and 6.2.2, pages 48 and 54; validation error on page 56. Official 63-page PDF opened; dated 16 September 2026 and linked on 25 October. May lag deployed service; no live transaction performed. Observed 2026-10-25. https://single-market-economy.ec.europa.eu/document/download/079a45e2-469f-4eec-b1e5-32e8e05d1357_en?filename=dpp_registry_user_guide_for_economic_operators.pdf

[89] Data Spaces Support Centre. 2026. DSSC Blueprint 3.0. Data Models and Publication and Discovery building blocks. Shared models/vocabulary services and offering catalogues are distinct functions. Public blueprint inspected; no deployment validation. Observed 2026-10-25. https://blueprint.dssc.eu/

[90] Roefs, D.; van Nieuwenhuijze, H.; Chawla, K.; Smeets, N.; Rongen, S.; Kuiper, J.; Rurup, R.; Bernier, C. 2026. Risks and mitigations: a companion to D4.1 Reference Architecture. Version 1.1, submitted/published 5 June 2026; document marked Draft. Full text verified against repository MD5 44a6593a78656709ad6ad6737d0813a2. Printed pages are PDF pages minus two. Internal front-matter dates differ; the version-specific deposit date is used. Access: full text inspected. Observed 2026-10-25. https://zenodo.org/records/20670585

[91] Stöcker, C. 2026. 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. Related author-affiliated architectural interpretation; not independent validation of the CIRPASS-2 report or this paper. Access: local full text available; cover and abstract inspected. Observed 2026-10-25. https://spherity.github.io/spherity-research/verifiable-access-controlled-digital-product-passports.html

[92] UN/CEFACT. 2026. Digital wallets. UNTP work-in-progress design guidance; pre-production pilots. Locator: Overview; enterprise wallets; access control. Primary source inspected for the version 1.0 manuscript supplement; frozen release 0.1.0 remains unchanged. Observed 2026-10-25. https://untp.unece.org/docs/design-patterns/DigitalWallets/

[93] World Wide Web Consortium. 2026. Recognized Entities v1.0. W3C Working Draft, 6 September 2026; experimental, not fit for production deployment. Locator: Status; Sections 2.4 and 3; informative ecosystem examples. Primary source inspected for the version 1.0 manuscript supplement; frozen release 0.1.0 remains unchanged. Observed 2026-10-25. https://www.w3.org/TR/2026/WD-vc-recognized-entities-1.0-20260906/

[94] UN/CEFACT. 2026. Digital Identity Anchor. UNTP version 0.7.0; pre-production pilot specification. Locator: Overview; conceptual model; requirements DIA-01 and DIA-05. Primary source inspected for the version 1.0 manuscript supplement; frozen release 0.1.0 remains unchanged. Observed 2026-10-25. https://untp.unece.org/docs/0.7.0/specification/DigitalIdentityAnchor/

[95] UN/CEFACT. 2026. About the GRID and DIAs. Supporting document; Stage 5 Deliverable Acceptance Check. Locator: Purpose; registrar-level directory and project status. Primary source inspected for the version 1.0 manuscript supplement; frozen release 0.1.0 remains unchanged. Observed 2026-10-25. https://grid.unece.org/docs/draft/About/

[96] World Wide Web Consortium. 2018. ODRL Information Model 2.2. W3C Recommendation, 15 February 2018. Locator: Sections 2 and 3: policies, rules, constraints and profiles. Primary source inspected for the version 1.0 manuscript supplement; frozen release 0.1.0 remains unchanged. Observed 2026-10-25. https://www.w3.org/TR/2018/REC-odrl-model-20180215/

[97] World Wide Web Consortium. 2018. ODRL Vocabulary and Expression 2.2. W3C Recommendation, 15 February 2018. Locator: Common vocabulary; actions, parties and constraints. Primary source inspected for the version 1.0 manuscript supplement; frozen release 0.1.0 remains unchanged. Observed 2026-10-25. https://www.w3.org/TR/2018/REC-odrl-vocab-20180215/

