a blueprint for

THE PHYSICAL INTERNET

PILL imec VUB AGENTSCHAP INNOVEREN & ONDERNEMEN

Acknowledgments

This blueprint marks the culmination of four years of fundamental research, realized through the Physical Internet Living Lab project—a cornerstone in logistics innovation. It is the result of multiple iterations of design, build, and test, reflecting the collective effort of many dedicated contributors.

We extend our gratitude to **VLAIO (Flemish Agency for Innovation & Entrepreneurship)** for recognizing the transformative potential of this research and for incentivizing initiatives that drive progress in the transport sector.

A special thanks to **VIL (Flemish Innovation Platformr for logistics)** for providing invaluable feedback from its logistics community and to **VUB (Vrije University Brussels)** for its critical insights into trusted governance frameworks. We are also immensely grateful to the **companies** that actively participated in the real-life tests along the Port of Antwerp-Bruges – Genk corridor, helping to validate and refine our work, and specifically to the Flemish Waterways (DVWW) for their active support and feedback. We also give credit to the **Sytadel project team** for collaborating and sharing valuable insights on the practical implementation of decentralized trusted data-sharing technologies.

Through its evolution, the Blueprint was inspired by other initiatives such as the **FeDERATED project**, **ETP Alice** and the assorted European **Data Space** projects and organizations. We believe that many of the concepts they introduce are strong catalysts for the establishment of the Physical Internet.

We would like to thank the active members of our **advisory board** for their guidance, strategic direction, and for challenging us with real-world insights that strengthened our project.

Finally, a heartfelt thank you to the multidisciplinary **PILL project team** for its unwavering dedication—you paved the way for a more collaborative, sustainable, and resilient logistics ecosystem.

Thank you for your interest in this blueprint. We hope it inspires you and serves as a foundation for larger collaborations that drive meaningful impact in the transport and logistics industry.

On behalf of the Physical Internet Living Lab project and its partners:
Philippe Michiels (IMEC) & Dries Van Bever (IMEC)

Abstract

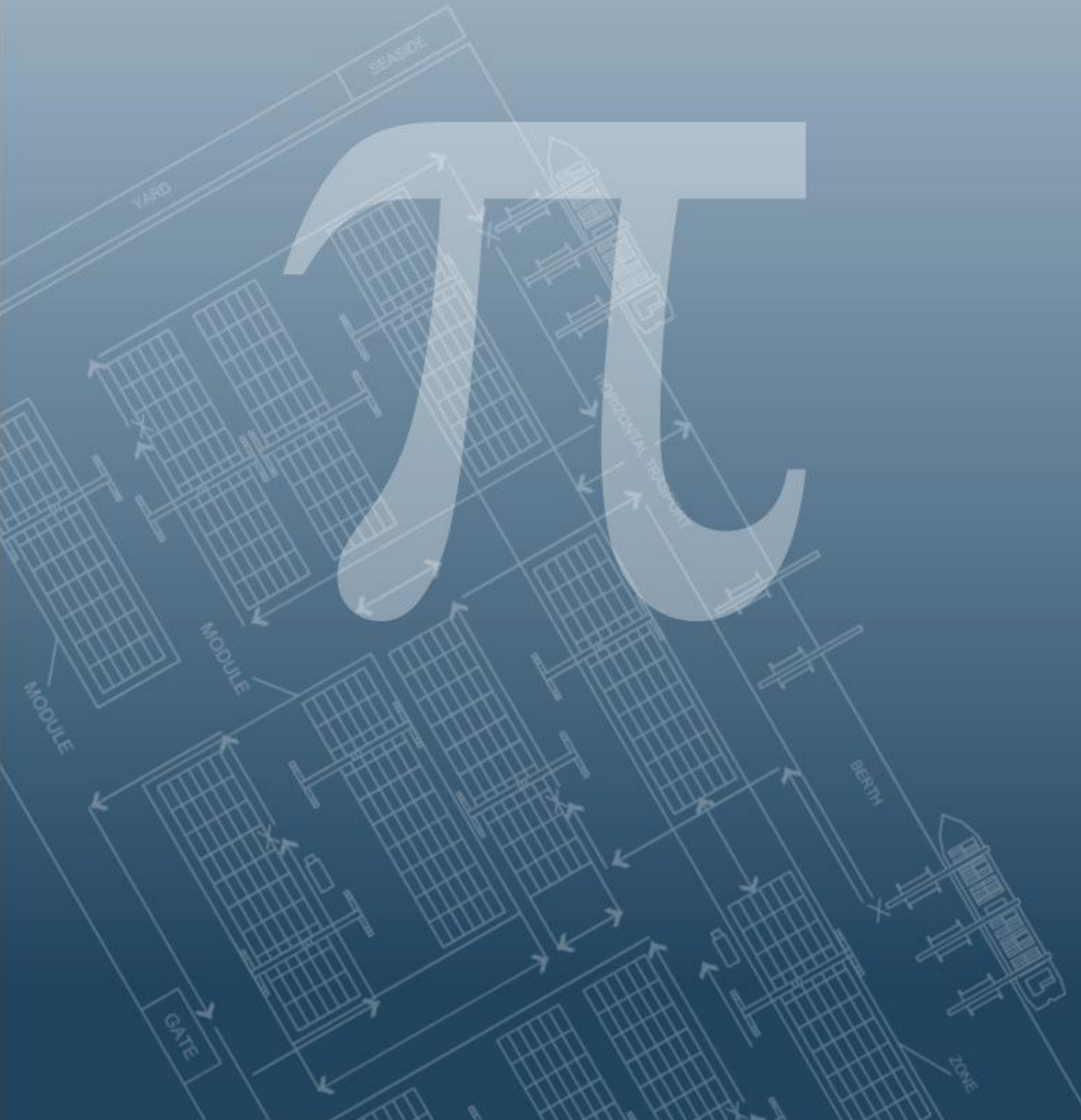
This blueprint outlines a comprehensive vision for implementing the **Physical Internet (PI)**, a transformative concept aimed at optimizing global logistics networks by leveraging principles of interoperability, decentralization, and trust. Inspired by the Digital Internet, the PI envisions goods moving seamlessly across a network of interoperable nodes, guided by standardized protocols and real-time data. The blueprint emphasizes three core challenges: achieving physical, digital, and governance interoperability, each critical for creating a robust, scalable, and secure logistics ecosystem.

The document introduces the foundational building blocks of the PI, including **PI-nodes, PI-capabilities, PI-movers**, and **PI-containers**, which enable a structured representation of logistics networks. A key focus is the development of a **PI Connector**, based on data space architecture, which facilitates secure data sharing, service discoverability, and process orchestration. The blueprint also highlights advancements in routing algorithms, network state synchronization, and agent-based modeling to enhance decision-making and efficiency.

To address gaps in standardization, governance, and technology, the blueprint advocates for robust policy frameworks, federated governance models, and the use of **verifiable credentials** for trust-building. It identifies critical next steps, including the development of machine-readable service descriptions, process orchestration standards, and scalable event pipelines. Living labs are proposed as essential testbeds to validate innovations and foster collaboration among stakeholders. Together, these elements form the foundation for a globally interconnected logistics system that mirrors the efficiency and adaptability of the Digital Internet, offering unparalleled benefits in efficiency, sustainability, and resilience.

Table of Contents

List of Figures


SEASIDE
YARD
MODULE
MODULE
HORIZONTAL TRANSPORT
BERTH
GATE
ZONE

Introduction to the Physical Internet (PI)

What is the Physical Internet?

The Physical Internet (PI) is a visionary concept aimed at transforming the global logistics and supply chain ecosystem by making it as interconnected, efficient, and flexible as the digital internet. Inspired by the way data packets move seamlessly across interconnected networks in the Digital Internet, PI proposes that goods—whether parcels, pallets, or containers—could move through a similarly open and standardized network of physical and digital infrastructure.

Imagine that every product can find its way automatically through a network of transport hubs, warehouses, and distribution centers, choosing optimal routes and methods of transport based on real-time data. Just like email or web data, physical goods could be *routed* dynamically, sharing infrastructure and information across different logistics providers to find the most efficient, sustainable path. The result would be a seamless, globally interconnected logistics network where each element—goods, vehicles, routes, and handling systems—interacts transparently and dynamically to optimize efficiency and reduce environmental impact.

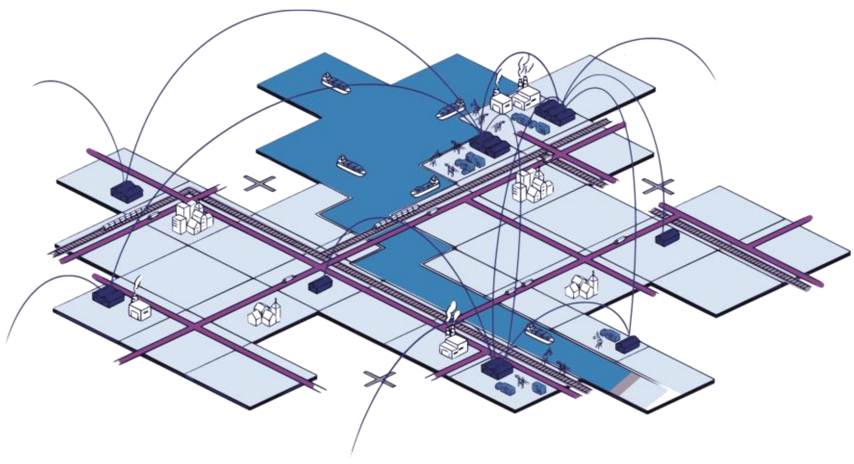


Figure 1: *The Physical Internet represented as a network of digitally interconnected and interoperable nodes.*

The Physical Internet Vision and Benefits

The Physical Internet was first conceptualized in 2010 by Benoit Montreuil (Montreuil, Meller, & Ballot, 2010) and proposes a new approach to logistics with four main objectives:

- **Efficiency**: Achieve optimal utilization of resources by reducing empty transports, optimizing routes, and speeding up deliveries.
- **Sustainability**: Minimize environmental impact by cutting down on CO_2 emissions and energy usage, as goods and vehicles are efficiently coordinated.
- **Transparency**: Enable real-time tracking and increased visibility across the supply chain for all stakeholders, enhancing security and traceability.
- **Resilience**: Create a more flexible and robust system by reducing dependency on any single logistics provider and ensuring continuity during disruptions.

Key Pillars of the Physical Internet

A fully functioning Physical Internet requires three types of interoperability:

- **Physical Interoperability**: Standardize physical assets, such as modular containers and hubs, to facilitate easy handling, storage, and transportation across the network.
- **Digital Interoperability**: Ensure data and information can flow freely across systems and platforms, enabling real-time coordination and optimal routing.
- **Governance**: Establish shared protocols, standards, and regulatory and legal frameworks to manage interoperability, data privacy, and competitive fairness across stakeholders.

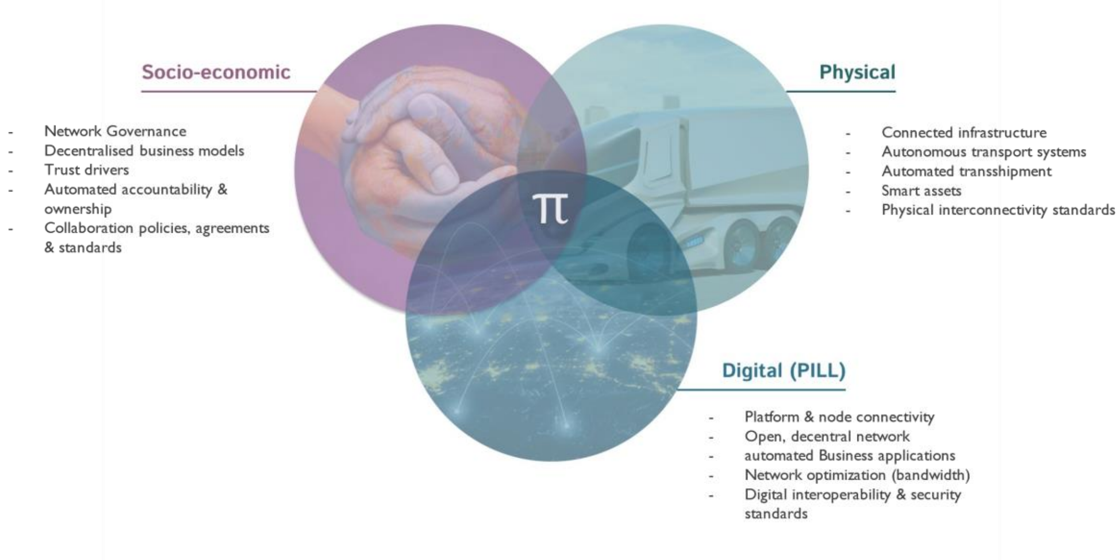


Figure 2: *The three major challenge domains for the realization of the Physical Internet.*

Although the PILL project focusses primarily on establishing a digital PI-network, interoperability on the Physical Internet requires a systemic approach. Any full vision of the Physical Internet, requires interoperability on these three systems: socio-economic systems interoperability (governance), physical systems interoperability and digital systems interoperability.

Related Initiatives

ETP Alice

Organizations like ETP ALICE (Alliance for Logistics Innovation through Collaboration in Europe) and various collaborative research projects, including PILL (Physical Internet Logistics Labs), are driving this vision forward by developing roadmaps, technical frameworks, and proof-of-concept implementations. While the journey to a fully realized PI is complex, the commitment to a standardized, open logistics network promises transformative improvements for global logistics and supply chains by 2040.

The ALICE Roadmap for the Physical Internet (ETP ALICE, 202 C.E.) is guiding research projects and other initiatives towards the realization of PI which is expected by 2035-2040.

