TWIN

twin.org

• TWIN Whitepaper

Reference Architecture

Trade Worldwide Information Network

Seamless Trading for All

Table of Contents

Trade Worldwide Information Network 1
Seamless Trading for All 1
TWIN Whitepaper 1
Table of Contents 2
Document information 4
- Revisions 4
- Credits 4
  - Rapporteurs 4
  - Technical vision 4
  - Other contributors 4

Executive Summary 5
Purpose and Scope 8
Introduction 9
- The Problem 9
- TWIN's Approach 10
  - Preliminary Concepts 11
  - High-Level View 13
  - Application Plane 14
  - Data & Services Plane 15
  - Infrastructure Plane 16
  - Example Scenario 17

TWIN Reference Architecture 18
- Design Principles 18
- Service Anatomy 20
- TWIN Trust Framework 22
  - Preliminary Concepts 22
  - Description 23
- Enabling and Federation Services 24
  - Participant Onboarding 26
- Visibility Services 26
  - Functional Overview 26
  - Auditable Item Services 27
  - Event Management 31
- Document Management Services 35
  - Functional Overview 35
  - Description and Functionalities 36

Data Exchange Services 42
Functional Overview 42
Service publication and discovery 44
Policy Management 46
Authentication and Authorization 48
TWIN Data Space Connector 49
TWIN Adaptor 52
Infrastructure services 52
DLT and TWIN 53
Edge Devices and Connectors 55
Common Platform Services 56
Local User Management and Policies 56
Glossary 58
Technology-related 58
Identity and Credentials 58
Data Spaces 60
DLT 61
Domain-specific 63
Value chains 63
International trade 65
References 67

Revisions

Version	Date	Comments
Draft-1	December 2024	First version
Draft-2	January 2025	Second version. Reviewed by the IOTA team.
Draft-3	February 2025	Version for partner's comment

Credits

Rapporteurs

José Manuel Cantera Fonseca, David Philips (IOTA)

Technical vision

José Manuel Cantera Fonseca, Christoph Strnadl, Martyn Janes, Michele Nati, Isaac Odhiambo (IOTA)

Other contributors

Jens Lund-Nielsen, Ian Clark, Andrew Brough, Antony Magayu, Adrian Grassl, Åsa Dahlborn, (IOTA)

Executive Summary

TWIN, *Trade Worldwide Information Network*, is an **open** and **interoperable** infrastructure and software platform for data integrity and self-sovereign data management. The TWIN infrastructure constitutes a digital pipeline accessible to all parties involved in different value chain ecosystems. By leveraging **Distributed Ledger Technology**[1] (public, permission-less blockchain), **Data Spaces**[2], **DID**[3] **and Verifiable Credentials**[4], TWIN ensures:

- Scalable and cost-effective data exchange.
- Verifiable data integrity and transparency, as blockchain's decentralized ledger securely records and verifies all data exchanges.
- Confidentiality, privacy and security.

TWIN technology can be used to build different solutions, such as:

- **Document and data exchange in international trade**, e.g. providing advance information throughout a consignment journey, including digital trade certificates to

[1] A public, permissionless **DLT** is a type of public ledger that is shared, replicated, and synchronized in a distributed and decentralized manner, and where permissions are not required to maintain and operate a node.

[2] The term '**Data Space**' refers to a type of data relationship between trusted partners who adhere to common high level standards and guidelines in relation to data storage and sharing within one or many vertical ecosystems. A critical aspect of Data Spaces is that data is not stored centrally but rather at the source. Thus, data is only transferred through semantic interoperability as necessary.

[3] A **Decentralized Identifier (DID)** is a unique, self-sovereign digital ID used to securely verify and manage identities without relying on central authorities.

[4] **Verifiable Credentials** are secure, tamper-proof digital certificates that prove the authenticity of an issued credential concerning the attributes or qualifications of an individual, organisation or thing (e.g. a shipment).

pre-clear consignments and minimise the frequency of manual document and physical inspections.

- **Environmental and sustainability compliance**[5], **declaration, and assessment** (provable with traceability evidence), particularly through the use of Digital Product Passports.
- **Supply chain visibility and optimization,** by increasing transparency and enabling data exchange and data verifiability through the use of Data Spaces and immutable ledger entries.

