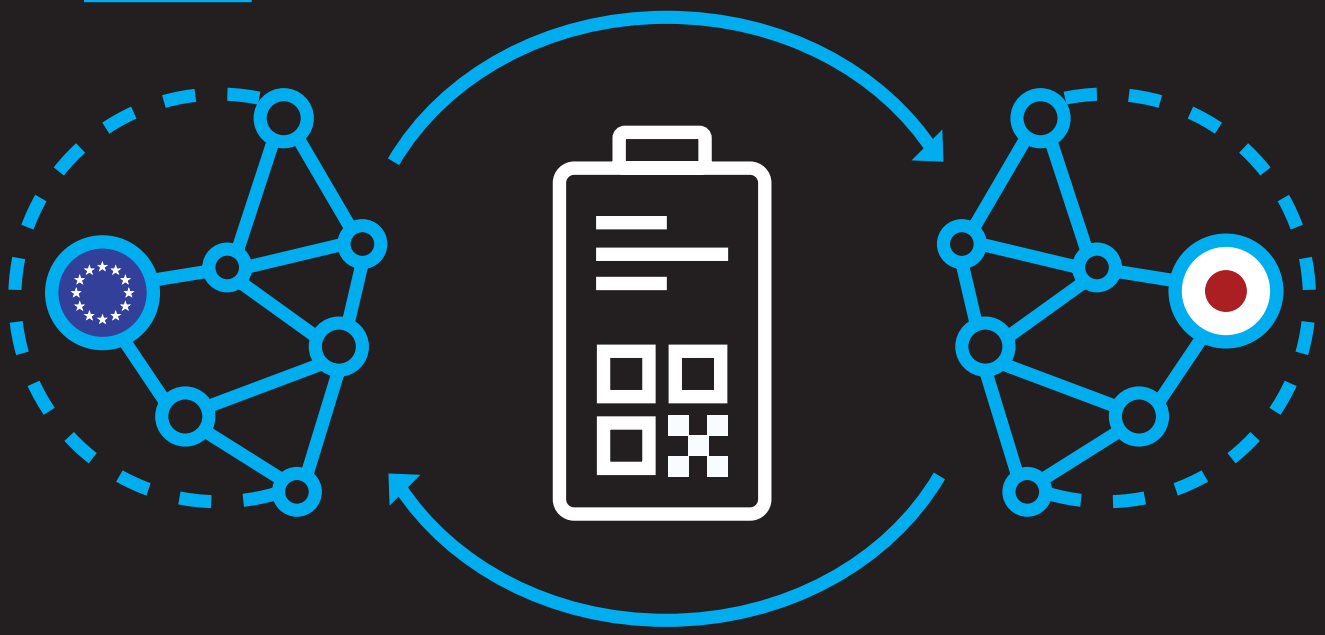
INTERNATIONAL DATA SPACES ASSOCIATION

Position Paper | Version 1.0 | Sep 2026

Trust Anchor Federation for International Data Spaces

Evidence from an EU-Japan Battery Passport Data Exchange



- ○ Position Paper of members of the IDS Association
- ○ Position Paper of bodies of the IDS Association
- ● Position Paper of the IDS Association
- ○ White Paper of the IDS Association

Publisher

International Data Spaces Association
Emil-Figge Straße 80
44227 Dortmund
Germany

Editor

Christoph Schlueter Langdon, T-Systems
Takahide Matsutsuka, Fujitsu
Christoph Mertens, IDSA

Cite as

Schlueter Langdon C. et al., Trust Anchor Federation for International Data Spaces, Evidence from an EU-Japan Battery Passport Data Exchange, International Data Spaces Association, September 2026

Authors & contributors

Yawen Huang, DENSO CORPORATION
Takahide Matsutsuka, Fujitsu
Sebastian Steinbuss, IDSA
Akira Sakaino, NTT DOCOMO BUSINESS, Inc.
Christoph Schlueter Langdon, T-Systems

Disclaimer

The views expressed in this paper are those of the individual authors and do not necessarily reflect the positions of their organizations.