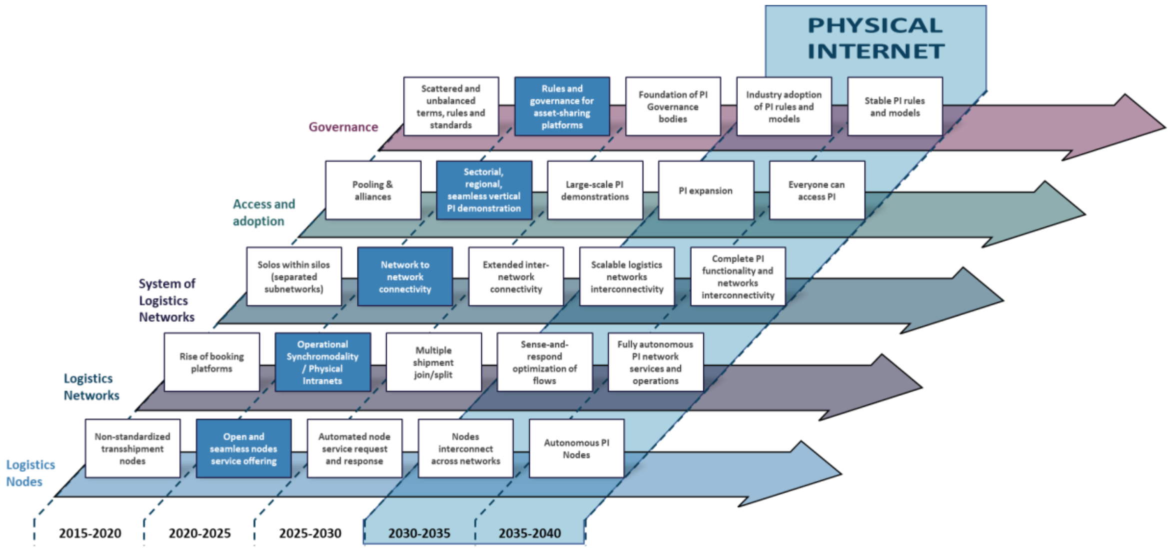


Figure 3: *The Physical Internet roadmap according to ALICE illustrates the relevance of the work done in PILL. (Source: ETP ALICE)*

European Data Spaces

Traditional logistics networks lack transparency due to siloed data and incompatible IT systems. Point-to-point data exchange is costly and doesn't scale. To address this, initiatives created platforms for logistics stakeholders. However, competing platforms and mistrust of central data collection have hindered their impact.

Recognizing these challenges, data spaces have tried to fill these gaps and are revolutionizing logistics by enabling secure, transparent, and efficient data exchange across a fragmented industry. The key to data spaces is that they support:

1. direct bilateral exchange of data, using fit-for-purpose standards, without requiring the data to be centralized, and
2. shared governance infrastructure to facilitate trust, discoverability and interoperability

Data spaces (Nagel & Lycklama, 2021a) take a layered approach towards establishing full data interoperability. We identify the following layers (as depicted in **Figure 4**):

- Interoperable, easy-to-deploy data space connectors ensure uniform connectivity, acting as gateways to an organization's digital services and data sources while managing security, access control, and data usage monitoring.
- Open web standards like Decentralized Identities and Verifiable Credentials enable a uniform security approach with Generic Identity Management and Access Control Mechanisms.
- Uniform metadata publishing and federated catalog services, governed by the community, support the discoverability of Data Space Parties and their services.
- Machine-readable policies within contractual agreements provide a legal and technical foundation for proper data usage.
- Data exchange occurs through specific adapters in the data plane of the connector.

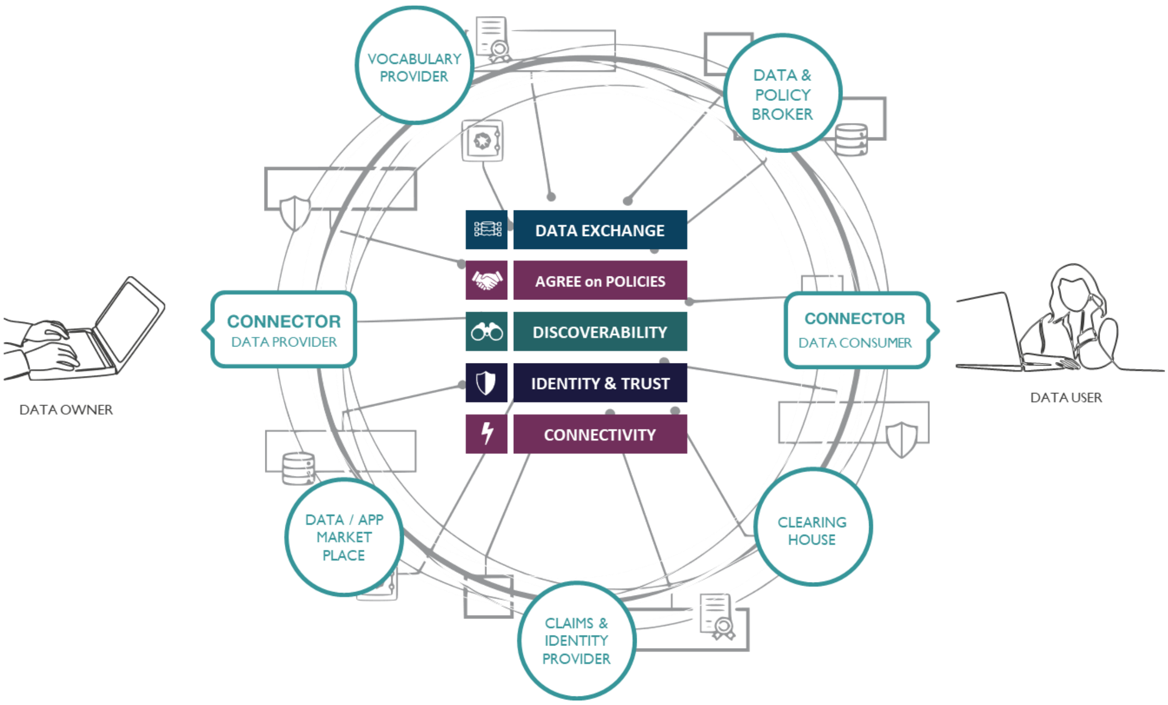


Figure 4: *A schematic view of the typical data space architecture. Data owners and publishers connec to the data space via connectors. Federation services offer dicoverability, trust & governance. The different concers are depicted centrallly as abstraction laye*

Several logistics-oriented data space initiatives exist such as (iSHARE Foundation, 2024), Fenix, (Catena-X: an Automotive Industry Data Space), proving the relevance for data spaces in this domain. This Blueprint for the Physical Internet fully aligns with data spaces and uses their design principles as its foundation.

SYTaDeL Project

SYTaDeL[1], a project closely related to PILL explores the potential of data space technology to share logistics information across stakeholders. SYTADEL investigated the possibilities and requirements of a logistics data space as a **framework for sharing and consulting data across logistics partners with mutual consent**, to make transportation planning more efficient, flexible and sustainable.

The data space building blocks in the SYTADEL project enable trusted and privacy-secure data sharing for logistics planning. It highlights the need for advanced data access policies as a part of a logistics data space. Such policies are equally necessary in a broader Physical Internet context that relies on publishing events that contain confidential data as well. Showing that such policy management and enforcement can be implemented in a dataspace is thus relevant for Physical Internet applications as well.

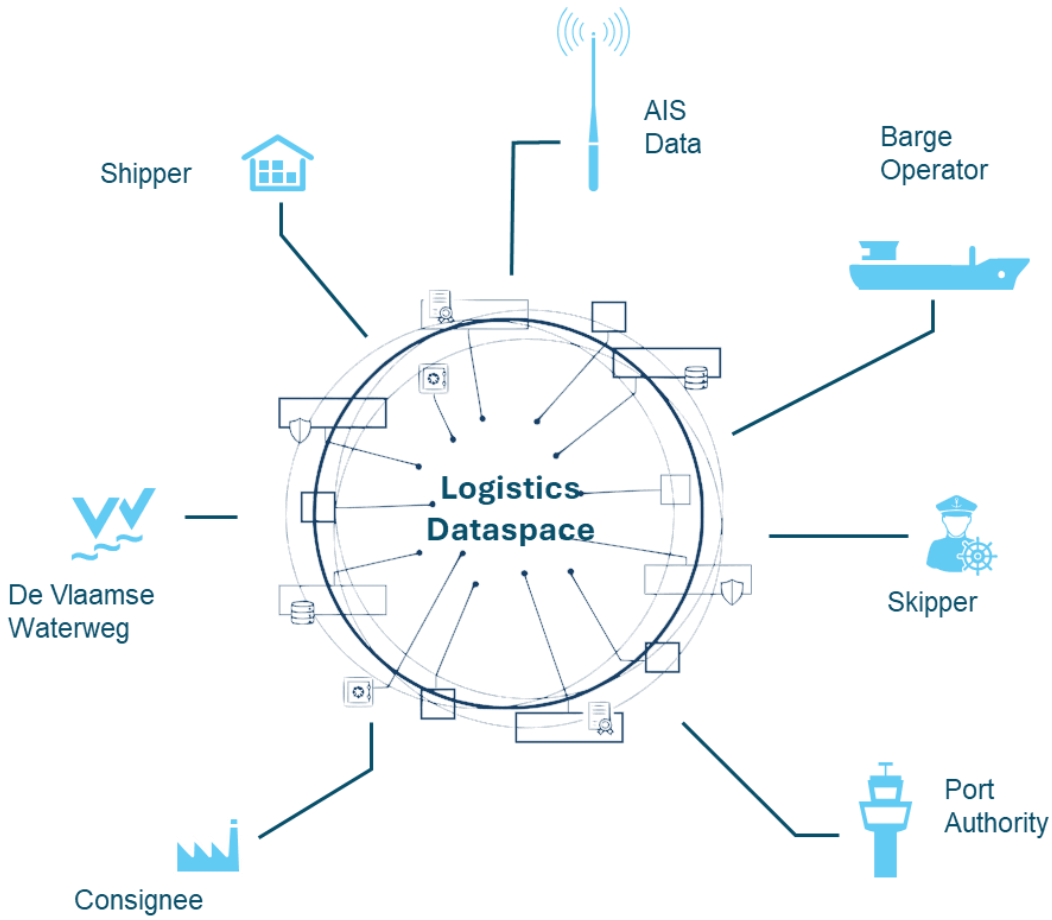


Figure 5: *SYTaDeL allows the exchange of privacy-sensitive vessel tracking data in the inland waterway logistics chain.*

[1] https://www.imec-int.com/en/sytadel

PILL's Focus

PILL (*Physical Internet Living Lab*)[2] is a Flemish strategic fundamental research project aimed at bringing the current research on Physical Internet and its principles into practice and laying the foundation of a full stack Physical Internet implementation framework for Europe and beyond. This document serves as a key outcome of PILL and defines a blueprint for the PI.

The key research question that we address in this document is the following:

What is needed to establish a trustworthy full-stack Physical Internet that allows stakeholders (1) to connect seamlessly and effortlessly, (2) to publish and discover logistics services, (3) to agree on the conditions of said services and to (4) automatically exchange the execution status of the pre-agreed process, while (5) seamlessly integrating with connected processes?

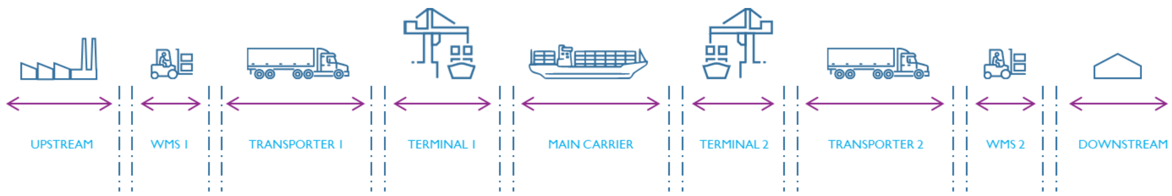


Figure 6: *Supply and logistics chains can involve many stakeholders. Coordinating such chains effectively requires a high degree of interoperability to ensure data can flow eefortlessly and securely across. (Source: imec)*

With this research question in mind, PILL has focused on the following major topics, which will be discussed more elaborately in subsequent chapters.

Network state and routing

In a Physical Internet context, the "network state" is a comprehensive digital representation of the logistics network. It includes detailed information on available infrastructure (such as hubs, corridors, and terminals), participating stakeholders, and their respective capabilities. The goal is to provide a transparent and real-time view of the logistics landscape to all participants, facilitating informed decision-making and enabling seamless collaboration.

Network dynamics

Effective routing is one of the most transformative applications of the Physical Internet, where logistics assets dynamically choose the most efficient paths based on the real-time network state. PILL's routing innovations are grounded in agent-based models and simulations that allow digital agents to act as autonomous decision-makers in route

[2] https://www.imec-int.com/en/pill

planning. This facilitates both individual and collaborative routing, enhancing efficiency across the network.

Data spaces as a foundation for PI

PILL leverages data space connectors to link logistics data across organizations securely and flexibly. This ensures data sovereignty, allowing each participant to control access to their data while contributing to a collective network state. It also enables interoperability with other data ecosystems, such as those in transportation or manufacturing. A key insight of the PILL project is the value that data space design principles bring to establish federated networks for collaboration that can serve as a foundation for the Physical Internet.

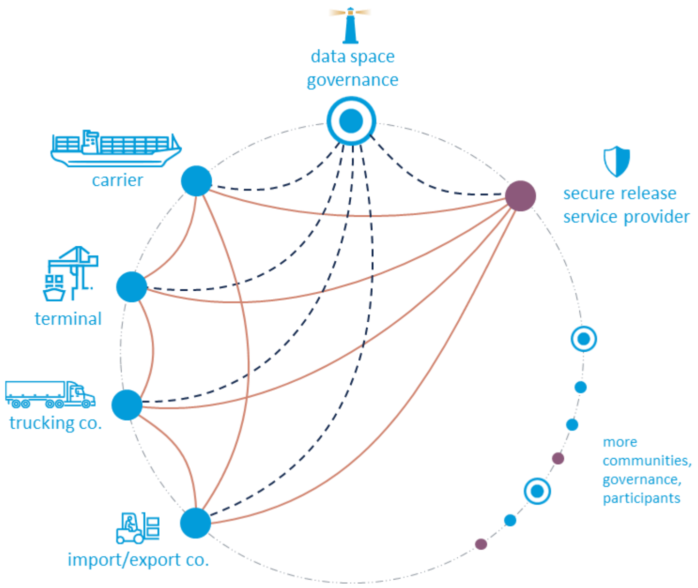


Figure 7: *A Federated approach to digitally connecting stakeholders in logistics communities. A governance bodu is used to assure trust, but all data is exchanged directly between stakeholders en suring data sovereignty. (Source: imec)*

Data space architecture relies on the ability for stakeholders to establish direct connections and exchange data bilaterally with the need for central data brokerage. At the same time the cater for trust by supporting a federated approach for managing stakeholders and ensuring well behaved and trustworthy ecosystems.