In an ecosystem of value chain partners, the TWIN digital pipeline is crucial as it fosters **collaboration** and **efficiency**. It allows stakeholders to access accurate and consistent data, enabling them to **make informed decisions** and **coordinate efforts seamlessly**. Additionally, it provides a comprehensive view of the ecosystem's performance, helping users to **identify issues early**, optimize operations, and innovate faster. In essence, TWIN empowers an **ecosystem** of users by promoting a unified, transparent, and data-driven approach.

TWIN's approach has already been tested and evaluated by the Trade Logistics Information Pipeline Project[6] (TLIP) in use cases involving the digitizing of consignment certificates in East Africa. Alongside the direct benefit of increasing speed and reducing errors in cross-border goods movement, TLIP brings the indirect benefit of creating touch-free information and document sharing. TLIP has been primarily focused on interactions with government and border agencies, but with the potential of seamless integration with private sector platforms through interoperable, open interfaces and open source connectors.

To **minimise digitalisation costs** and unnecessary changes, TWIN complements rather than replaces existing digital systems, enabling them to evolve and integrate into a **broader ecosystem** while preserving data integrity, sovereignty and privacy. It also democratises access to trade digitisation to micro, small and medium-sized enterprises (MSMEs), particularly in low and middle-income countries. As a result, potential export barriers can be overcome – for example, by making it easier to provide verifiable evidence of compliance with ESG regulations[7] aligned with [UN/CEFACT-Rec-49] recommendations.

From a technology viewpoint, TWIN aims at scaling the efficiency, transparency, traceability, interoperability and trust of value chain ecosystems by digitising processes. It offers open APIs

---

[5] Examples: EU's *ESPR Regulation* (Digital Product Passport) [EC-ESPR], the FDA's *Food Safety Modernization Act* [US-FSMA], or the *EU Deforestation Regulation* [EC-Deforestation] or several ESG standards and regulations.

[6] https://www.tlip.io

[7] https://en.wikipedia.org/wiki/Regulation_of_ESG_rating_in_the_European_Union

and formats based on open software standards and on the recommendations of global trade and economic intergovernmental organizations. It also pursues interoperability with the **Data Spaces** architectures as recommended by the Gaia-X Consortium [Gaia-X] and the International Data Spaces Association [IDSA-RAM-4]. Last but not least, the TWIN infrastructure incorporates the public, permissionless **IOTA** Distributed Ledger[8] off the shelf, a market leading Distributed Ledger Technology (DLT) project and ecosystem.

TWIN is an ongoing initiative that is the result of more than four years of research and development by the **IOTA Foundation** and its ecosystem, and is the recipient of sponsorship by non-governmental organizations (NGOs) – namely **Trademark Africa**, UK Chartered Institute of Export & International Trade (CIoE&IT) – and public funded research programs (EU Horizon).

TWIN is committed to open-source and open standards that foster innovation, prevent monopolistic practices and enable large-scale, global implementation. Thereby, the TWIN-specific software is **open source,** together with key parts of the underlying infrastructure – namely the IOTA DLT. At the same time, TWIN can work with and complement proprietary software that organizations might own. Both models can coexist in the open architecture of TWIN.

[8] https://iota.org

Purpose and Scope

This white paper describes the **Reference Architecture** that allows the implementation of TWIN (*Trade Worldwide Information Network*), an **open** and **interoperable** infrastructure and software platform for data integrity and self-sovereign data management. Here, we understand "architecture" as the fundamental organization of a system embodied in its components, as well as the relationships between the components to each other and to the environment. The architecture as described in this whitepaper is a reference point for any future solutions built on TWIN. Therefore, this document is intended for a technical audience – software architects, solution architects and software engineers – who want to understand the whole vision, problem landscape and outlined solution designs. Nonetheless, the introductory chapter can serve as a summary for those more generalist audiences.

This Reference Architecture whitepaper outlines our vision and long-term aspirations. However, at the time of writing, the TWIN software implementation is at varying levels of maturity. While some components are production-ready, notably those being used by TLIP, others are still in development, testing, or early conceptualization. During 2025, the TWIN open source codebase[9] will continue growing and the open source community governance models will be launched. Future technical whitepapers may address the design landscape of specific components or deployment aspects of the TWIN infrastructure and software platform.