Contributing organizations

DENSO CORPORATION
Fujitsu
NTT DOCOMO BUSINESS, Inc.
T-Systems

Table of Contents

List of Figures

1 Purpose and background

AI-readiness, digital twins, and compliance with sustainability and product passport regulation require companies to exchange data across company boundaries and jurisdictions with IP protection. Fortunately, decentralized data space technology has emerged as a response to this critical business need. As international data spaces continue to expand, establishing trust has become an indispensable requirement. At the same time, trust today remains fragmented across regions and institutional frameworks. In many non-European regions in particular, trust anchors aligned with data space requirements have yet to be put in place.

Think of a regular passport: countries accept it not because they know the traveler, but because they recognize the issuing government as a trust anchor. Data spaces need the same cross-border recognition for companies and AI agents. As AI technologies become more widely adopted, ensuring the trustworthiness of AI agents has emerged as a critical issue (Turkmayali, 2026).

This paper reports on a multi-company initiative that builds on last year's prototype, which established an initial milestone for cross-ecosystem interaction by extending data space network-layer capabilities with federated identity and trust management (Mertens, 2025); the new work expands this stack toward EU–Japan data exchange for a battery passport application and leverages Japan's gBizID system on a trial basis. This paper reveals how a data consumer in Europe can use data from a data provider in Japan for a battery passport application to comply with EU Battery Regulation (European Parliament & Council of the European Union, 2023). It should be noted that the scope of trust addressed in this paper is specifically Identity Trust — that is, trust in the existence and authenticity of entities.

2 Problem definition and gaps in Japan

Building on our experience with global interoperability, roaming, and trusted network operations, the previous milestone showed how data spaces can scale sovereign, secure, and interoperable data exchange across countries and industries. To make the interoperability challenge actionable, the IDSA's 3-layer stack was utilized to separate the key issues (Guggenberger et al., 2025): data space networks for trusted peer-to-peer transactions, a data products layer for standardized reusable data assets, and applications for business use-case automation. Figure 1 illustrates the overall system stack of a data ecosystem. The pilot focused on the data space network layer, especially identity, trust, governance, and data space core services, where interoperability depends on mutual recognition of trust anchors and aligned protocols such as Decentralized Claims Protocol (DCP) and Data Space Protocol (DSP) (Castellvi, 2026). In this context, T-Systems and NTT connected European and Japanese trust environments as an experimental "network of networks" and foundation for cross-border data commerce in global supply chains.

However, mutual trust between different trust anchors does not arise automatically — a challenge that must be directly addressed. While Europe has established institutional trust frameworks such as eIDAS, Japan lacks any unified trust anchor mechanism dedicated to data spaces, although existing identity infrastructures such as gBizID can serve this role on a trial basis (see Section 4.1). As a result, the interoperability of trust anchors has emerged as a fundamental challenge in enabling international data space interoperability.

This challenge is contingent on differences in each country's legal system and existing infrastructure, as well as differences in the party responsible for trust assurance (i.e., who bears accountability for trust). Rather than converging on a single trust model, it is therefore necessary to design for the federation of diverse trust models.