Conceptual Model of the Physical Internet

Foundational Theories

The foundation of the Physical Internet (PI) rests on a vision of interconnected, efficient, and flexible logistics networks that resemble the Digital Internet. Just as data packets are routed through various nodes in digital networks, the PI aims to transport physical goods through a globally connected network. The structure of this network relies on standardized building blocks, each of which represents essential elements of logistics. By defining these building blocks—PI-entities, PI-nodes, PI-capabilities, PI-movers, and PI-containers (Montreuil, Meller, Ballot, et al., 2010)—the Physical Internet provides a common framework to model logistics networks and supply chains with enough detail to facilitate planning, routing, tracking, and optimization. We discuss ow each building block contributes to the broader system.

PI-Entities

Definition PI-entities are the individual participants within the Physical Internet ecosystem, encompassing various logistics stakeholders such as shippers, carriers, hubs, terminals, and warehouses.

PI-entities represent all participants with roles in logistics processes. Each PI-entity can define its services, locations, capabilities, and operating constraints. This formalization ensures that each participant's unique role is recognized within the network, enabling collaboration and interoperability. With clearly defined PI-entities, logistics networks can map complex supply chains, ensuring that each participant has a digital representation within the system, which supports planning, communication, and coordination.

PI-Nodes

Definition PI-nodes are the locations within the Physical Internet network where physical interactions with goods occur, such as sorting, routing, transferring, or storing. Examples include hubs, terminals, warehouses, distribution centers, and cross-docking points.

PI-nodes provide the physical infrastructure of the network. Each node is a fixed point where goods can stop, be transferred, or temporarily stored. By modeling nodes as standardized locations with specific capabilities, logistics planners can create detailed maps of the network, defining pathways that goods can travel through. This granular representation of logistics locations is essential for routing, as it enables agents within the system to determine which nodes can facilitate specific logistics tasks, like customs processing or warehousing. PI-nodes also serve as critical checkpoints in tracking goods as they move through the network, ensuring visibility and control over each segment of the logistics journey.

PI-Capabilities

Definition PI-capabilities refer to the specific functions or services that a PI-node or PI-entity can provide, such as loading, unloading, transferring, storing, or assembling goods. Each node and entity can define its capabilities based on its infrastructure and services.

PI-capabilities are critical in defining the functional role of each node and entity within the network. By categorizing nodes based on their capabilities, logistics networks can facilitate more intelligent planning and optimization. For instance, if a shipment requires cold storage, only nodes with the necessary PI-capability can be chosen for routing. This structure allows the system to filter and select appropriate nodes and entities for each logistics operation, enhancing efficiency. Furthermore, PI-capabilities ensure that assets and infrastructure are optimized according to their unique functions, avoiding bottlenecks and unnecessary detours.

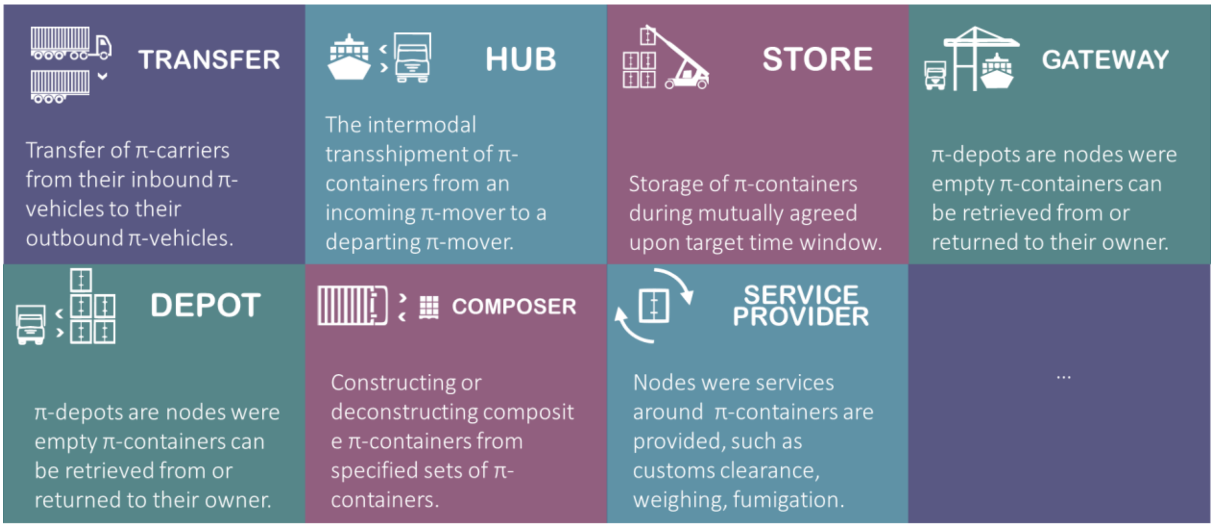


Figure 8: *The Physical Internet Logistics Capabilities are a key building block for a generic and interoperable representation of the Logistics Network. (Source: imec)*

PI-Movers

Definition PI-movers are the means of transport that move goods through the Physical Internet network. They include vehicles and carriers of various types, such as trucks, trains, ships, and planes, which operate between PI-nodes.

PI-movers represent the dynamic aspect of the logistics network, transporting goods between nodes. In the PI model, movers are standardized in terms of their attributes, such as capacity, speed, and scheduling, allowing for efficient matching between goods and transport resources. PI-movers play a vital role in route optimization, as they enable the system to calculate and assign transport modes that meet the specific requirements of a shipment, whether it's time-sensitive, cost-sensitive, or capacity-intensive. By defining movers as standardized assets, PI enables logistics networks to allocate resources more effectively and streamline multi-modal transport coordination.

PI-Containers

Definition PI-containers are standardized, modular containers used to hold and transport goods. Similar to data packets in the Digital Internet, PI-containers are designed for efficient handling, transport, and storage across the PI network. They vary in size, from large shipping containers to small parcel-sized units.

PI-containers are a key enabler of interoperability within the PI, as they provide a standardized way to handle goods across different nodes and movers. Each PI-container has unique identifiers and can include sensors or tracking devices, allowing it to be routed, tracked, and managed in real-time. Standardization in container design facilitates easier transfers between nodes and movers, minimizes handling errors, and ensures seamless interoperability, even in complex multi-modal journeys. With PI-containers, the system can also dynamically consolidate shipments, filling containers to capacity and reducing transport inefficiencies.

Network State Publication

In the PILL project, we leverage the formal building blocks of the Physical Internet (PI) to create a dynamic, decentralized system that benefits both transport service providers and customers. By modeling logistics networks with standardized PI constructs, we enable real-time publication, synchronization, and routing within a "network state"— a collective view of the logistics landscape.

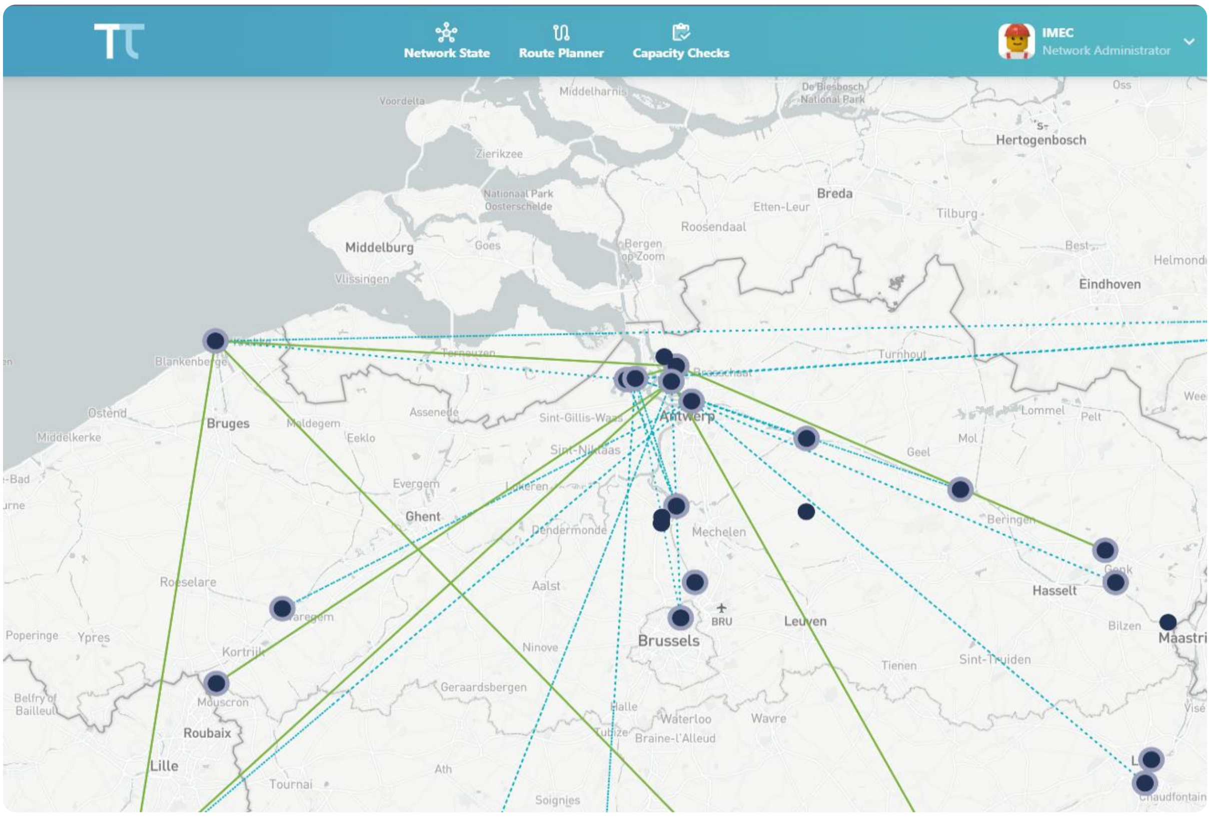


Figure 9: A screen shot of the PILL client that allows shippers to find multi-modal routes for their cargo (source: imec).

Publishing Logistics Services in a Network State

PILL uses PI-nodes, PI-capabilities, PI-movers, and PI-containers as the foundational elements to represent transport services within a unified, standardized structure. This formalization allows transport service providers to share their logistics offerings in a transparent and interoperable manner:

- **PI-Nodes and PI-Capabilities**: Each service provider's assets (e.g., terminals, hubs, warehouses) are defined as PI-nodes with specific PI-capabilities (such as loading, storage, or transfer). These capabilities allow the network to understand what each node can perform, which makes it possible for other participants to identify relevant logistics hubs that meet their requirements, such as cold storage or high-speed handling.

- **PI-Movers and PI-Containers**: Transport modes (PI-movers) and container types (PI-containers) are also standardized and integrated into the network state. By publishing this information, service providers can communicate the types of goods they handle (in this case, Full Container Loads), their transport routes, schedules, and other relevant characteristics. For example, if a provider offers barge services for container shipments between two ports, they can publish this mover-specific data alongside their node capabilities.

- **Interoperability through Data Standards**: Using data standards within PI-building blocks, PILL ensures that service information is published in a format accessible to other network participants. Service providers upload information about their transport routes, schedules, and capacities to the decentralized network, which enables other entities to discover and view these services in real-time without needing custom integrations.

By using the formal PI building blocks to publish this data, PILL creates a shared network state that aggregates logistics services and infrastructure in a structured, accessible way, making it easy for service providers to participate and share their services transparently.

Local Synchronization of the Network State

To facilitate real-time decision-making, PILL enables transport customers to synchronize the aggregated network state to their local systems. By accessing a real-time view of the network state, customers can make informed decisions on routing and service selection, enhancing their logistics operations.

- **Network State Synchronization with Decentralized Technology**: PILL leverages decentralized technologies, such as InterPlanetary File System (IPFS), to synchronize network state data across participants. This means each transport customer has a locally synchronized, up-to-date view of the logistics network, ensuring they can access accurate information on service availability, routes, and node capabilities.

- **Reduced Dependence on Centralized Systems**: Since the network state is decentralized, transport customers don't rely on a single source for updates. Each update to the network state (e.g., a new route offering or capability) is distributed across the network. Customers automatically receive these updates through IPFS or data space connectors, which provide a secure and reliable way to synchronize data.

- **Flexible Access and Offline Functionality**: By synchronizing network data locally, transport customers gain flexible access to the network state, even in offline or low-connectivity environments. This approach minimizes potential delays and ensures that logistics planning, and adjustments can happen in real time, based on the latest network state.

This synchronization approach enables transport customers to seamlessly access the full range of logistics services and infrastructure published by providers, allowing for quick and informed routing decisions.

Scalable Publication

In the early stages, PILL leveraged the InterPlanetary File System (IPFS) for decentralized management of the network state within the Physical Internet (PI) framework. IPFS, a peer-to-peer distributed file system, was selected for its ability to store and synchronize data across decentralized networks without the need for a central server. This approach aligned with PILL's goals of ensuring data privacy and autonomy for logistics stakeholders, allowing them to publish updates to the network state in a distributed manner. However, several limitations emerged in practice, which ultimately led PILL to adopt Linked Data Event Streams (LDES) across a Data space Connector, providing a more robust, scalable, and secure alternative (Lancker et al., n.d.).