For business-oriented audiences, several business-focussed background papers will be released during 2025 explaining in more detail how the TWIN technology is applied in different industries. The first of these papers, "*TWIN for International Trade*", will be made available on www.twin.org, explaining TWIN's approach to and suitability for international trade.

9

Introduction

The Problem

Modern **value chain ecosystems** are highly complex, involving not only many actors in both the public and private sectors but also different local and global regulations (*trading, sustainability, environmental, etc.)*. For example, international trade ecosystems involve actors playing different business roles (*buyer, seller, exporter, importer, border control agent, health inspector, certification body, insurance companies, banks*, etc.), multiple procedures and rules (regulatory, transport, etc.), and the exchange of multiple documents (*Invoice, Import/Export Declaration, product certificate, Bill of Lading, Digital Product Passport*,[10]etc.) and business process data.

In addition to the complexity described above, value chains also face a fundamental technical challenge: the absence of digital ecosystems that can support a collaborative, sustainable, circular economy, allowing multiple participants to interact (i.e. exchange data/documents/credentials) without *a priori* knowledge and on a need-to-know basis. However, to achieve this, there are several technical challenges to be tackled [as described by Gaia-X], namely:

- **Interoperability:** The lack of standardized systems, interfaces, and protocols creates barriers to interoperability, making it difficult to deliver seamless, end-to-end solutions.
- **Integration** (particularly legacy systems): Integrating disparate systems and technologies across different countries and industries without a common framework can be costly, time-consuming, and prone to errors.

[10] Digital Product Passports are part of new regulations and recommendations (**EU Ecodesign for Sustainable Products** [EU-ESPR], **UN/CEFACT Recommendation #49. Transparency at scale** [UN/CEFACT-Rec49]) where businesses can accredit sustainability compliance to border control agencies, market surveillance authorities, environmental control agencies or other businesses and consumers.

- **Data Sovereignty**: Ensuring that sharing data does not lead to potential risks: business leaks, or legal and compliance issues.
- **Limited Resources and Complexity**: Companies, especially smaller traders, often lack the resources to manage complex IT infrastructures or navigate intricate compliance requirements.
- **Vendor Lock-in**: The presence of ad-hoc integrations and bespoke applications makes it difficult to switch services or scale solutions.
- **Security and Compliance**: Mitigating the risks associated with data breaches, non-compliance, and third-party service providers.

To address the challenges listed above, several underlying factors must come into play:

- **Decentralization**: Designing a system with no single point of failure, no central information silos, and no single target of cybersecurity attacks, while harnessing network effects for simpler management.
- **Identity Management**, i.e. how different actors can be onboarded, issued an immutable digital identity, and start interacting in a trustworthy environment without a priori knowledge among them, and without the moderation of a central authority.
- **Information Management**, i.e. how to model and represent ecosystem's information such as data about items, documents, etc. in a way there is semantic interoperability and flexibility to accommodate different business needs and industry-specific particularities.
- **Data Exchange,** i.e. how actors can keep sovereignty of their data while establishing policies permitting data exchange and collaboration without intermediaries or the need to make complex changes to existing systems.
- **Data Verifiability and Authenticity,** i.e. how actors can verify the provenance and authenticity of the exchanged data.
- **Traceability, Immutability, and Transparency** in the interactions among actors and also concerning the assets they own. These are key to guaranteeing trust for frictionless collaboration that can solve disputes.

TWIN's Approach

Trade solutions based on centralized digital platforms[11] face not only scalability challenges but also resistance from the many actors within these complex ecosystems – especially when sharing sensitive data, such as Internet of Things-generated information, trade volume, commercially sensitive details, or personal data. This concentration of control can grant too much power to a single infrastructure provider while creating an attractive target for malicious actors. Furthermore, integrating different digital systems into a single proprietary infrastructure without well-defined open standards exposes organizations to the **risk of vendor lock-in**.

Additionally, most value chains are not linear, but rather dynamic compositions that cross industry boundaries (e.g. the automotive sector is composed of metals, plastic, textile, etc.) and jurisdictional boundaries (e.g. materials or parts can be sourced from multiple countries). Actually, value chains **intersect** at **multiple points**, which poses interoperability challenges. Thus, actors have to gather data from different parties, and, as the number of stakeholders and value chains increase, the problem of data interoperability, verification, authorization, and authentication intensifies. This is critical for both governments (border control agencies, market surveillance authorities, etc.) and businesses (customs brokers, freight forwarders, carriers, ports, manufacturers, recyclers, importers, etc.).