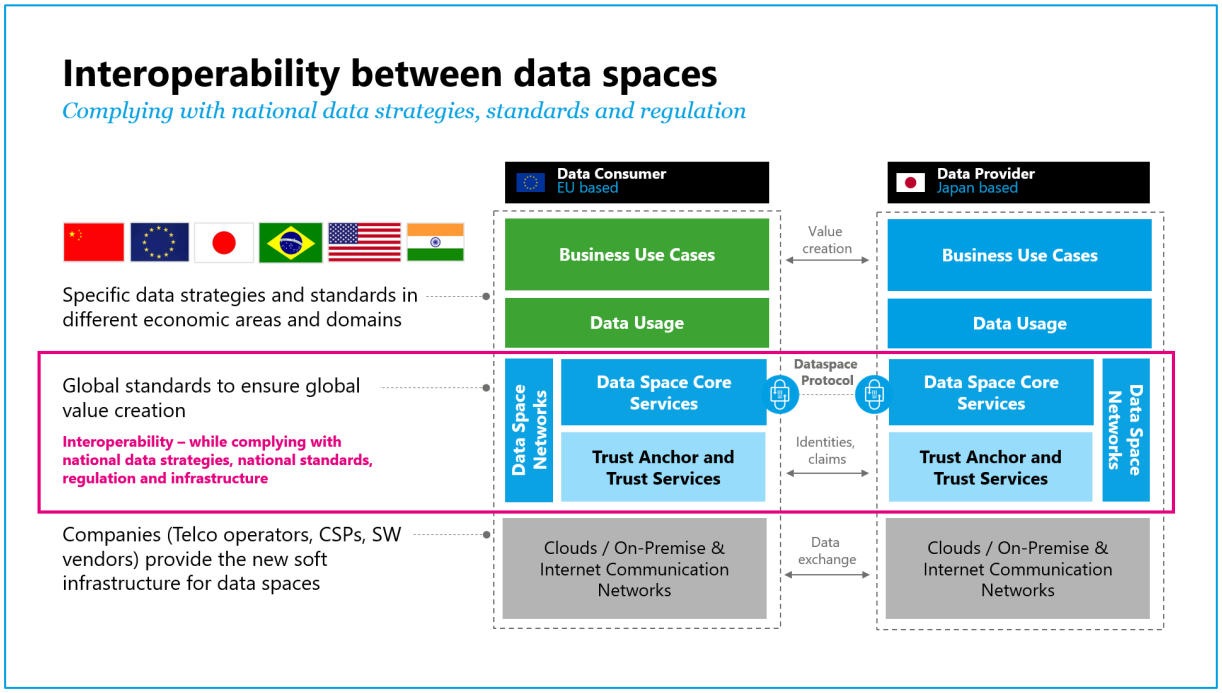


Figure 1: Data ecosystem stack

3 The battery passport use case

The battery passport use case is a compelling showcase for demonstrating trust interoperability. As the world accelerates its transition toward electrification and carbon neutrality, batteries are becoming a core enabler of this transformation. At the same time, the significant value embedded in used batteries — particularly their potential for second-life applications and resource recycling — has not been fully realized. One fundamental barrier has persisted for years: information asymmetry.

When used batteries enter the market, reliable data on product specifications, chemical composition, usage history, and state of health (SoH) is often not sufficiently shared. As a result, buyers must independently evaluate and analyze each battery, while the reliability and comparability of the available data remain limited. This has led to situations in which batteries that could still be reused are undervalued, heavily discounted, or prematurely discarded.

To address this challenge, the EU Battery Regulation (Regulation (EU) 2023/1542; European Parliament & Council of the European Union, 2023) requires the introduction of a digital battery passport for applicable batteries starting on February 18, 2027. A battery passport is a digital mechanism for managing and sharing key battery information. It is intended to serve as an essential foundation for transparency, traceability, and the circular economy.

Its greatest commercial value lies in transforming batteries from "black-box assets with limited information and uncertain value" into "energy assets that can be assessed and

traded based on trusted information." In doing so, the battery passport can unlock latent value across the entire battery value chain.

To achieve this impact, a battery passport must satisfy four key requirements. Figure 2 summarizes how each is supported by the EU Battery Regulation and related standardization efforts.