[98] Eclipse Foundation. 2026. Dataspace Protocol 2025-1. Stable specification; errata release 2025-1-err2, 11 September 2026. Locator: Catalogue; contract negotiation; transfer processes; authentication. Primary source inspected for the version 1.0 manuscript supplement; frozen release 0.1.0 remains unchanged. Observed 2026-10-25. https://eclipse-dataspace-protocol-base.github.io/DataspaceProtocol/2025-1-err2/

[99] Eclipse Foundation. 2025. Decentralized Claims Protocol. Version 1.0.1, 13 November 2025; page heading retains v1.0. Locator: Trust model; presentation protocol; scope exclusions. Primary source inspected for the version 1.0 manuscript supplement; frozen release 0.1.0 remains unchanged. Observed 2026-10-25. https://eclipse-dataspace-dcp.github.io/decentralized-claims-protocol/v1.0.1/

[100] Eclipse Dataspace Components contributors. 2026. Policy Engine. Eclipse Dataspace Components implementation documentation. Locator: Policy model; evaluation functions; execution scopes. Primary source inspected for the version 1.0 manuscript supplement; frozen release 0.1.0 remains unchanged. Observed 2026-10-25. https://eclipse-edc.github.io/documentation/for-adopters/control-plane/policy-engine/

[101] Eclipse Dataspace Components contributors. 2026. Connector v0.18.1. Software release, 25 September 2026. Locator: Release tag; implementation version for reproducible follow-up. Primary source inspected for the version 1.0 manuscript supplement; frozen release 0.1.0 remains unchanged. Observed 2026-10-25. https://github.com/eclipse-edc/Connector/releases/tag/v0.18.1

[102] UN/CEFACT. 2026. Decentralised Access Control. UNTP version 0.7.0; pre-production pilot specification. Locator: Public and protected access; authentication alternatives. Primary source inspected for the version 1.0 manuscript supplement; frozen release 0.1.0 remains unchanged. Observed 2026-10-25. https://untp.unece.org/docs/0.7.0/specification/DecentralisedAccessControl/

[103] UN/CEFACT. 2026. Identity Resolver. UNTP work-in-progress specification. Locator: Resource discovery and independent credential verification. Primary source inspected for the version 1.0 manuscript supplement; frozen release 0.1.0 remains unchanged. Observed 2026-10-25. https://untp.unece.org/docs/specification/IdentityResolver/

[104] Spherity Research. 2026. Release 0.1.0 checksum and reconstruction verification. Companion research package: releases/0.1.0-verification.json. 41 manifest-listed files and byte-identical frozen-input rebuild.

[105] Spherity Research. 2026. Global DPP Atlas explorer verification for release 0.1.0. Companion application: dpp-explorer/qa/QA-report.md. 24 interface-model tests and documented browser checks; no usability study.

[106] World Wide Web Consortium. 2012. OWL 2 Web Ontology Language Primer (Second Edition). W3C Recommendation, 11 December 2012. Locator: Section 2 What is OWL 2?. Primary W3C primer consulted for open-world semantics; not an implementation or conformity evaluation. Observed 2026-10-25. https://www.w3.org/TR/2012/REC-owl2-primer-20121211/

[107] World Wide Web Consortium. 2017. Shapes Constraint Language (SHACL). W3C Recommendation, 20 July 2017. Locator: Abstract; Sections 3.4 Validation and 3.5 Conformance Checking. Primary W3C specification consulted for graph validation and conformance scope. Observed 2026-10-25. https://www.w3.org/TR/2017/REC-shacl-20170720/

[108] Carsten Stöcker. 2026. From Trustworthy AI to Trusted, Operational Agentic Systems. Spherity Research. Locator: Trust infrastructure for agentic AI. Local research-page summary inspected; AI Service Passport is a proposed architecture. Country ratings are not adopted in this manuscript. Observed 2026-10-25. https://spherity.github.io/spherity-research/trusted-agentic-ai-china-eu-us-comparative-analysis.html