Routing in the Physical Internet

In a Physical Internet context, efficient routing relies on an interconnected and decentralized network of logistics nodes and transport services. However, many logistics companies are hesitant to fully engage in collaborative networks due to concerns over data privacy and competitive positioning. The PILL project proposes a solution by structuring routing based on “capabilities” (Cassan et al., 2023) rather than on sensitive capacity or demand data, thus addressing the dual needs for privacy and interoperability.

Capability-Based Routing in the Physical Internet

The study introduces a capability-based routing model, where PI-nodes are defined by the specific services, or capabilities, they offer, optionally accompanied with their up-to-date schedules. This model emphasizes a minimalistic data-sharing approach in which companies only disclose their logistics capabilities (e.g., transfer, storage, or container composition) rather than sharing sensitive details about available capacity or demand.

This approach achieves two objectives:

- **Decentralized Information Sharing**: By sharing only capabilities, logistics providers reduce the need for centralized data exchange, maintaining control over sensitive operational data.
- **Trust-Building**: The limited data-sharing requirement mitigates concerns about privacy and data exploitation, fostering trust among stakeholders.

Network State Synchronization and Local Routing

In the capability-based model, the network state is maintained in a decentralized manner as discussed in the previous chapter. Each logistics provider periodically publishes updates to their capabilities, which can then be synchronized across the network. This event-based decentralization allows each participant to maintain an up-to-date local copy of the network state, incorporating only the relevant services for their operations.

Physical Internet A* (PIA*) Routing Algorithm

To operationalize routing on this capability-based network state, the study introduces the Physical Internet A (PIA) algorithm. PIA* is an adaptation of the traditional A* algorithm, designed specifically for the decentralized and capability-focused nature of the PI. In this model:

Nodes and Edges: Nodes represent logistics locations (p-nodes) defined by capabilities, while edges represent possible transitions between these nodes, facilitated by transport services (p-movers).

Vertices and Transitions: A route is constructed as a sequence of vertices (states) and transitions (edges) that move a container through the network, optimizing criteria such as cost, distance, and greenhouse gas emissions.

Constraint-Driven: Constraints such as pickup/drop-off locations, time windows, and transit conditions are used to filter route options and find the most viable paths.

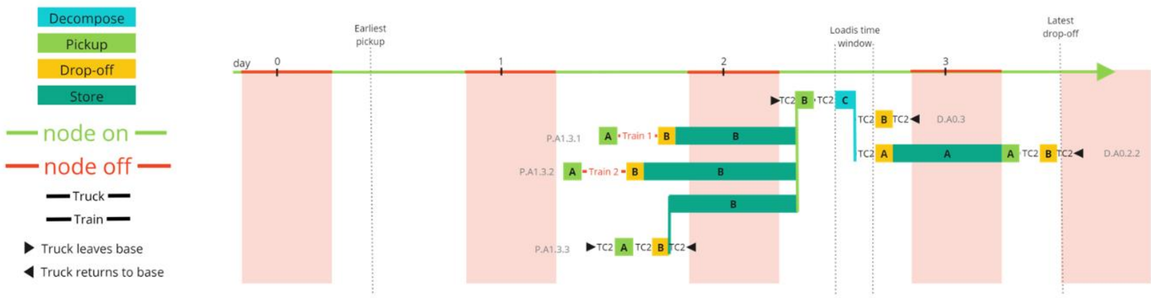


Figure 10: *The PIA* algorithm developed in PILL enables decentralized route calculation, allowing each entity to independently apply routing logic on their synchronized network state, minimizing reliance on a central orchestrator.*

Logistics Decision Support Systems

Agent Based Models (ABMs)

The capability-based routing model was validated using an Agent-Based Model (ABM) that simulated real-world logistics operations in the hinterland network of the Port of Antwerp-Bruges. The ABM environment enabled the PILL team to test various routing scenarios, analyze performance across different conditions, and fine-tune the capability definitions to best reflect the operational realities of PI networks. Simulation results showed that capability-based routing effectively balanced efficiency, data privacy, and trust, supporting viable routes for container transport while limiting unnecessary data exposure.

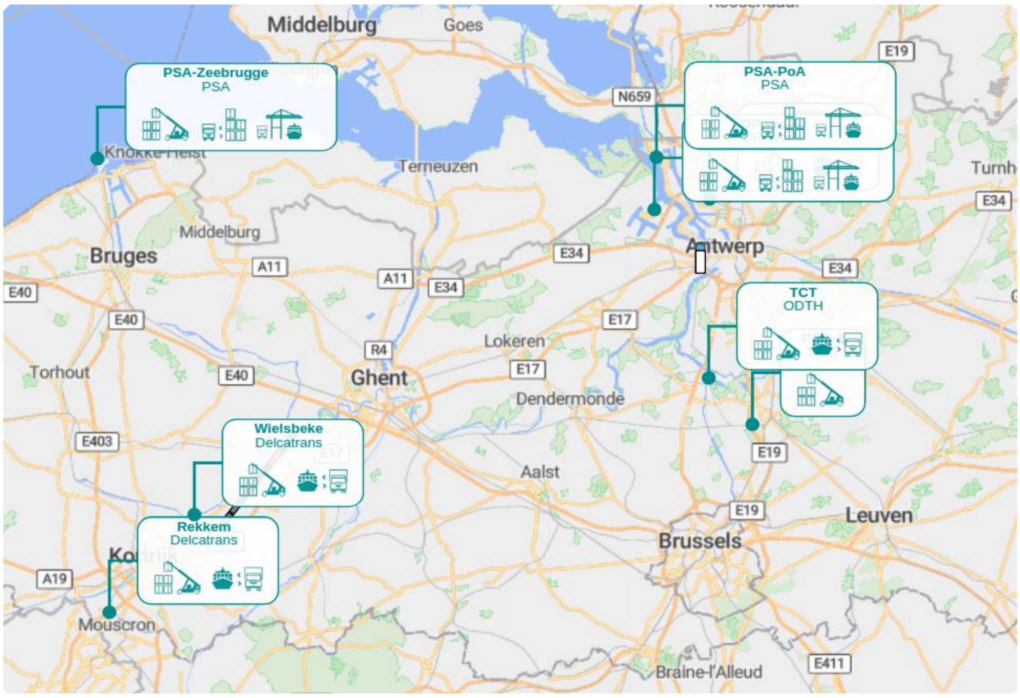


Figure 11: A screen shot of an ABM which uses the PILL logistics network representation and routing algorithm to simulate a logistics network.

Agent Based Models for Logistics Networks can be used for several purposes:

Replay or Post-Mortem Analysis: ABMs can recreate past logistics scenarios, providing insights into how events unfolded and identifying factors that led to specific outcomes. By simulating past decisions, disruptions, or delays, logistics managers can analyze performance metrics and pinpoint areas for improvement, making ABMs a valuable tool for learning from historical operations.

Route Planning and Optimization (Static): ABMs help plan and optimize logistics routes by modeling interactions between different network nodes and transport modes. In static route planning, ABMs calculate efficient paths for shipments through a predefined network. This approach provides optimized routes based on known conditions, such as current infrastructure, available resources, and demand, supporting better decision-making in route selection.

Policy Design with What-If Scenarios (Simulation): ABMs are highly useful for exploring the potential impacts of various policies, allowing logistics managers to test "what-if" scenarios before implementation. By simulating different policy options—such as introducing new transportation regulations, adding hubs, or changing routing protocols—ABMs provide insights into potential outcomes and trade-offs. This predictive capability helps policymakers design strategies that minimize risks and optimize network performance.

Prediction: ABMs allow logistics managers to forecast the future state of the network by simulating agent behaviors and interactions based on expected trends. By modeling potential demand spikes, traffic congestion, or disruptions, ABMs support predictive logistics, helping companies proactively adjust capacity, resource allocation, or routes to optimize network resilience and responsiveness.

The Physical Internet and Digital Twins

In the next chapter we discuss the synergies between the Physical Internet and Data Space Design Principles, where we envision the Physical Internet to be a logistics data space driven by Physical Internet-specific standards and agreements. A key principle is the use of a connector, a gateway component that enables stakeholders to connect to the Physical Internet. As we will go on to explain, these connectors will not only facilitate stakeholders to find each other and interact, they will also make data about logistics assets and processes accessible for other applications, such as digital twins.

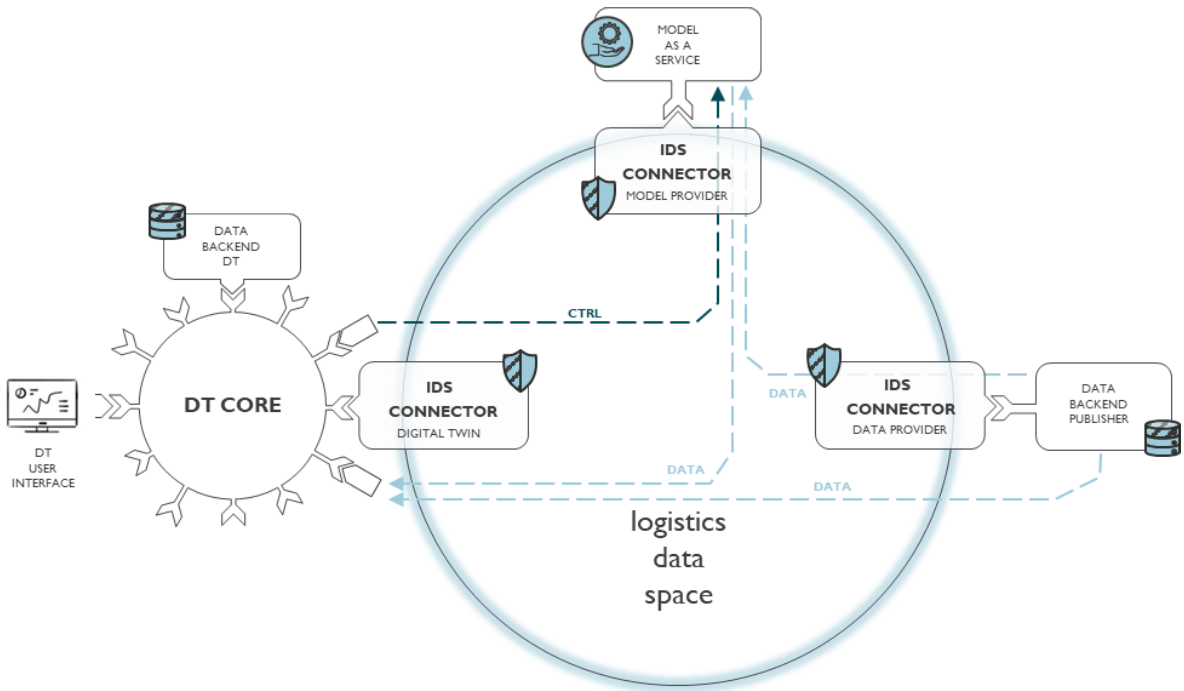


Figure 12: *A schematic depiction of how data spaces can enable the realization of digital twins by making bot data and algorithms more discoverable and accessible.*

A digital Twin is an integration of three components: Data, Algorithms (or models) and an analytical environment typically represented as a dashboard or a geographical visualization (Raes et al., 2022). A DT system also provides the possibility to link data sources and algorithms into a pipeline, enabling things like real-time or historical data visualization and simulations.

The robust data sharing infrastructure and the event-based approach for coordinating logistics processes fit nicely into such a digital twin architecture. The built-in systematic exchange of trace data of the Physical Internet will also empower digital twin systems, which typically face challenges when it comes to data access.


12

Remaining Challenges

PILL in Context

While the PILL project has made substantial progress in logistics network modeling, discoverability, and routing, a fully operational, "full-stack" Physical Internet solution will require tackling many remaining technical and organizational challenges. These include achieving seamless data interoperability, real-time process synchronization, secure data governance, and broad stakeholder engagement. Addressing these challenges through collaborative governance, technical innovation, and industry-wide adoption strategies will be crucial in transforming PI from a vision into a reality.

Technical Challenges

- **Connectivity and Ease of Access:** The Physical Internet can only fulfill its promise if it is open and freely accessible. Therefore, it is important that there are easy ways to connect and integrate backend systems through readily available connection components, which we typically refer to as a *Physical Internet Connector*. [→ discussed in the next chapter]
- **Security, Privacy, and Data Sovereignty:** In today's platform dominated landscape requires a multitude of logins. Additionally, platforms typically act as data brokers, aggregating data from multiple stakeholders. This is typically perceived as a problem by the data owners. The Physical Internet in contrast, should not rely on central data brokerage and should allow to connect using a single identity where access control is done based on verifiable credentials linked to that identity.
- **Interoperable Discoverability:** Although PILL has covered network discoverability for a large part, establishing standards for exchanging network state in line with best practices and existing semantic standards still needs work.
- **Policies & Agreements:** When logistics services are being performed, the terms and conditions of the service need to be clear. In a world where more flexibility is required in planning and executing transport, it is important that contractual agreements can be negotiated and closed automatically as well.
- **Real-Time Network and Process Synchronization:** Supply chains are in fact not really chains at all. They manifest as a series of parallel processes that are interconnected at certain steps for the sake of their proper execution. The ability to orchestrate these processes and have them properly synchronized by automatically exchanging data is essential.

Organizational Challenges

- **Stakeholder Engagement and Trust:** For the physical internet to become reality, it must be adopted a critical mass of participants. This requires communities of stakeholders to come together and establish a foundation for trustworthy collaboration.
- **Regulatory and Policy Compliance:** Operating an open, cross-border logistics network involves navigating a web of national and international regulations concerning data privacy, customs, environmental standards, and transport safety.
- **Investment and Funding:** Building and maintaining a PI infrastructure requires substantial initial investment, which can be a barrier for smaller logistics providers and startups. Therefore, having accessible and affordable connectivity components is indispensable and shared costs for infrastructure and governance require coverage from the PI communities.
- **Business Models and Compensation Mechanisms:** The Physical Internet is a paradigm shift away from dominant platforms. This will render existing business models redundant and give rise to new value propositions that leverage the power of the network. Another concern is compensation mechanisms for shared resources and services in PI. These can prove to be complex, as this requires fair distribution of costs and revenues among all participants.
- **Change Management and Adoption Barriers:** Shifting from traditional, siloed logistics operations to a collaborative PI model requires a significant change in mindset, operational processes, and technology adoption. Resistance to change is common, especially in well-established companies with traditional logistics models.