- **Accuracy of dynamic data.** The EU Battery Regulation requires information that changes during use, such as SoH, to be updated continuously. In particular, Article 77 and Annex XIII outline the information to be included in the battery passport and the approach for keeping that information up to date.
- **Interoperability.** Because battery passports are expected to be used across companies, industries, and regions, data must be understandable and exchangeable across different systems. To support this, European standards and data models related to battery passports are being developed and refined.
- **Confidentiality and access control.** A battery passport includes not only publicly accessible information but also information that should be available only to stakeholders with a legitimate interest. Therefore, access to information must be appropriately controlled based on each user's role and authorization level.
- **Trustworthiness & verifiability.** For battery passport information to be used with confidence in the market, data provenance, tamper resistance, and verifiability must be ensured. Relevant regulatory provisions and technical standards to support these capabilities are currently being developed.

These requirements and regulatory urgency make the battery passport a representative trust-interoperability challenge and an instructive application for developing and demonstrating our solution.

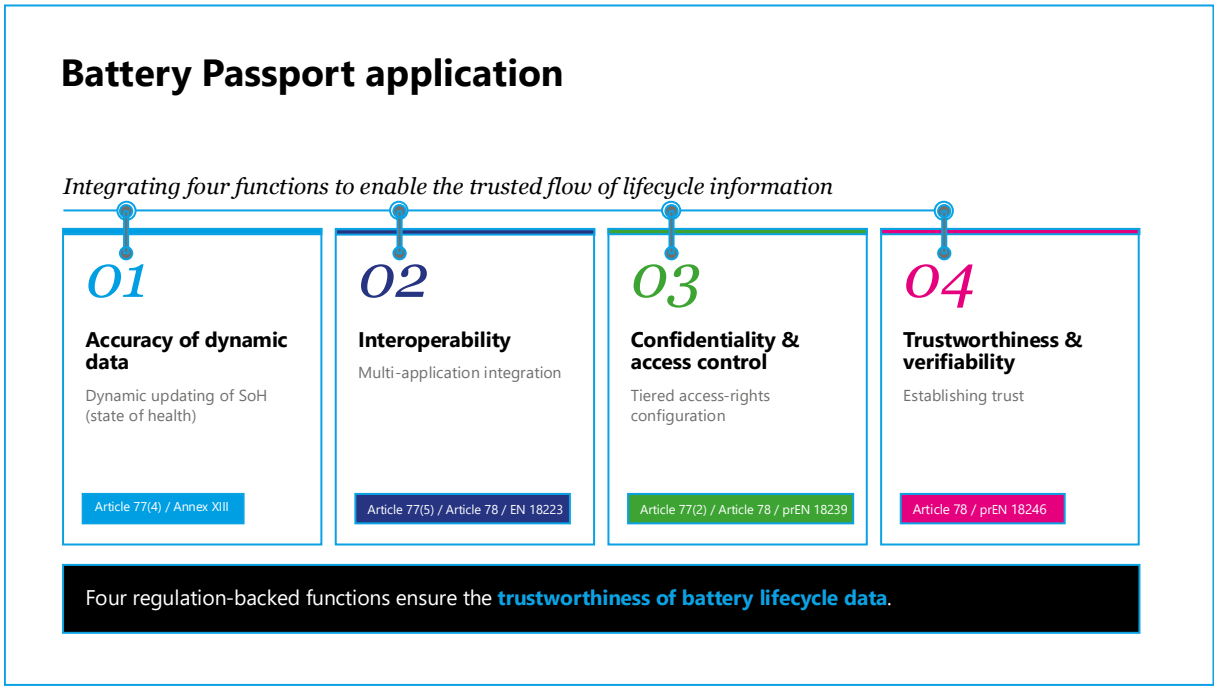


Figure 2: Battery passport — enabling trusted lifecycle data flow

4 Approach and demonstration

Of the four requirements in Figure 2, this Proof of Concept (PoC) focuses on the Identity-Trust foundation underpinning them, in line with the scope defined in Section 1.

4.1 gBizID: the building block leveraged in this PoC

gBizID is a unified authentication infrastructure for electronic administrative procedures operated by Japan's Digital Agency, enabling an enterprise to access multiple government application systems with a single account (Digital Agency, 2026). Its top-tier "gBizID Prime" account confirms that the holder is the company's legal representative (or the individual proprietor), with identity verification performed either through a document-based mail application or through an online application that reads the My Number Card via the gBizID app; the Corporate Number (法人番号) is retained as an account attribute (Digital Agency, 2026).