Our proposed architecture revolves around a **TWIN Node**, a modular agent with open interfaces that facilitates participation in a TWIN Ecosystem without requiring ad-hoc integration between trading partners' IT systems. A TWIN Node encompasses all required infrastructure – including hardware infrastructure, processing, data storage and object storage, and DLT – and platform software services essential for managing information in value chains. It also integrates the core TWIN functionality, which facilitates the exchange of data and documents such as certificates and credentials. TWIN Nodes can run within Participants' own data centers or, alternatively, a Participant can be onboarded and authorized to make use of the services offered by a TWIN Node provided by a third party (Node as a Service).

However, it is noteworthy that there is no vendor or technology lock-in in our approach. In fact, it is not even necessary to deploy a TWIN Node in order to participate in a TWIN Ecosystem The paramount goal is to comply with the rules established by the governance of each TWIN Ecosystem, and at least offer a public, open interface compliant with TWIN – called a **TWIN Data Space Connector** – for data exchange. This unique approach enables existing supply chains and third-party platforms to seamlessly evolve from silos to ecosystem Participants, leading to real, digital value chains for the benefit of governments, businesses, and consumers.TWIN Architecture Overview

To understand TWIN and its vision, it is necessary to put different concepts into context.

---

[11] https://wisechainconsult.substack.com/p/8-why-did-tradelens-failed-and-and

Preliminary Concepts

In alignment with Gaia-X principles[12] the following ecosystem-related definitions are in scope:

- **TWIN Ecosystem**: A value/supply chain ecosystem composed of: the *governance,* which defines the set of *rules* agreed upon by the ecosystem's parties and its implementation; and *infrastructure* - i.e., hardware and software for computing, storage, and network services, which adopts the rules defined by the governance.
- **Governance:** This defines the rights and duties of formal data management, ensuring quality and trust throughout a TWIN Ecosystem. This is mission-critical to TWIN, given that a central supervisory authority is missing by design.
- **Participant**: An actor who participates in a TWIN Ecosystem. Through a TWIN Ecosystem, Participants collaborate towards a common goal: the efficiency and effectiveness of global trade and supply/value chain processes. Participants adopt the *governance*, using the ecosystem's *infrastructures* "*to access and use data in a fair, transparent, proportionate and/non-discriminatory manner with clear and trustworthy data governance mechanisms*."[13] The Participant can have one of two main roles:
    - **Consumer:** A Participant (or a service acting on their behalf) who searches Service Offerings and consumes service instances (for example, a service that allows fetching trade documents) in a TWIN Ecosystem.
    - **Provider:** A Participant who operates service instances in a TWIN Ecosystem and publishes them as one or more *Service Offerings* through Service-Offering credentials. For instance, a data Provider makes data available in a TWIN Ecosystem to be transmitted to a data Consumer.

In addition, the following related technical concepts are paramount:

- **TWIN Node**: Infrastructure and platform software (agent) that enables Participants to interact within a TWIN ecosystem. A TWIN Node encompasses several service instances that can be published to the TWIN Catalog as Service Offerings.
- **TWIN Adaptor**: The technical component that acts as a **software bridge** adapting the proprietary formats and API calls of an origin IT system (that needs to take part in a TWIN Ecosystem) to the protocol and formats of a TWIN Data Space Connector.
- **TWIN Data Space Connector** (TWIN DS Connector): The technical core component of the **Data Exchange Services** of a TWIN Node.

---

[12] https://docs.gaia-x.eu/technical-committee/architecture-document/24.04/gx_conceptual_model/

[13] https://interoperable-europe.ec.europa.eu/collection/semic-support-centre/data-spaces

- **TWIN Catalog:** A Federation Service that realizes the catalog of compliant Participants, Data Resources and Service-Offerings, enabling their registration and discovery.
- **TWIN Native Solution:** A software system that solves a particular customer problem by participating in a TWIN Ecosystem through the services offered by a TWIN Node.