We dig deeper in some of the challenges that relate to the technical architecture.

Connectivity & Ease of Access

Generic connectivity serves as a foundational element for achieving interoperability across logistics networks. By enabling a standard means of connection, generic connectivity reduces the need for each participant to build custom integrations or navigate complex data-sharing protocols. This is particularly crucial for smaller stakeholders with limited technical resources or for those hesitant to invest heavily in integration technologies.

The vision for **data space connectors** aligns well with the goals of the Physical Internet by promoting a low-barrier, user-friendly means of connecting to the logistics network. These connectors reduce technical and operational friction for all stakeholders, enabling a more inclusive, scalable logistics ecosystem. By providing generic connectivity, plug-and-play integration, and configurable access control, data space connectors help realize the Physical Internet's vision of an open, interoperable logistics network, accessible to both large and small players.

Ultimately, this low-barrier connectivity model empowers stakeholders to collaborate more effectively, share data securely, and unlock the full potential of a decentralized logistics ecosystem. Through data space connectors, stakeholders can engage in seamless data sharing and reap the benefits of interoperability without the typical technical complexities of data integration.

Security, Privacy, and Data Sovereignty

Security, privacy, and data sovereignty are critical challenges in realizing a robust Physical Internet (PI) due to the open, decentralized, and highly interconnected nature of PI networks. As diverse logistics stakeholders—ranging from large companies to small operators—share data, the PI must balance accessibility with strict control over data security, user privacy, and ownership rights. These challenges are particularly pronounced because each participant may have unique regulatory, competitive, and security requirements that must be respected to encourage their trust and participation.

Self-Sovereign Identity (SSI)

SSI offers a decentralized model for managing digital identities, allowing users to own and control their identity data. Within the context of PI, SSI could be implemented through solutions like **Web ID**[3], providing participants with an identity that they control rather than relying on a central authority. This approach addresses several key challenges:

[3] WebID - W3C Wiki

1. **Data Privacy**: With SSI, each participant can control which parts of their identity they share with others in the PI network, minimizing the risk of data exposure.

2. **Authentication**: SSI enables secure, decentralized authentication, allowing PI participants to verify the identity of others within the network without relying on a single point of failure.

3. **Trust and Autonomy**: By granting stakeholders control over their identity, SSI enhances trust and autonomy within the network, which is critical for onboarding diverse participants who may otherwise be reluctant to share data in an open network.

The implementation of SSI in PI, via standards like Web ID, would allow participants to present only the identity data required for a specific interaction. This selective sharing builds trust and aligns with the PI's goals of secure and autonomous data exchange.

Verifiable Credentials

In addition to SSI, **verifiable credentials**[4] are essential for building a secure and trustworthy PI. Verifiable credentials allow participants to prove specific claims or qualifications without exposing all underlying details. This approach is particularly useful in a PI context, where stakeholders may need to validate their capabilities, certifications, or compliance with certain standards without sharing sensitive business data.

1. **Credential Verification**: Verifiable credentials can prove a participant's capacity to perform specific logistics functions (e.g., cold storage capabilities, hazardous material handling) without revealing sensitive operational details.

2. **Decentralized Trust**: Credentials can be issued and validated by trusted third parties (e.g., certification bodies or regulators), ensuring that each credential is independently verifiable. This decentralized trust model reduces the need for a central authority while maintaining reliability.

3. **Scalability**: Verifiable credentials are scalable across diverse PI participants, from large corporations to small logistics providers, allowing each to participate in the PI network with the necessary trust assurances.

The use of verifiable credentials enables PI participants to validate claims and capabilities in a standardized, privacy-preserving manner.

[4] https://www.w3.org/TR/vc-data-model-2.0/

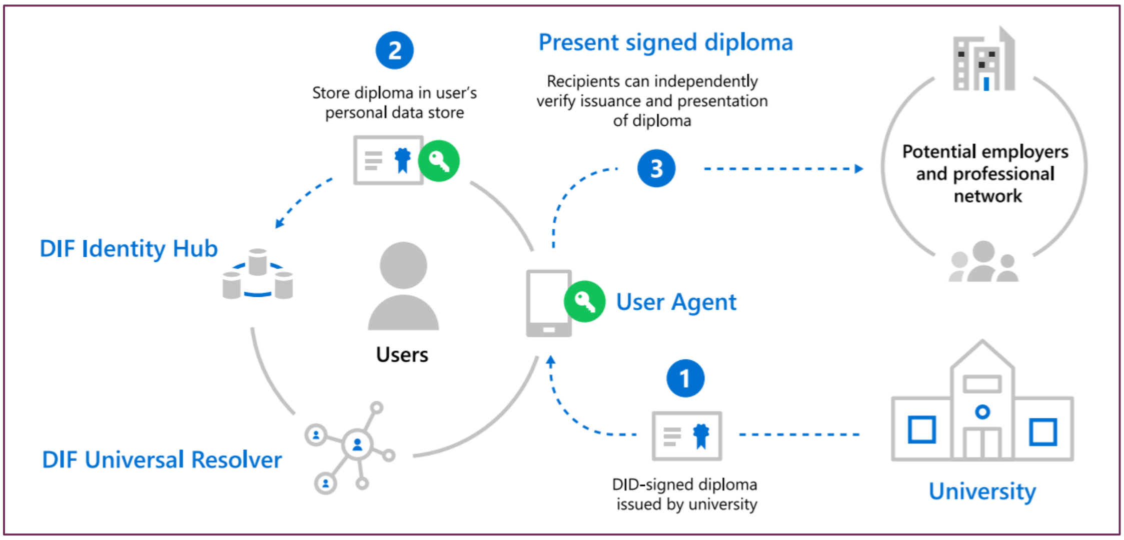


***Figure 13**: Example case of the use of decentral Identity (DID), Verifiable Credentials (VC) and Identity Hub where the authenticity of a VC-document (diploma) that is associated with a DID can be independently verified (Source: Microsoft).*

Policies and Agreements for Terms of Use

To further ensure security, privacy, and data sovereignty, PI requires **clear policies and terms of use agreements** that govern data-sharing interactions. These policies define acceptable use, data access, and retention rules, providing a legal and operational framework for data sovereignty.

1. **Terms of Use Agreements**: These agreements outline specific terms under which data can be accessed, used, and stored, protecting data owners' interests. For instance, terms may specify that data shared for route optimization cannot be reused for other purposes without consent.

2. **Data Access Policies**: Policies determine who can access specific types of data and under what circumstances. By embedding data access policies in the PI network, stakeholders can ensure that their data is shared only with authorized parties.

3. **Automated Compliance**: Integrating automated policy enforcement mechanisms within data space connectors can help ensure compliance with terms of use agreements. For instance, access control policies could automatically limit access to sensitive data based on location, role, or credentials.

These policies are vital for encouraging participation across diverse stakeholders, as they provide assurance that data privacy and sovereignty will be maintained, even in complex multi-party interactions. Open standards for expressing machine-readable policies such as the commonly used ODRL (Open Digital Rights Language)[5] exist.

[5] https://www.w3.org/TR/odrl-model/

Interoperable Discoverability

Discoverability within the Physical Internet (PI) is essential for achieving optimization and resilience, despite some views that it's not core to PI's functionality. Enabling logistics stakeholders to publish services in a standardized, machine-readable format allows for automated, data-driven decisions that enhance operational flexibility. The PILL project has demonstrated that discoverability can work effectively in a federated, collaborative network, proving its value for real-world PI applications.

Benefits of Discoverability

Discoverability enables logistics agents to locate available storage or handling facilities dynamically, helping **optimize space and resource use** across the network. For instance, during peak demand, participants can quickly discover additional nearby storage, minimizing bottlenecks and maximizing resource utilization. Machine-readable service data, including metadata on locations, pricing, and capacity, enables systems to **autonomously plan** routes based on real-time conditions. This reduces manual intervention and ensures routes are optimized for cost and efficiency. When disruptions occur, automated systems can use discoverable service information to **adjust routes** or resources quickly, selecting alternatives based on availability, cost, and service compatibility.

Scaling Discoverability

For discoverability to work at scale, PI must rely on open standards and widely accepted vocabularies:

- Open Standards ensure seamless data exchange, enabling diverse systems to connect and interact across the network. This is crucial for scalable integration and reducing custom setup needs for new participants.
- Reusable Vocabularies provide consistency in how logistics data is published, facilitating a shared language among stakeholders and simplifying data interpretation.

By building on open standards and reusable vocabularies, PI can make discoverability accessible and scalable, fostering a more connected and resilient logistics ecosystem.

Policies & Agreements

Digital policies and agreements play a critical role in the Physical Internet (PI) by establishing a framework for secure, fair, and efficient data exchange among diverse stakeholders. These policies set the rules for data usage, access control, and collaboration, ensuring that all participants can trust the network while maintaining autonomy over their data and operations. We discuss some key opportunities:

Data Access and Usage Control

Digital policies define who can access certain data within the PI network and under what specific conditions, supporting each stakeholder's need for data privacy and sovereignty. By granting controlled access, these policies ensure that only approved parties have visibility into sensitive information, which is especially important in competitive logistics environments. Additionally, usage restrictions protect data from being repurposed outside of agreed-upon uses, preventing misuse by third parties.

Terms of Use

Clear terms of use outline responsibilities, accountability, and data handling practices for all participants, building a foundation of trust. By addressing data confidentiality, proper handling, and dispute resolution, terms of use mitigate risks associated with data sharing in a collaborative network. They create a fair framework for data exchange that reassures participants about the integrity of their data, fostering greater trust and openness and willingness to share within the PI ecosystem.

Automated Contracting

In dynamic logistics scenarios, such as route finding and optimization, contracts often need to be closed immediately. Automated contracting enables such instant transactions by facilitating auto-negotiation, where terms are established and agreed upon by algorithms within seconds. Machine-readable agreements allow these contracts to execute automatically, reducing delays and ensuring that each party has agreed on terms instantly. This capability not only supports efficient route planning and real-time optimization but also makes transactions scalable across a growing network where subcontracting is the norm. By embedding these terms directly into data-sharing protocols, automated contracting reduces manual intervention and friction, enabling the Physical Internet to operate at speed and scale.

Regulatory/Legal Compliance

Digital policies help PI participants comply with data privacy regulations, like GDPR, and address regional data sovereignty requirements, allowing stakeholders to confidently engage in data sharing across borders. Security standards embedded in these policies, such as encryption and user authentication, safeguard data throughout the network. By enforcing compliance in real-time, automated policies and protocols reduce security risks, foster trust, and maintain regulatory alignment, ensuring a secure and resilient PI network.

Logistics Service Transparency & Orchestration

In the Physical Internet (PI), logistics service and process transparency — or "**process sharing**" — is essential for efficient, real-time coordination across the supply chain.

Process sharing involves the continuous exchange of events between logistics service providers and their customers, allowing all parties to keep track of the execution of individual logistics processes. Through this bilateral data exchange, providers and customers gain visibility into the status of specific operations, enhancing control and responsiveness. However, while bilateral data exchange works well between individual providers and customers, real-world supply chains require a more complex, multi-party flow of information to function optimally.

The Challenge: Tracking Complex, Interlinked Supply Chains

Supply chains are inherently multi-tiered and involve numerous independent processes, each governed by its own bilateral agreements and timelines. Yet, for true end-to-end transparency, these isolated processes need to be interconnected, creating a unified flow of information that enables a comprehensive view of the entire supply chain. The challenge lies in finding a scalable way to track and manage these interconnected processes while respecting the independence and privacy of each bilateral relationship.

Inter-process Coordination is a key challenge is the realization of PI. Supply chains are composed of various independent logistics processes that need to be aligned to maintain smooth flow. Synchronizing these processes without a centralized orchestrator requires robust, interlinked data streams that convey updates between parties in real time.Finding the Right Level of Abstraction for Process Standardization

While transparency and process sharing are critical for optimizing supply chains in the Physical Internet, attempting to standardize every variation of every logistics process is neither practical nor scalable. The diversity of logistics operations, each with unique workflows, informal practices, and specialized requirements, makes it challenging to define rigid standards that would apply universally across the industry.