Because the existence and authenticity of the representative are verified by the government in this way, gBizID can serve as an authoritative, government-backed trusted data source for attesting to the identity of Japanese companies. National policy positions gBizID as a component of Japan's Digital Public Infrastructure and, in light of trust-related discussions under the Ouranos Ecosystem, envisions expanding its use to private-sector authentication (Digital Agency, 2025a). This PoC was itself conducted as part of the Digital Agency's FY2025 public call for private-sector use cases of gBizID and associated trial connection experiments (Digital Agency, 2025b).

4.2 Participants

This PoC was conducted jointly by four organizations, DENSO CORPORATION (hereinafter, referred to as "DENSO"), Fujitsu Limited, NTT DOCOMO BUSINESS, Inc., and T-Systems. Each participant assumed the following role.

DENSO

DENSO contributed a battery passport application built to comply with the regulatory and digital standards of multiple countries, leveraging blockchain technology to ensure tamper-resistant data propagation. The application was enhanced to display the trust information of counterpart companies, including their Corporate Number and the trust anchor from which it was obtained, at the time of data exchange, and was used to conduct data exchange between Japanese and European companies via the data space.

Fujitsu

Fujitsu served as the Verifiable Credential (VC) issuing entity responsible for attesting to the existence and identity of companies, functioning as the Notary in the Gaia-X architectural framework though not as a Gaia-X-accredited Notary service, using its IDYX-TI technology. By leveraging gBizID as a trusted data source — specifically through the login authentication result and the associated Corporate Number — Fujitsu established a mechanism to assure the authenticity of Japanese companies and issue VCs compliant with the Gaia-X specification. This represented the first instance in Japan of VCs for Japanese companies being generated using gBizID as a trusted data source.

NTT DOCOMO BUSINESS

NTT DOCOMO BUSINESS deployed the open-source software of the Gaia-X Digital Clearing House (GXDCH) on a cloud environment, providing VC verification functionality (Compliance Check) through the Gaia-X Registry and Gaia-X Compliance components. In this proof of concept, this environment was configured to simulate and interconnect with trust services in Europe and other regions.

T-Systems

T-Systems, a key developer of open-source data space software, provided the infrastructure through its Build & Operate Dataspace-as-a-Service environment, based on Eclipse Tractus-X and aligned with Gaia-X requirements, together with data space connectors, or "data phones," with the first-ever IDSA-certified EDC. This setup enables connectivity with European data space participants and serves as the integration layer between the Japanese and European sides of the proof of concept.

4.3 PoC experiment

This PoC extended its scope beyond demonstrating Japanese company participation in a data space by using a battery passport application to showcase how business users can exchange and consume information across borders. Figure 3 applies the generic three-layer architecture introduced in Figure 1 to the specific PoC, showing its key components and major workflows. Specifically, the PoC demonstrated a cross-border data exchange scenario within a global battery supply chain, in which a European battery reuse and recycling operator required battery information from a Japanese battery manufacturer in order to comply with regulatory requirements and support battery lifecycle management.

From the perspective of the business user, the interaction takes place entirely through the battery passport application rather than through direct operation of data space components. The data consumer searches for the required battery information, submits a request through the application, and receives the requested information once access conditions have been satisfied. The application presents the exchanged battery information together with trust-related metadata regarding the counterparty organization. This includes information such as the organization's corporate identifier and the trust anchor through which its identity was verified. Such information enables users to understand not only the content of the data but also the basis on which the data provider's identity has been authenticated.