High-Level View

Figure 1 describes a basic overview of the TWIN Architecture gravitating around TWIN Nodes. From top to bottom, three main planes can be distinguished:

- The **Application Plane** consists of applications and services that deliver solutions aligned with value chains by leveraging the capabilities provided by the Data & Services Plane.
- The **Data & Services Plane** is embodied by TWIN Nodes and the software services they provide, particularly Data Exchange Services, with the TWIN DS Connector as its core component.
- The **Infrastructure Plane** consists of the software infrastructure that facilitates decentralization, data sovereignty and availability, discovery and trust. A central element of this plane is the TWIN Catalog.

The TWIN architecture incorporates a core component known as the **Decentralized Trust Framework,** which facilitates self-sovereign Participants and Service Offerings onboarding, governed by rules specific to each ecosystem. This framework is designed to ensure interoperability with Gaia-X and EU Common European Data Space recommendations [EU-Data-Spaces] and is built on **W3C Decentralized Identities** [W3C-DID-Core], **W3C Verifiable Credentials** [W3C-VC-DATA-MODEL], and **Trust Anchors**[14]. It enables the implementation of data-sharing policies through attribute-based access control, ensuring secure and regulated data exchange. [15]

[14] https://docs.gaia-x.eu/technical-committee/architecture-document/24.04/component_details/#gaia-x-trust-anchors

[15] https://docs.gaia-x.eu/technical-committee/identity-credential-access-management/24.07/trustframework_implementation/

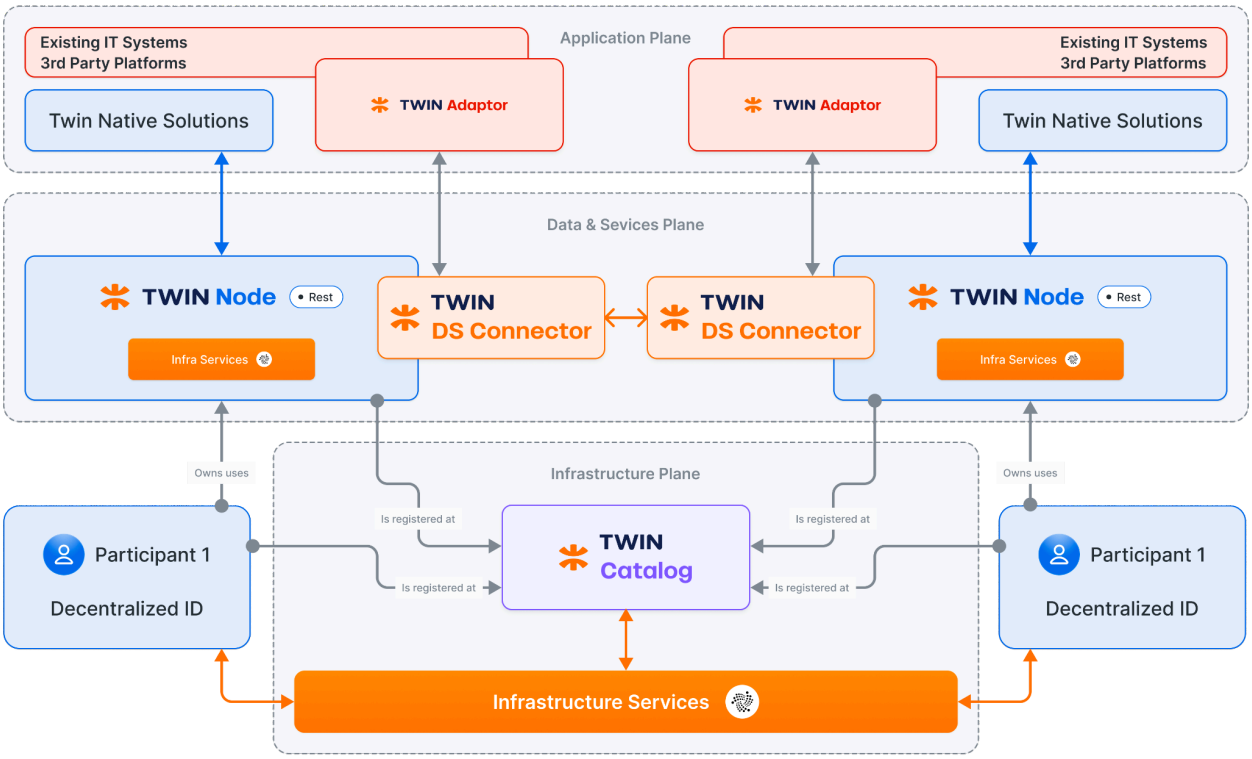


Figure 1 TWIN Node(s) and their interactions

Application Plane

The Application Plane includes:

- **Existing or legacy IT Systems** that can participate in TWIN ecosystems through a TWIN Adaptor. They could be government-owned Single Window Systems, trade operations systems, Enterprise Resource Planning systems, sustainability management systems (which are the source of sustainability data like carbon intensity), customs broker Solutions, automated compliance checkers, etc.
- **TWIN Native Solutions** such as track and trace solutions, custom dashboards that allow users to monitor the status of consignments of interest, automated checkers for consignment clearance at borders based on Artificial Intelligence, analytics tools, trade finance tools, etc.

  TWIN Native Solutions can interact directly with a TWIN Node, performing read and write operations. These interactions happen through open Web APIs that involve payloads represented by industry-standard JSON-LD Vocabularies [W3C-JSON-LD] (GS1 Web

Vocabulary[16], schema.org[17], UN/CEFACT BSP[18], etc.) The use of these standards enables semantic interoperability, so all exchanged data is machine-readable and unambiguous to participants.

- **Third-party, cloud-native, digital platforms** can also complement a TWIN Ecosystem. These are IoT platforms that supply real-time data points along the trade journey and Track and Trace (traceability) platforms that supply real-time data points giving visibility to the flow of goods and tracing products, materials, or components across a value chain.

Data & Services Plane

TWIN Nodes are the core of the Data & Services Plane. Apart from offering value chain visibility and document management services, TWIN Nodes can share data and documents with other TWIN Nodes and existing systems or third-party platforms. Actually, through TWIN Nodes, Participants exercise **sovereign control** over their data, i.e. they can choose which documents or data they wish to share and with whom. Each business or government can own one or more TWIN Nodes. For discovery purposes, TWIN Nodes need to be **registered** by a participant in the TWIN Catalog. Each application may interface with one or more TWIN Nodes according to internal policies, data availability, etc.

At any time, an authorised participant can query a TWIN Node for information about a specific item in the supply chain (e.g., a consignment or shipment). When needed, the TWIN Node can delegate the request to other TWIN Nodes or third-party applications – discovered through the TWIN Catalog – effectively acting as a broker.

The interaction among different TWIN Nodes happens through a **TWIN Data Space Connector** (TWIN DS Connector)**,** whereas existing IT systems can interact with TWIN Nodes by implementing a **TWIN Adaptor** that in turn speaks to a TWIN DS Connector. The interactions happening through a TWIN Data Space Connector (realized through Web APIs, i.e. REST or Websocket) are either directly related to fetching specific resources (documents, items, etc.) or receiving notifications of “events of interest”. While the former does not mutate the state of the receiver Node, the latter could. For instance, notification of the availability of a new document will result in the mutation of an item and, optionally, the storage of the document on the receiving Node.

TWIN DS Connectors and TWIN Adaptors are actually registered in the TWIN Catalog as Service Offerings and Data Resources so that Participants or other services (offered by TWIN

[16] https://ref.gs1.org/voc/

[17] https://schema.org

[18] https://vocabulary.uncefact.org

Nodes) can discover them when needed. The registration shall be accompanied by metadata including, for example, the jurisdiction for which data/documents are provided, the associated policies, the type of document/data items provided, etc. All these descriptions are represented using Linked Data Vocabularies – namely, the Gaia-X Ontology[19], the GS1 Web Vocabulary, the UN/CEFACT BSP Vocabulary, or Schema.org.

It is envisaged that general-purpose extensions can also be deployed as additional services to complement the core of a TWIN Node (*TWIN Apps*), for instance, to implement a custom protocol or format for a certain supply chain subdomain. Another example is a TWIN App that is deployed to interface with an external OCR software as a service provider so that scanned documents' data points can be extracted and persisted, as structured data, to the Node.