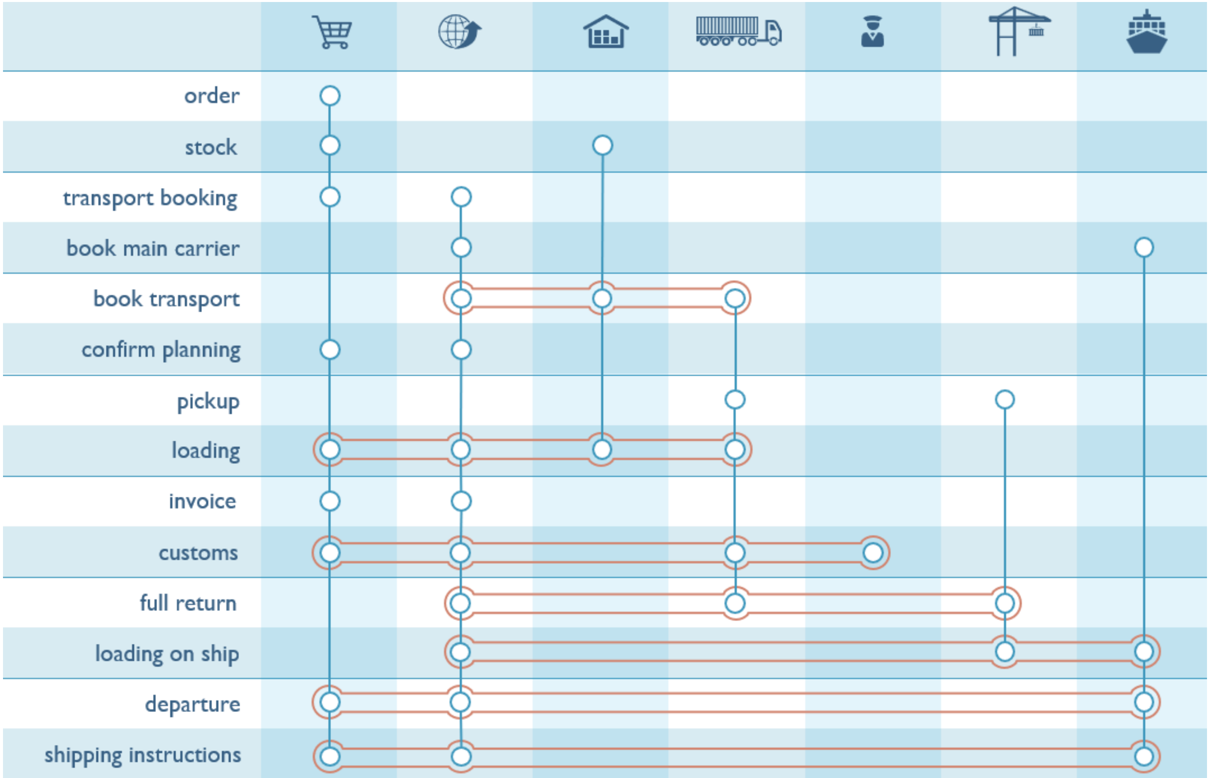


Figure 14: *An example of a process metro-map for a maritime container export. This illustrates how the different processes that are under control of a principal party are interlinked by events. Determining a correct abstraction level for defining process events and their semantics is a key challenge.*

Finding the Right Level of Abstraction for Process Standardization

To achieve effective process sharing, we need to carefully select an **appropriate level of abstraction**—one that is clear enough to be understood and adopted by industry experts but flexible enough to accommodate the variations inherent in real-world logistics. Striking this balance ensures that process standards are both usable and adaptable, allowing logistics networks to function efficiently without stifling the natural diversity of operations.

Choosing the right level of abstraction for logistics processes enables a more streamlined and scalable approach to process sharing within the PI, making standards adaptable to various scenarios without losing essential transparency. This approach facilitates industry-wide adoption, supports innovation, and ensures that process standards can evolve alongside the diverse and dynamic nature of modern supply chains.

Stakeholder Engagement and Trust

Trust is a cornerstone for collaboration in the Physical Internet (PI), given the diverse and often competitive nature of the logistics ecosystem. For stakeholders such as shippers, logistics service providers, and receivers to engage fully, they must feel confident in the security, fairness, and reliability of the system. Without trust, participation dwindles, and the transformative potential of PI remains unrealized.

The need for trust spans multiple dimensions:

Data Confidentiality and Control: Stakeholders need assurances that their sensitive data is protected and shared only with authorized parties. The decentralized and federated approach in PI helps address these concerns by enabling data ownership and secure sharing through trusted connectors and access control mechanisms.

Transparency and Accountability: Visibility into logistics processes and traceability of shared data foster trust among participants. Transparent governance frameworks, coupled with event-based data sharing, allow stakeholders to monitor compliance with agreements and ensure fairness.

Adoption and Mutual Benefit: Stakeholders are more likely to adopt PI technologies if they perceive clear benefits, such as cost efficiency, operational optimization, or reduced environmental impact. Trust also depends on the perception that others in the network will adopt and comply with shared standards and practices.

Trust in Automation: The extensive use of automation in PI for process orchestration and smart contracts requires stakeholders to trust these systems' ability to operate reliably and fairly. Overcoming skepticism towards automation is critical for broader acceptance.

The PILL project demonstrates how federated architectures, supported by data space principles, can enhance trust(Sun et al., 2024). By prioritizing data sovereignty, bilateral agreements, and decentralized orchestration, it addresses stakeholder concerns while enabling collaboration. To ensure widespread engagement, future efforts must focus on refining trust frameworks, establishing verifiable credentials, and maintaining governance mechanisms that align with stakeholder expectations. Trust, as both an enabler and outcome, is vital for unlocking the full potential of the Physical Internet.

PI Technical Architecture

Design Principles

The challenges presented in the previous chapter have clear implications for the conceptual design of the Physical Internet. We identify the following key design principles:

Control & Sovereignty

Ensure stakeholders maintain full control over their data and operations, with the ability to decide how, when, and with whom they collaborate and share data. Trust hinges on stakeholders retaining ownership of their sensitive information and processes, ensuring their competitive position is not undermined.

Decentralization & Federation

Avoid reliance on centralized platforms by designing a distributed system where governance is shared among participants. Allow for the establishment of independent (sub)networks and avoid centralization of power. Decentralization prevents monopolization, avoids vendor lock-in, and creates a more balanced power dynamic among stakeholders. See **Figure 15** for a comparison of different network models.

Discoverability, Transparency and Accountability

Enable stakeholders to publish and discover logistics services and maintain verifiable traceability of processes to foster trust and collaboration. Transparency ensures stakeholders have visibility into operations, while accountability builds confidence that agreements and processes are upheld. Furthermore, such transparency and traceability are fundamental to establish the Physical Internet 's full potential that relies on having insight into logistics network dynamics.

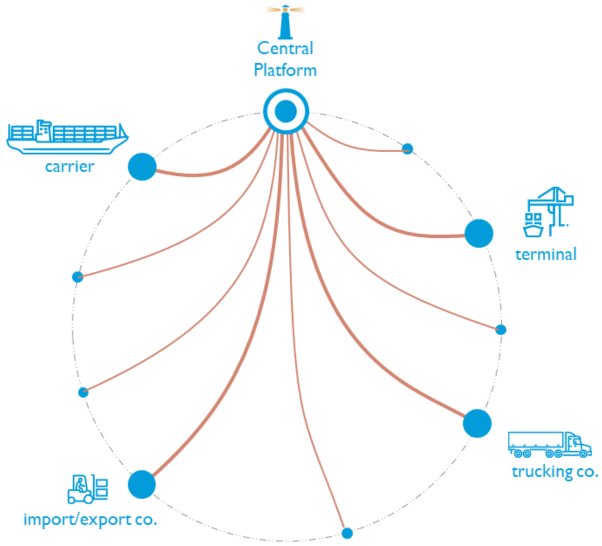
Interoperability & Flexibility

Ensure the system can integrate with diverse stakeholders and adapt to varying processes and informal practices while maintaining structured communication. Logistics ecosystems are highly diverse, and rigid systems fail to accommodate the nuances of real-world operations.

Modularity

Data spaces have a modular design that allows stakeholders to comply with them at the levels that matter to them and ensuring that there is no vendor lock-in at the level of the data space components themselves.

Figure 15: The different network organization models along with their key advantages and disadvantages



Centralist Platform

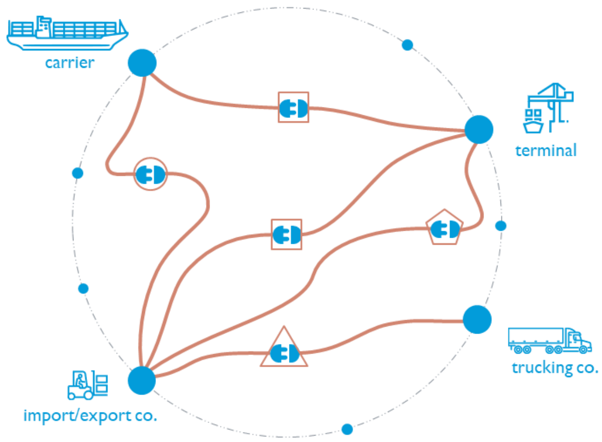
- Stakeholders must connect to a central platform
- Protocols and formats are determined by the platform
- All data pass through or are stored on the central platform

ADVANTAGE:

- Relatively easy to connect

DISADVANTAGE:

- Platform hosting cost
- Difficult to maintain data sovereignty



Decentral Connectivity

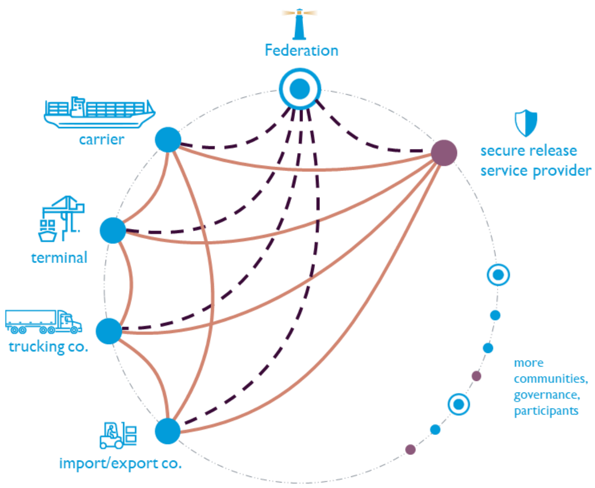
- Stakeholders are connected directly
- Middleware takes care of format mapping and orchestration
- Data is exchanged bilaterally

ADVANTAGE:

- Control over data can be maintained

DISADVANTAGE:

- Integration cost



Federated Network

- Stakeholders connect to their community of choice via federation services
- Protocols and formats are determined by the community
- Trust is established by the community governance
- Data is exchanged bilaterally

BEST OF BOTH WORLDS

- Relatively easy to connect
- Control over data can be maintained

- Choice of what community you want to join, whom you want to collaborate with

Data Space Design as a Foundation for PI

The Physical Internet (PI) requires a robust, scalable, and secure foundation to enable seamless collaboration across diverse logistics stakeholders. Data spaces provide an ideal architecture for meeting these needs.

Data spaces are designed to prioritize data **sovereignty**, allowing stakeholders to retain ownership and **control** over their data while participating in a collaborative network. The **federated** architecture of data spaces mirrors the decentralized nature of the PI, enabling collaboration without reliance on a single controlling entity. Data spaces facilitate discoverability and transparency while enabling accountability through event-based data sharing and real-time visibility into network activities. Data spaces are built on open standards and **modular** components, enabling seamless integration and **adaptability** to diverse logistics processes.

Separation of Concerns: A Layered Architecture

Data space architecture (Nagel & Lycklama, 2021b) addresses different concerns at different levels. It can be perceived as a layered architecture depicted in the below figure. We discuss each layer below and explain how and why this layered architecture can be used to implement a **Full Stack Physical Internet**.

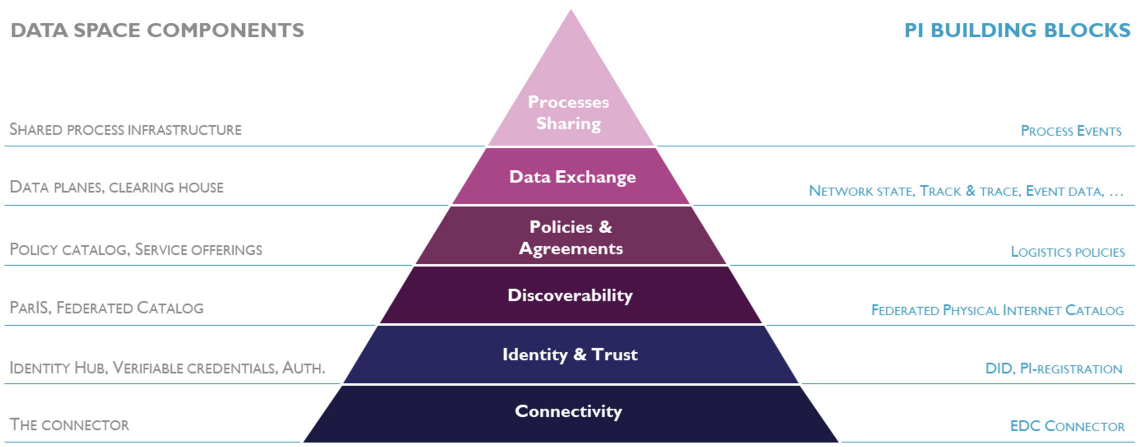


Figure 16: *A schematic mapping of data space and physical internet concerns onto architectural layers.*

Layer 1: Connector

The connector serves as the entry point for stakeholders to interact with the PI network. It facilitates secure communication, data exchange, and integration with local systems, enabling stakeholders to publish and consume data and services.

Standards:

- **Data space Connector** specifications (e.g., IDSA connectors).
- Open and standardized communication protocols like HTTPS, MQTT, and REST APIs.

Technical Components:

- Physical Internet Connector (PIC) tailored to PI use cases.
- Transport-layer security tools for encrypted data transfer.
- Plug-and-play modules for rapid deployment and integration.

Implementations: IDS Data Space Connector (IDS), Eclipse Data Space Connector(EDC), TRUsted Engineering (TRUE) Connector (Dam et al., 2023).

Layer 2: Identity & Trust

The identity and thrust layer manages stakeholder identities and ensures trust between participants. It governs authentication, authorization, and access control, enabling secure interactions across the decentralized network.

Standards:

- **W3C Decentralized Identifiers (DID)** for identity management.
- **Verifiable Credentials (VC)** for issuing and validating identity claims.
- Role-based and attribute-based access control standards.

Technical Components:

- Identity management systems using DID and VC frameworks.
- Access control modules for defining permissions and roles.
- Credential issuance and verification mechanisms.
- Federated identity services for cross-platform interoperability.

Implementations: Walt.id[6], DIDKit[7], IDWay

Layer 3: Discoverability

Discoverability facilitates the publication and discovery of logistics services and capabilities, enabling stakeholders to identify resources and optimize their operations dynamically. This may include the registration of participants in a community of collaboration. Participants can be onboarded as part of establishing trust. Membership of the community can be proven by means of a verifiable credential issued by the a party governing the community.

Standards:

- DCAT[8] for data publishing.
- Linked Data Event Streams (LDES) for synchronizing network states and event-based updates.
- Federated catalog protocols for service discovery.

Technical Components:

- Service catalogs and registries for publishing service metadata.
- Indexing and search tools to enable efficient discovery.
- Synchronization modules to maintain up-to-date service visibility.
- Participant Information System (ParIS).