The demonstration further addressed one of the practical challenges currently faced in cross-border data space adoption. Companies participating in different regional data spaces often use different trust frameworks, communication protocols, interfaces, and data models. As a result, exchanging information across data spaces typically requires technical expertise and integration effort. In this PoC, the battery passport application acted as an intermediary layer that simplified this complexity for business users. Companies could continue using their existing national trust systems and regional data spaces while interacting through a unified application experience. The application handled interoperability-related functions and enabled data exchange between Japanese and European participants without requiring users to understand the underlying trust and data space infrastructure.

The scenario demonstrated that the value of trust federation extends beyond technical interoperability. For business users, it enables trusted cross-border collaboration with organizations that may not have a direct contractual relationship. Before exchanging battery-related information, the participating organizations were able to verify the existence and authenticity of their counterparties through the federated trust framework. This reduces onboarding friction, increases confidence in exchanged information, and supports regulatory use cases such as the battery passport envisioned under the EU Battery Regulation.

It should be noted that, due to constraints inherent to the gBizID PoC program, a test environment rather than the production environment was used for the VC-issuance integration trial.

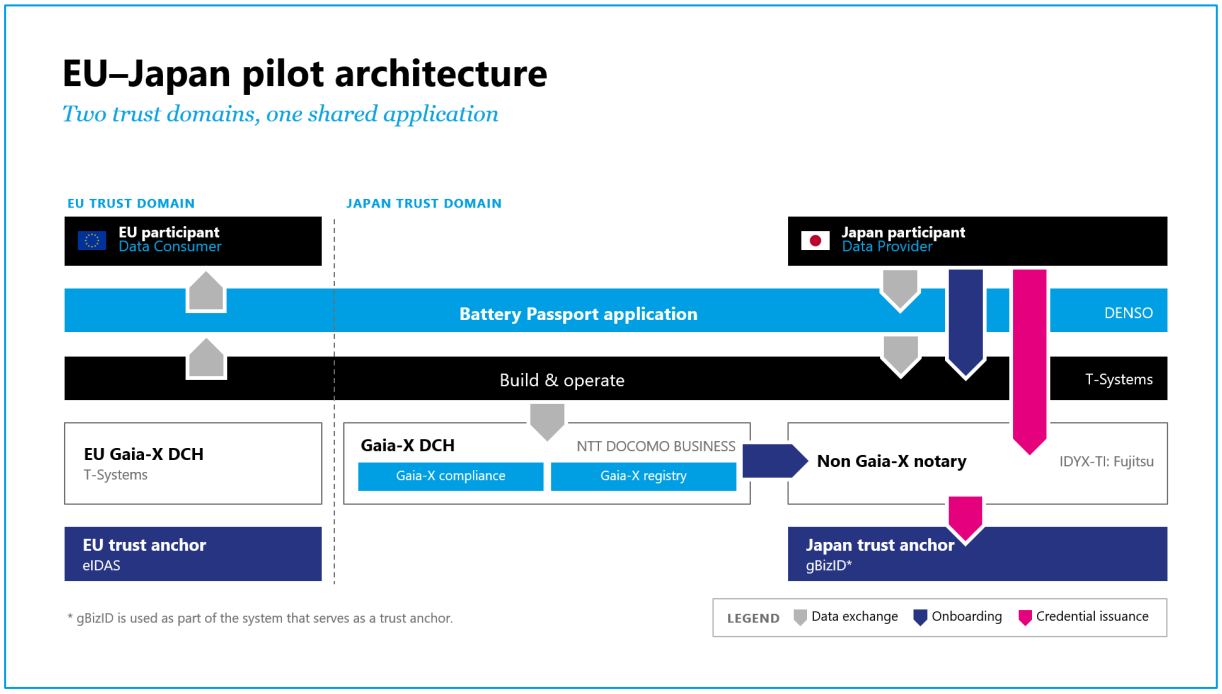


Figure 3: PoC architecture

The outcomes of this proof of concept were disseminated through a poster exhibition at Data Spaces Week 2025 (October 2025, Japan), a collaborative Federated Trust demonstration with International Manufacturing-X at Smart Production Solutions 2025 (November 2025, Germany), and a joint presentation by all four organizations at Hannover Messe 2026 hosted by IDSA and the OPC Foundation (April 2026, Germany).