[109] Carsten Stöcker. 2026. PACE: Verifiable Safety and Cyber Evidence Graphs for Physical AI. Spherity Research topic page accompanying Verifiable Safety Assurance Evidence Graphs for Modular Humanoid Robot Arms. Locator: Robot Arm Reference Model; access-controlled VSAEG; sources and boundaries. Local topic-page summary inspected; proposed architecture and evaluation protocol, not adopted certification or measured commissioning improvement. Observed 2026-10-25. https://spherity.github.io/spherity-research/physical-ai-compliance-evidence-pace.html

[110] Carsten Stöcker. 2026. Governed Memory for Physical AI: Evidence Roles, Integrity and Revocation from Experience to Action. Spherity Research. Locator: Memory supply chain; revocation and physical recovery; results and limitations. Local research-page summary inspected; reported bounded protocol findings not reproduced. Robot behavioural evaluation and proposed BOM profiles remain distinct. Observed 2026-10-25. https://spherity.github.io/spherity-research/governed-robot-memory-physical-ai.html

[111] Carsten Stöcker. 2026. AI Agent Revocation and Containment in Multi-Agent Systems. Spherity Research overview of an executive brief and two technical papers. Locator: Receiving boundary; containment and harm; pilot and acceptance tests. Local series overview inspected; conditional and bounded protocol evidence, not production containment validation. Observed 2026-10-25. https://spherity.github.io/spherity-research/ai-agent-revocation-containment-multi-agent-systems.html

[112] Carsten Stöcker. 2026. Risk-Bounded Runtime Assurance for Dynamic Multi-Agent Systems under Partial Observation. Spherity AI Safety Series, Paper 2. Locator: Authority and assurance; persistent episode risk; evaluation evidence and limits. Local summary inspected; conditional/synthetic findings, not measured field safety or a stopping guarantee. Observed 2026-10-25. https://spherity.github.io/spherity-research/risk-bounded-runtime-assurance-multi-agent-systems.html

[113] The White House. 2025. White House Unveils America's AI Action Plan. Released 23 July 2025. Strategic policy direction; no comparative assessment of AAS or measured technology outcome. Official release opened in full; underlying plan additionally indexed. Observed 2026-10-25. https://www.whitehouse.gov/releases/2025/07/white-house-unveils-americas-ai-action-plan/

[114] Ministry of Industry and Information Technology and seven other Chinese authorities. 2025. Implementation Opinions on the Special Action for AI Plus Manufacturing [English translation of Chinese title]. Notice dated 25 December 2025; published 9 January 2026. Describes policy targets and intended work, not completed deployments or rejection of AAS. Locator: General requirements; Sections II(1)-(3), IV(9)-(11), VI(15)-(16). Official National Data Administration republication inspected in full; machine-assisted translation of Chinese primary text. Observed 2026-10-25. https://www.nda.gov.cn/sjj/zwgk/zcfb/0112/20260107214358696030895_pc.html

[115] CESMII. 2026. CESMII Releases i3X 1.0: A Complete, Implementation-Ready Open API Specification for Manufacturing Interoperability. Consortium API specification, version 1.0, announced 18 June 2026; distinct from an IEC or ISO International Standard. The announcement does not measure operational adoption. Official article indexed text read; direct open timed out. Date corroborated by official CESMII archive page. Stable 1.0 status corroborated by official GitHub repository. Observed 2026-10-25. https://www.cesmii.org/cesmii-releases-i3x-1-0/

[116] Carsten Stöcker. 2026. Private Verification of Action Eligibility across Trust Domains. Spherity AI Safety Series, Paper 3. Locator: Eligibility semantics; reference architecture; evidence and limits. Local summary inspected; proposed cross-domain protocol with reported finite/plaintext evaluation, not a deployed private-proof system. Observed 2026-10-25. https://spherity.github.io/spherity-research/private-verification-action-eligibility-trust-domains.html