Implementations:

- Many DCAT compatible implementations for data management and publication exist as DCAT is a well-established standard.
- Discoverability of logistics services was a key subject of the PILL project. At the time of writing, no established standard for logistics service publication exists. So implementation beyond PILL are limited and vendor-specific. For example: https://www.routescanner.com/ is a route finding application for cargo based on known logistics services, this is a centralized solution that could benefit from connecting with the PI.
- Existing scalable synchronization solutions exist, for example Home | LDES Server (https://informatievlaanderen.github.io/VSDS-LDESServer4J/3.3.0-SNAPSHOT/)
- Participant Information Systems are offered by some projects but not all as these are not a mandatory part of a data space. For example : Open-Core IDS Participant

[6] https://walt.id/
[7] https://www.sprucekit.dev/verifiable-digital-credentials/didkit
[8] https://www.w3.org/TR/vocab-dcat-3/

Information Service (https://github.com/International-Data-Spaces-Association/ParIS-open-core)

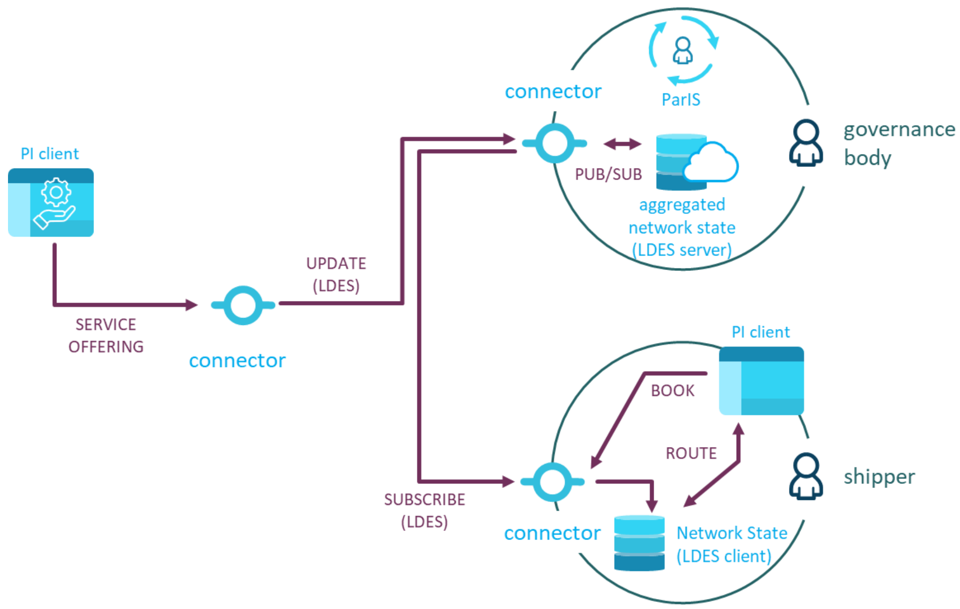


Figure 17: *High level architecture of the PILL discoverability feature implemented using data space connectors.*

Layer 4: Service descriptions and Policies

This layer provides formalized descriptions of services, their conditions of use, and associated policies. It ensures stakeholders can automate agreements and understand service capabilities.

Standards:

- Several **open specifications** for modeling processes, some based on BPMN exist. In the context of logistics several formalisms for sharing process data via events are proposed (Van Gessel & Hofman, 2023) which can also be used to denote specific processes.
- **Policy languages** like ODRL (Open Digital Rights Language) for expressing terms of use and service level agreements.

Technical Components:

- Policy enforcement engines for automating compliance checks.
- Frameworks for executing agreements dynamically.

Implementations: The event-based data sharing for logistics has a prototype implementation (https://github.com/tno/federated-bdi). Several implementations for ODRL exist as well. Examples are https://github.com/mosaicrown/policy-engine and https://gaia-x.eu/news-press/gaia-x-and-the-policy-reasoning-engine/.

Layer 5: Data sharing & interoperability

This layer ensures seamless data exchange across stakeholders while maintaining data sovereignty and regulatory compliance. It supports data transformation, validation, and integration.

Standards:

- **Interoperable formats**: JSON-LD, XML, and CSV for structured data exchange
- **Standard vocabularies and ontologies**
- **Open protocols** for data sharing such as HTTP(s) based formats LDES and REST, GraphQL, WebSocket, etc.

Technical Components:

- Data transformation tools for format compatibility.
- Secure data exchange platforms with encryption and validation.
- APIs for integrating local systems with the PI network.
- Federated query systems for accessing distributed data.

Implementations: Data sharing solutions are broadly available with many solutions and many semantic data schemas to choose from. In the context of logistics, particular standards of interest are UNCEFACT and derivatives and the FeDERATED ontology. In terms of open standards for exchanging events, LDES is available as a scalable approach.

Layer 6: Process Orchestration

The process orchestration layer coordinates logistics processes across multiple stakeholders by linking their operations into coherent workflows. It ensures smooth execution and real-time monitoring of collaborative processes.

Process orchestration begins with the exchange of process state within bilateral business relationships. But when an event in one process has an influence in another (dependent) process, the events should also be sent to the proper stakeholders there. This requires an event-based approach where events and their semantics are clear to everyone, so interoperability is an essential part of this.

Standards:

- Semantic notations for BPMN (Business Process Model and Notation) process definition and visualization.
- Event-based orchestration standards (e.g., FEDeRATED's process-sharing ontology).

- ISO standards for supply chain interoperability.

Technical Components:

- Orchestration engines for managing distributed workflows.
- Event-based APIs to synchronize process states.
- Event logging systems for real-time updates and audit trails.

Implementations

An example of an event-based architecture for sharing process data is the FeDERATED node prototype. (Hofman, n.d.). Most likely it is not the only example. What sets the FeDERATED node apart from typical solutions is the use of a semantic framework that allows alignment of events across stakeholders.

Another proposition for a process sharing framework, which is being implemented in a prototype environment, is discussed in an ALICE discussion paper(Maurin et al., 2024). Interestingly, the work describes a novel approach for data synchronization for efficient logistics data exchange which recognizes the need for flexibility at the level of logistics processes (Maurin & Liesa, 2024).

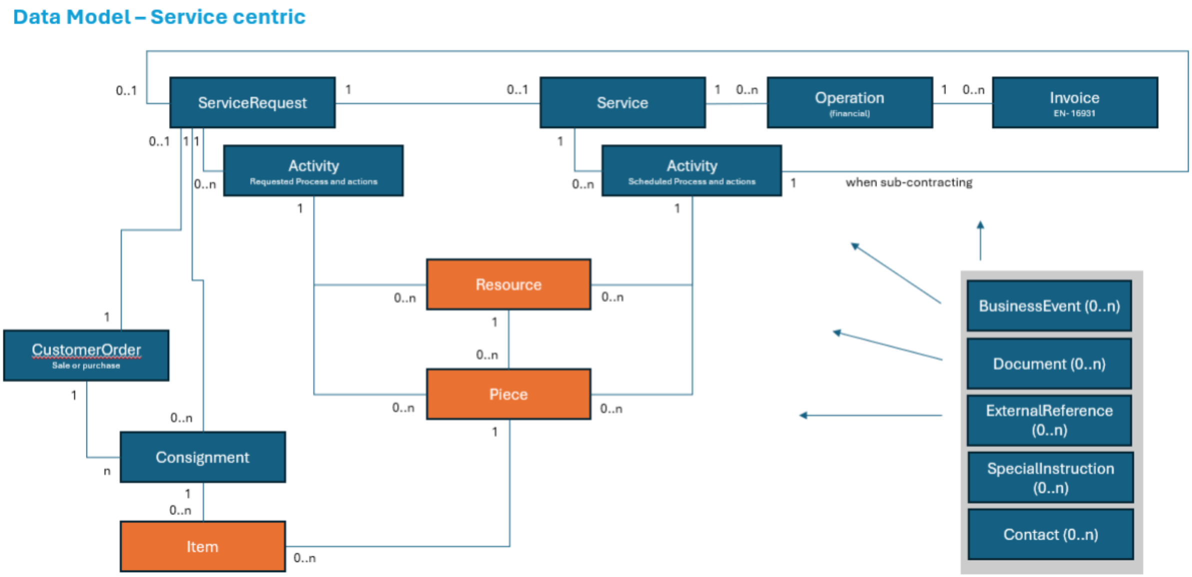


Figure 18: *The service centric data model introduced in(Maurin & Liesa, 2024)*

High Level Physical Internet Architecture

Connector Level

We envision a Physical Internet connector as a data space connector that exposes certain specific Physical Internet Services and APIs. We discuss every component below.

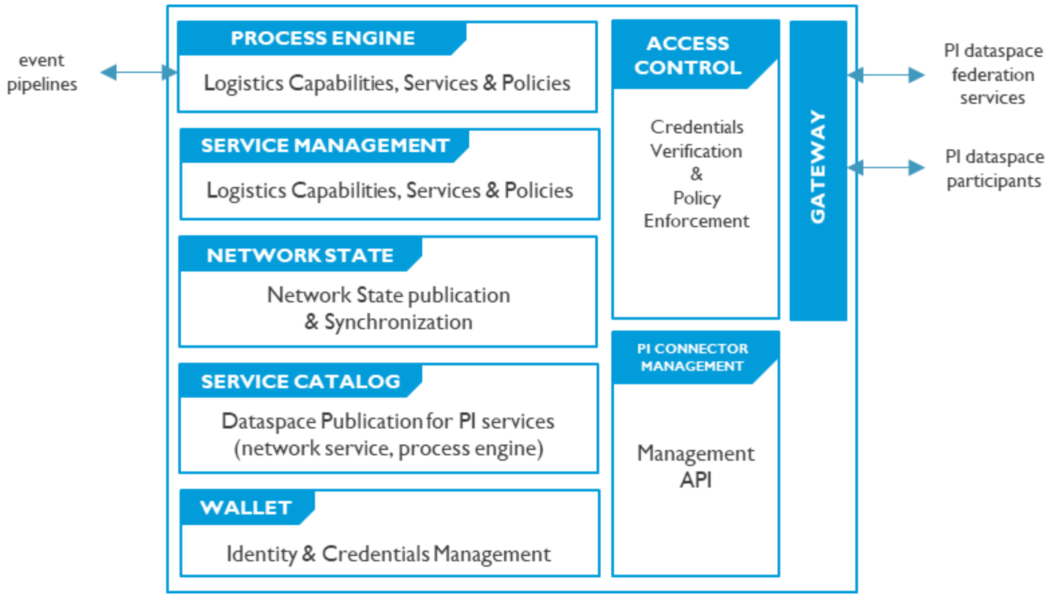


Figure 19: A schematic overview of the composition of a Physical Internet Connector

Wallet

The wallet manages digital identities (DIDs), credentials (VCs), and tokens necessary for authentication, authorization, and trust-building.

Service Catalog

The service catalog as a data space component that allows participants to publish their Physical Internet endpoints. These PI-specific endpoints are discussed below and distinguish a Physical Internet connector from a common data space connector. A PI connector is in that sense a PI-enabled data space connector.

Network State

The network state is a locally synchronized version of the network, filtered by the interest of the user in terms of geography, modalities, etc. The service subscribes a federated repository that contains metadata about participant and their capabilities, locations, and operational preferences in a standardized, machine-readable format. This functionality ensures that logistics services can be easily discovered and matched to specific needs, such as transport capacity, storage availability, or specialized handling requirements. This information can then be used for route discovery.

Service Management

The service management module allows stakeholders to publish logistics services along with their attributes such as modalities, pricing, schedules and capacities. In addition to that they contain the policies associated to these services that define the terms and conditions, access control, and the details of the services provided.

Any agreements for the use of the services are managed by this component as well such that future transactions (see process steps below) can be associated to a specific agreement.

Process Engine

The process engine is a PI-specific service that allows stakeholders to exchange process updates by means of events. These events are exchanged between the two connectors directly without the involvement of a central platform or orchestrator. Based on the pre-agreed policies that govern the service, these process steps are validated by the recipient

Access control

Access control ensures that event data is only sent and received to the endpoints of stakeholders that are involved in an ongoing agreement that are underpinned by predefined policies. These policies also define access control on individual data points ensuring data is disclosed selectively the right roles in the process.

Gateway

The gateway manages data exchange between the local systems of stakeholders and the PI network. It handles the routing of data to the proper components and can ensure that incoming requests have the proper authentication and authorization.

Management API

The management API provides an interface for configuring, monitoring, and managing the PI connector.

Event Pipelines

In the Physical Internet (PI), real-time synchronization of logistics processes across diverse systems is critical for achieving efficiency, transparency, and adaptability. Event pipelines play a pivotal role in enabling this synchronization by translating updates between proprietary backend systems and standard PI event formats. These pipelines act as a bridge, ensuring that logistics events are interoperable, actionable, and accessible across the PI network while preserving the integrity and functionality of stakeholders' existing systems.

One of the beneficial aspects of the PI connector as middleware is that the integration problem is reduced to the mapping of process data to standard events. All other integration concerns such as security, access control, orchestration, validation, etc. are shifted to the connector. This considerably lowers the integration cost.

Applications

The connector architecture provides a uniform way for applications to interact with network data. These applications include:

- Existing ERP systems that can leverage the Physical Internet to automate their systems;
- New applications that allow users to find routes for their cargo and book services;
- New web services that use network insights to optimize cargo flows across multiple stakeholders.