5 Implications and generalizations from the PoC

The PoC demonstrated that, from a technical standpoint, federation between different trust anchors is feasible. At the same time, the current integration relies heavily on bilateral coordination and specific components (e.g., GXDCH) and is progressing toward a configuration that is both generalizable and scalable. It should be noted that this reliance reflects a practical choice made to integrate with existing, already-operational components (IDYX-TI and GXDCH) rather than a requirement imposed by the underlying protocols themselves — the Decentralized Claims Protocol (DCP) used in this PoC does not itself mandate third-party verification (Eclipse Dataspace Working Group, 2025).

The fundamental challenge, therefore, lies not in the implementation of individual technologies, but in how to design and delineate the relationships between trust anchors and the role of the verification and trust mediation layer. The verification entity is not limited to a specific component; multiple forms are conceivable, including the data consumer, a Clearing House, or a data space governance body such as the Catena-X Association for the automotive industry. The Catena-X Association itself serves as a concrete example of a governance body that operationalizes a trust framework — demonstrating that verification mechanisms need not be confined to dedicated components. From these perspectives, it is important to abstract the verification mechanism as a defined role rather than binding it to a specific technology.

Furthermore, the gBizID-based approach demonstrated in this PoC can be positioned as a lightweight trust construction methodology that leverages existing identity infrastructure to assure entity authenticity in countries and regions where trust anchors have not yet been established. This concept is generalizable as one implementation pattern for non-European regions.

6 Recommendations and conclusions

Realizing international data space interoperability requires standardization that presupposes federation between trust anchors. In this context, rather than converging on a single trust model, the design must accommodate interoperability across different trust models. The verification and trust mediation layer, in particular, requires abstraction and standardization that are not tied to specific implementations, so that an appropriate verification mechanism can be selected and applied according to the characteristics of each data space.

Ultimately, what international interoperability requires is not a single, universally mandated trust implementation, but a shared, abstract vocabulary for trust — common enough to enable mutual recognition across data spaces, yet flexible enough to accommodate the differing legal systems, accountability structures, and institutional arrangements of individual countries and regions. Standardization efforts should therefore prioritize this abstraction layer over the standardization of any single implementation, so that national and regional trust ecosystems can retain the autonomy to realize it in ways consistent with their own institutional context and sovereignty.

This direction resonates with several ongoing efforts to define trust as an independent, implementation-agnostic layer. Open Data Spaces (ODS), for instance, treats trust as an independent "Trust by Design" perspective in its reference architecture (IPA, 2026b), and its Identity & Trust (L3) protocol allows verification roles to be performed by separate parties under federation, treats Verifiable Credentials as an optional cross-data space extension, and requires federated subject identifiers to remain issuer-identifiable (IPA, 2026a). A more structural example of this separation between a common abstraction layer and sovereign implementation can be found in the EU's own eIDAS 2.0 framework: while the European Digital Identity Architecture and Reference Framework (ARF) mandates a common technical architecture and interoperability requirements across all Member States (European Parliament & Council of the European Union, 2024), the issuance and operation of each national EU Digital Identity Wallet — and its integration with pre-existing national identity infrastructure — remains the responsibility of individual Member States. This framework itself remains under active rollout, with Member States progressively deploying wallets and implementing acts continuing to be finalized through 2026. Realizing genuine convergence

around abstracting the verification mechanism as a role, rather than a fixed component, will likely require sustained technical and institutional coordination between these efforts over time — building on, and moving beyond, the bilateral, component-dependent integration demonstrated in this PoC (Section 4).

On this basis, the gBizID-type approach demonstrated here — leveraging an existing identity infrastructure, operating under the jurisdiction and sovereignty of the country in question, to attest to the existence and authenticity of an entity — can be positioned as a practical reference model for non-European regions. What is generalizable is not that such infrastructure must be state-operated, nor the specific credential format used to convey this attestation in the PoC, but the underlying function it performs: supplying an Identity Proofing capability, rooted in a trust basis that each country or region determines for itself, that a federated trust framework can draw upon regardless of which specific protocol or credential technology ultimately carries that attestation between parties. Realizing it at scale makes the standardization of assurance levels (e.g., IAL) and the development of mutual-recognition mechanisms across heterogeneous trust anchors key agenda items. Such trust infrastructure is expected to grow in significance as a foundational layer supporting requirements such as data provenance and accountability in the context of AI adoption.

Going forward, it will be imperative to advance trust technologies in coordination with initiatives such as International Manufacturing-X, design for cross-border data space interoperability from the outset, and reuse data space trust services for AI agents (Turkmayali, 2026, Table 1, pp. 10–11) to build toward international mutual recognition spanning legal entities, individuals, machines, robots, and physical AI systems.

References

1. Castellvi, S. (2026). Data Spaces Standardization Landscape – Europe and International. Position Paper Version 2.0 (May). International Data Spaces Association. https://doi.org/10.5281/zenodo.20849314

2. Digital Agency. (2025a). デジタル社会の実現に向けた重点計画（令和7年6月13日閣議決定）[Priority Policy Program for the Realization of a Digital Society]. https://www.digital.go.jp/policies/priority-policy-program

3. Digital Agency. (2025b). 令和7年度GビズIDの民間サービスでの活用事例等の募集及び実証的接続実験の実施に関する公募を開始しました [Launch of the FY2025 call for private-sector use cases of gBizID and proof-of-concept connection experiments]. https://www.digital.go.jp/news/03066d23-6b92-44b6-8847-4b6bdcb031ca

4. Digital Agency. (2026). Gビズ ID 接続システム向けガイドライン（2.8版）[gBizID guideline for connecting systems (Version 2.8)]. https://gbiz-id.go.jp/top/manual/pdf/Developer_guideline.pdf

5. Eclipse Dataspace Working Group. (2025). Eclipse Decentralized Claims Protocol (DCP) v1.0. https://eclipse-dataspace-dcp.github.io/decentralized-claims-protocol/v1.0/

6. European Parliament, & Council of the European Union. (2023). Regulation (EU) 2023/1542 of the European Parliament and of the Council of 12 July 2023 concerning batteries and waste batteries. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2023/1542/oj/eng

7. European Parliament, & Council of the European Union. (2024). Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng

8. Guggenberger, T. M., Schlueter Langdon, C., & Otto, B. (2025). Data spaces as meta-organisations. European Journal of Information Systems, 34(5), 822–842. https://doi.org/10.1080/0960085X.2025.2451250

9. Information-technology Promotion Agency (IPA). (2026a). Open Data Spaces Protocols (ODP): Identity & Trust (L3). https://open-dataspaces.gitbook.io/ods-docs/jp/odp/fandamentarupurotokoru/aidentititorasutol3/protocol

10. Information-technology Promotion Agency (IPA). (2026b). Open Data Spaces Reference Architecture Model (ODS-RAM) V2. https://open-dataspaces.gitbook.io/ods-docs/jp/ods-ram/v2

11. Mertens, C. (2025). Establishing a unified, sovereign, and open digital infrastructure [Position paper]. International Data Spaces Association. https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-Position-Paper-Establishing-a-Unified-sovereign-and-open-digital-infrastructure-1.pdf

12. Turkmayali, A. (2026). Data Spaces and AI: Trustworthy Agentic Participation in Data Spaces (Position Paper). International Data Spaces Association. https://doi.org/10.5281/zenodo.21279055

CONTACT

International Data Spaces Association

Emil-Figge-Str. 80
44227 Dortmund | Germany

phone: +49 231 70096 501
mail: info@internationaldataspaces.org

WWW.INTERNATIONALDATASPACES.ORG

international-data-spaces-association