Network Level

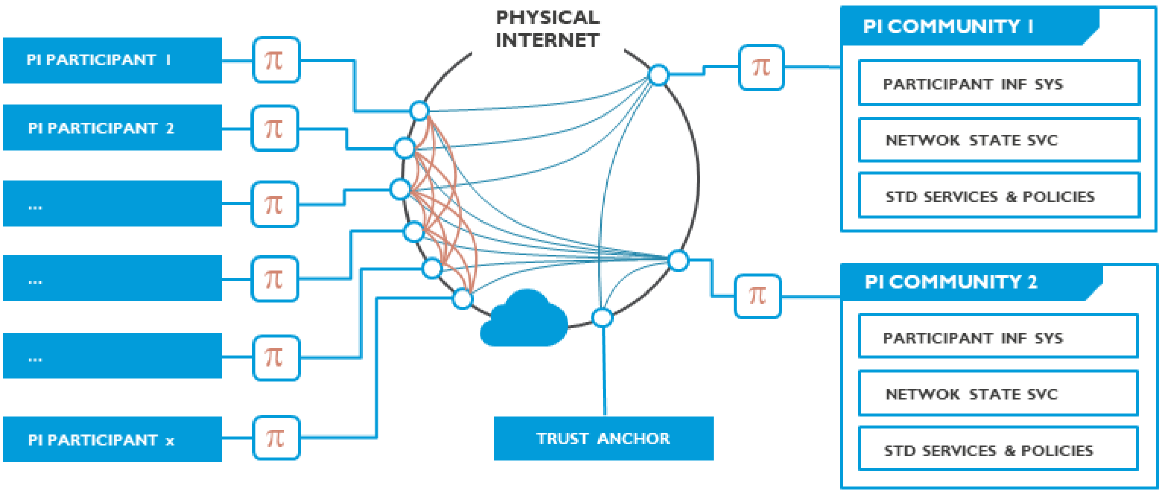


Figure 20: *A network deployment model for A schematic overview of the composition of the Physical Internet*

PI Participant

The participants connect their systems to the PI via a PI connector. Any actor can be a participant. A non-exhaustive list:

- Cargo shippers and receivers, in need of logistics services,
- Logistics service providers,
- Governance bodies representing PI communities and catering for trust and agreements among community members,

- IT service providers connecting platforms/data/algorithms to the PI, for instance, a service provider that enables cross-fleet optimization of trips for small and medium sized transport companies,
- Governmental actors allowing all other stakeholders to comply with regulation digitally, for example for customs declarations, dangerous goods regulations, eCMR verification, etc.
- Research institutions in need for real logistics process tracing data or testbeds for novel applications and services

PI Communities

PI communities are governed by an entity that is trusted by the community members and they are typically scoped by some parameters such as geography, kind of service, modality, ... All PI communities have a common foundation (standards) that allows participants to connect to multiple communities. Within each community, additional standards and agreements specific to that community can exist.

Trust Anchor

Trust anchors are dedicated digital service providers that are highly reliable, complying with the most stringent security standards, that are capable of issuing credentials on behalf of a community or stakeholder. They can be compared to the Certificate Authorities for SSL certificates on the Web. Trust anchors publish sets of public keys that allow third parties to independently verify the authenticity of the VCs they issue.

Participant Information System (ParIS)

The ParIS plays a crucial role in enabling discoverability within the Physical Internet (PI) by maintaining structured, up-to-date information about participants and their PI endpoints allowing services such as the Network State Service to aggregate data and to make it available to the participants.

In addition to discoverability, the ParIS is foundational for establishing trust within the ecosystem. It supports onboarding processes that verify participant identities and issue verifiable credentials (VCs) via a Trust Anchor to validate capabilities, compliance, and operational legitimacy. These VCs provide cryptographically secure and machine-readable proof of a participant's claims, enabling transparent, peer-to-peer interactions without reliance on a central system.

Network State (Aggregation) Service

The network state aggregation service real-time visibility into the current state of the logistics network. It aggregates, organizes, and shares information about the availability, status, and capabilities of resources such as transport routes, hubs, storage facilities, and transport modes. This information is vital for enabling efficient route planning, optimizing logistics operations, and maintaining resilience in the face of disruptions.

A federated approach to the Network State Service can ensure scalability and resilience by distributing its functionality across multiple stakeholders rather than centralizing it. This model allows each participant to manage and publish their network state data locally while contributing to a shared, interoperable view of the network.

Standard Services and Policies

Governance plays a pivotal role in the success of the Physical Internet (PI) by establishing the frameworks necessary to standardize logistics services and policies. A lack of uniformity in how logistics services are described, discovered, and managed can create inefficiencies, interoperability challenges, and barriers to adoption. Governance ensures that stakeholders across the logistics ecosystem can collaborate effectively while maintaining their unique operational practices and competitive advantages.

Next Steps for PI Implementation

Scaling the Physical Internet (PI) to its full potential involves addressing gaps in infrastructure, governance, and technology. While many mature components exist at the lower layers of the architecture (e.g., connectors and data-sharing protocols), higher-layer elements like discoverability, service descriptions, policies, and process orchestration remain less developed.

Infrastructure & Technology

The foundation of the Physical Internet (PI) relies on robust infrastructure and advanced technology to enable scalable, efficient, and secure operations. Developing and deploying **interoperable connectors** is critical for seamless data exchange between diverse logistics systems, ensuring inclusivity for stakeholders with varying technical capabilities. **Logistics service discoverability standards** are needed to standardize how services are published and found, allowing real-time optimization of supply chain operations. Similarly, **machine-readable service descriptions** empower automation by providing structured, actionable metadata about services, enabling faster planning and execution. At a higher level, **process orchestration standards and engines** are essential for coordinating complex logistics processes, allowing multiple stakeholders to work in harmony. Finally, **cross-organization workflow management** is vital for integrating individual logistics processes into cohesive end-to-end supply chains, ensuring the interoperability of independent workflows.

Governance, Policy and Regulation

Governance and policy frameworks are essential for creating a trusted and transparent PI ecosystem. **Standard policies** for data sharing, access control, and usage ensure that all participants operate under clear and consistent rules, enabling smoother collaboration. **Federated governance models** promote decentralized oversight, allowing participants to retain autonomy while ensuring accountability and fairness in a multi-stakeholder environment. **Business models** that provide fair compensation for shared resources and services are crucial for incentivizing participation, particularly among smaller players. Additionally, **regulatory support** plays a pivotal role in aligning PI with regional and global compliance standards, such as GDPR, ensuring data privacy and legal clarity across borders. These elements collectively build the necessary governance foundation to foster trust and adoption of the PI.

Stakeholder Engagement and Adoption

The success of the PI depends on **industry-wide engagement** to ensure broad adoption and effective integration across diverse stakeholders. To achieve this, trust must be established through secure data exchange mechanisms, transparent governance, and clear benefits for all participants. Smooth onboarding processes, supported by plug-and-play tools and comprehensive training resources, will lower adoption barriers, particularly for SMEs. Demonstration projects that showcase the practical benefits of PI—such as cost savings, improved efficiency, and enhanced resilience—are critical for building momentum and confidence among stakeholders. Encouraging collaboration through partnerships and knowledge-sharing initiatives will further strengthen stakeholder alignment, driving the widespread implementation of the PI vision.

Caveats of this Blueprint

Physical Interoperability

While much of this paper focuses on the digital dimensions of the Physical Internet (PI), **physical interoperability** remains a foundational pillar of its vision. Physical interoperability refers to the standardization of physical assets—such as containers, pallets, vehicles, and handling equipment—to ensure seamless integration and compatibility across logistics networks. Just as the Digital Internet relies on standardized data packets for efficient information transfer, the PI depends on modular, universally compatible physical units to enable efficient, flexible, and sustainable goods movement.

Key aspects of physical interoperability include:

- **Modular Containers**: Standardized containers of various sizes (from small parcel units to large freight containers) facilitate efficient loading, unloading, and transfer across diverse modes of transport, such as trucks, trains, and ships.
- **Intermodal Compatibility**: Ensuring that transport vehicles, handling systems, and infrastructure can accommodate standardized units eliminates inefficiencies and reduces handling times during transitions between modes.
- **Scalability and Resource Optimization**: Standardized physical units allow for easy consolidation and deconsolidation of shipments, optimizing space utilization and reducing empty transport miles.

Physical interoperability also supports sustainability goals by enabling better resource sharing and reducing waste in logistics operations. Achieving physical interoperability requires global collaboration on standards development, harmonized adoption across industries, and investments in compatible infrastructure.

Self-Routing in the Physical Internet

Self-routing of cargo using PI containers is inspired by how IP packets navigate in the Digital Internet. Cargo units carry "physical headers" embedded with digital metadata, including source, destination, routing preferences, and real-time updates. This data allows nodes in the logistics network to autonomously decide optimal routes based on current conditions like congestion, available resources, or disruptions.

For self-routing to work, seamless data exchange and process orchestration are essential. Cargo headers must interact dynamically with logistics nodes and systems, enabling decentralized, real-time decision-making. By integrating self-routing with robust data-sharing standards and process coordination, PI networks can adapt to disruptions, optimize resources, and meet diverse delivery priorities.

Self-routing eliminates reliance on centralized control, improving scalability, flexibility, and efficiency. Challenges such as standardizing cargo headers, retaining control over cargo flows, ensuring infrastructure readiness, and protecting data privacy must be addressed.

Conclusion

The Physical Internet (PI) represents a bold vision for transforming global logistics through interconnected, efficient, and sustainable networks. This paper has explored key aspects of PI implementation, focusing on infrastructure, governance, and technological advancements. While lower-layer components, such as data-sharing protocols and connectors, are relatively mature, significant gaps remain in higher-layer functionalities, including service discoverability, process orchestration, and workflow integration.

Federation, decentralization, Interoperability and trust

Central to the success of PI is the adoption of federated, data-driven approaches that prioritize decentralization, interoperability, and trust. Technologies like data space connectors, standardized service descriptions, and self-routing cargo highlight the potential for scalable, real-time collaboration. However, achieving PI's full potential also requires robust governance frameworks, regulatory support, and stakeholder engagement to address the complexities of multi-party logistics ecosystems.

The PI's emphasis on seamless data exchange, transparency, and autonomous decision-making offers immense opportunities for optimizing logistics networks. By bridging the remaining technological and organizational gaps, we can realize a globally interconnected logistics network that mirrors the adaptability and efficiency of the Digital Internet, delivering value for businesses, customers, and the environment alike. The road ahead demands collaboration, innovation, and commitment, but the transformative potential of the Physical Internet makes it a journey worth pursuing.

The need for Living Labs

Living labs are essential for advancing the Physical Internet (PI) by providing real-world environments where innovations can be tested, validated, and scaled collaboratively. They enable stakeholders to pilot technologies like self-routing cargo, data space connectors, and process orchestration engines under practical conditions, ensuring their feasibility and performance.

By fostering collaboration among logistics providers, technology developers, and policymakers, living labs build trust and address concerns around data sharing and governance. They showcase tangible benefits—such as cost savings, efficiency gains, and sustainability improvements—encouraging broader adoption of PI concepts. Additionally, they adapt PI solutions to regional and sector-specific needs while aligning regulatory frameworks with practical realities.

Living labs bridge the gap between theory and implementation, making them a critical tool for driving the PI roadmap and building an interconnected, resilient logistics network.

References

Cassan, C., Michiels, P., Sun, S., Lemos, V., Van Bever, D., Cant, A., Finck, J., & Macharis, C. (2023). *Data Sharing in the Physical Internet: A Capability-Based Approach for Trustless Logistic Networks*. https://www.pi.events/IPIC2023/sites/default/files/IPIC2023_Proceedings.pdf

Catena-X Operating Model Your Automotive Network. (n.d.).

Dam, T., Klausner, L. D., Neumaier, S., & Priebe, T. (2023). *A Survey of Data space Connector Implementations*. http://arxiv.org/abs/2309.11282

ETP ALICE. (202 C.E.). *Roadmap-to-Physical-Intenet-Executive-Version_Final*. https://www.etp-logistics.eu/wp-content/uploads/2020/11/Roadmap-to-Physical-Intenet-Executive-Version_Final.pdf

Hofman, W. (n.d.). *FEDeRATED node prototype development From concept to implementation*.

iSHARE Foundation. (2024). *iShare: Trust Framework for Data Spaces*. Https://Ishare.Eu/.

Lancker, D. Van, Colpaert, P., Delva, H., Van De Vyvere, B., Rojas Meléndez, J., Dedecker, R., Michiels, P., Buyle, R., De Craene, A., & Verborgh, R. (n.d.). *Publishing base registries as Linked Data Event Streams*. https://ogcapi.ogc.org/

Maurin, C., Ballot, E., Tiers, B., Ambra, T., & Liesa, F. (2024). *Discussion paper: A new level of data synchronization for efficient logistics data exchange*. https://eur-lex.europa.eu/EN/legal-content/summary/electronic-freight-transport-information.html

Maurin, C., & Liesa, F. (2024). *Workshop on Digitization and Data Sharing Discussion Paper*.

Montreuil, B., Meller, R. D., & Ballot, E. (2010). Towards a Physical Internet: the impact on logistics facilities and material handling systems design and innovation. *11th IMHRC Proceedings (Milwaukee, Wisconsin. USA – 2010)*, 40.

Montreuil, B., Meller, R. D., Ballot, E., Montreuil, B. ;, Meller, R. D. ;, Towards, ", & Paristech, M. (2010). *Towards a Physical Internet: the Impact on Logistics Facilities and Material Handling Systems Design and Innovation*. https://digitalcommons.georgiasouthern.edu/pmhr_2010/40

Nagel, L., & Lycklama, D. (2021a). *OPEN DEI Position Paper Design Principles for Data Spaces*. https://doi.org/10.5281/zenodo.5244997

Nagel, L., & Lycklama, D. (2021b). *OPEN DEI Position Paper Design Principles for Data Spaces*. https://doi.org/10.5281/zenodo.5244997

Raes, L., Michiels, P., Adolphi, T., Tampere, C., Dalianis, A., McAleer, S., & Kogut, P. (2022). DUET: A Framework for Building Interoperable and Trusted Digital Twins of Smart Cities. *IEEE Internet Computing*, *26*(3), 43–50. https://doi.org/10.1109/MIC.2021.3060962

Sun, S., Michiels, P., Macharis, C., Cant, A., & Mommens, K. (2024). *Unlocking the Potential of the Physical Internet: a Trust-enabling Decentralized Process Sharing Connector*.

Van Gessel, T., & Hofman, W. (2023). *An Interaction Pattern Ontology for Data Sharing about Logistics Activities*. http://ceur-ws.org