Infrastructure Plane

On this plane, several infrastructure software services appear, namely:

- The **TWIN Catalog**, a decentralized registry of Participants, Service Offerings (particularly those exposed by TWIN Nodes) and Data Resources that enable discovery, i.e. it can be queried to know who can provide which data, together with endpoints and data exchange policies.
- A **Verifiable Registry**, implemented by IOTA DLT technology, that contains traceable and immutable objects, namely a Participant's Decentralized Identities.
- Datastores, object stores, key management systems, etc. that facilitate (secure) data storage and availability.

Besides, **physical, edge devices** (such as RFID Readers, scanners, printers, mobile sensors, …) can also be part of the TWIN infrastructure, as they connect the physical world of trade items to the digital world, improving automated identification and data capture tasks. Devices manufactured by Zebra Technologies (namely fixed RFID Readers exposing the Zebra IoT Connector and Android scanners) have already been successfully tested[20] to interoperate with TWIN through their corresponding Edge Connectors (see Edge Devices and Connectors).

Example Scenario

The data exchange scenario can be better conceptualized through the example by Figure 2 , involving cross-border data/document exchange in international trade (one of the fundamental use cases of TWIN).

---

[19] https://docs.gaia-x.eu/ontology/development/

[20] https://developer.zebra.com/blog/introducing-zebra-iota-edge-sdk

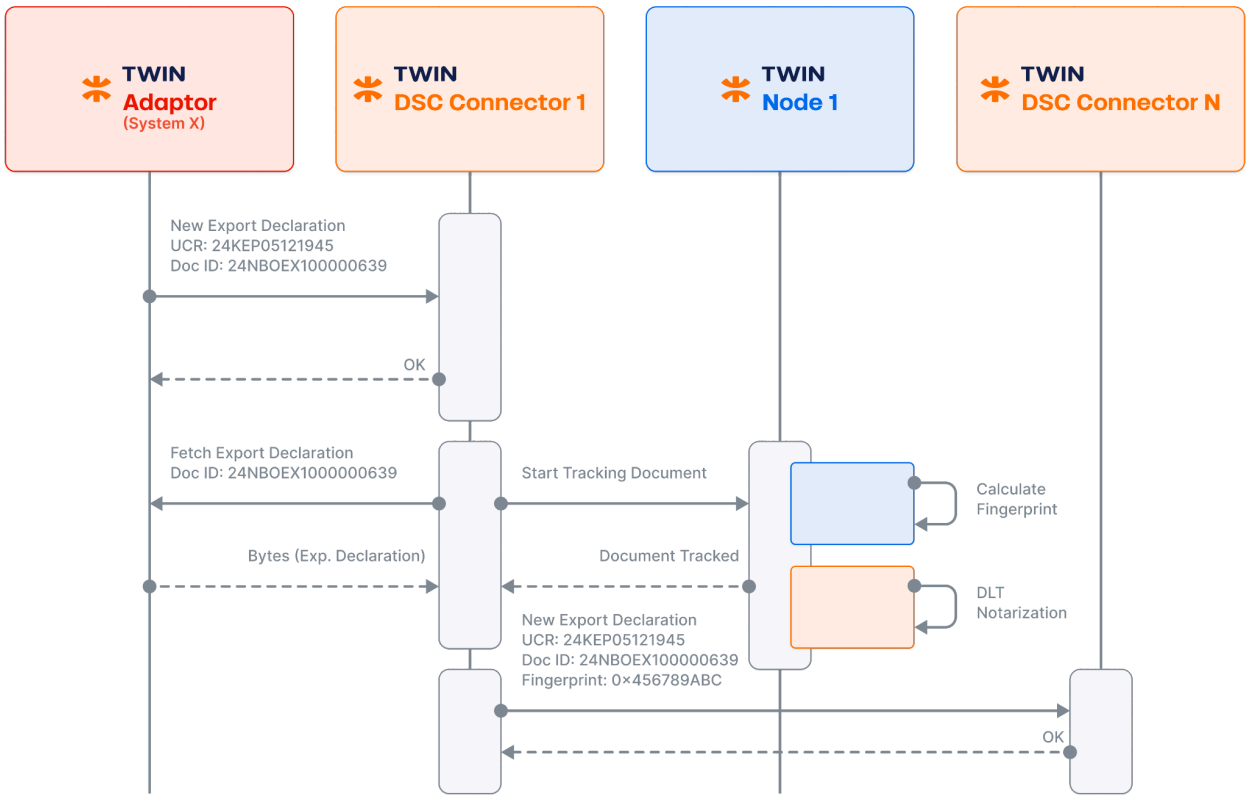


Figure 2 Scenario of interaction in a typical cross-border document exchange

When a trade document is issued (such as an *export declaration* as in the example above), an external, existing IT System that has implemented a TWIN Adaptor (for instance a Single Window System) can publish this activity information through a target Node's DS Connector. The TWIN Node can then start tracking the new trade document, preventing potential tampering (by first checking for the document's authenticity and then calculating and storing a fingerprint[21]). It is important to note that trade documents can remain at the source and only be revealed (through the mediation of a TWIN Node) to participants authorized by the document provider. The sharing policies are declared and published to the TWIN Catalog by the document's provider by means of a standard and interoperable language – W3C ODRL [W3C-ODRL-22] – referenced through a self-issued W3C Verifiable Credential (Service-Offering Credential).

On the other hand, we can imagine the destination country, namely border control agencies, being notified of the existence of an export declaration before the consignment arrival, for the

[21] There can be cases where the document is fully notarized in a DLT or even tokenized for further transfer operations

sake of efficiency and preparedness. In fact, the figure above shows another TWIN DS Connector that is also notified about the existence of the export declaration. This is feasible, as a TWIN DS Connector also offers a subscription interface that enables authorized Participants to subscribe to events of their interest that will be received by their respective TWIN Nodes.

TWIN Reference Architecture

Design Principles

The main technical design principles that guide the TWIN Reference Architecture are:

- **Interoperability:** To guarantee mainstream adoption, systems and solutions “Powered by TWIN” must be interoperable. This enables TWIN value chain ecosystems to grow quickly and smoothly without incurring high integration costs, stimulating participation and removing entry barriers. Interoperability requires addressing the **architecture, protocol, payload and policy** aspects of TWIN as a software product, in alignment with relevant standards.
- **Data at the source**: Instead of creating new systems, TWIN aims at interworking with existing ones and facilitating their expansion by integrating off-the-shelf software components and libraries that expose standardised open APIs. As a result, the exchange or sharing of existing data, rather than creation of new copies of them, can be achieved. The use of distributed ledger technology guarantees that exchanged data remains immutable and their source verified, thus increasing accountability and minimizing mistakes and fraud.
- **Data owner controls access**: Data Providers must be guaranteed direct control (**data sovereignty**) over who can access their data (and for which purpose), thus enforcing privacy and confidentiality. In TWIN, there are no central actors (i.e., platform owners) with privileged positions. Data Providers can start new relationships intended to exchange data at their own will and thus create an attractive market for solution providers to compete in providing new services.
- **Confidentiality and privacy**: Data security must be ensured, allowing access only to rightful parties on a need-to-know basis. Additionally, safeguards should prevent publicly shared value chain data from being exploited by other parties, such as competitors, for their own advantage.

- **Decentralized data/document sharing and verification**: In accordance with the principles of decentralized technology, data and document sharing among stakeholders – as well as the verification of their authenticity and integrity – shall be achieved without any intermediaries. Participants will be able to discover one another and securely share, exchange, and verify data/documents without the intervention of a central, privileged organization or intermediary.
- **Data minimization and selective disclosure**: For data and document sharing, it must be possible to expose only the minimal amount of information needed by other trade and supply chain Participants, for instance by enabling selective disclosure at fine-grained levels.
- **Open-Closed alignment with international standards**: To ensure interoperability, TWIN does not intend to create new standards but rather to adopt existing, relevant ones while allowing for extensions. For digital twin representation, TWIN endorses GS1 Web Vocabulary and schema.org, among others, while being ready to support other vocabularies based on JSON-LD and Linked Data principles[22]. For supply chain visibility, it aligns with GS1 EPCIS 2.0, [GS1-EPCIS], which is inherently extensible. Concerning Digital Identity, TWIN adheres to W3C standards, and, for Data Space and ecosystem aspects, it follows Gaia-X and International Data Spaces Reference Architecture (IDSA) models.

[22] https://www.w3.org/wiki/LinkedData

Service Anatomy

Figure 3 shows a functional overview of the architecture of TWIN aligned with the design principles outlined above and gravitating around the TWIN Node.

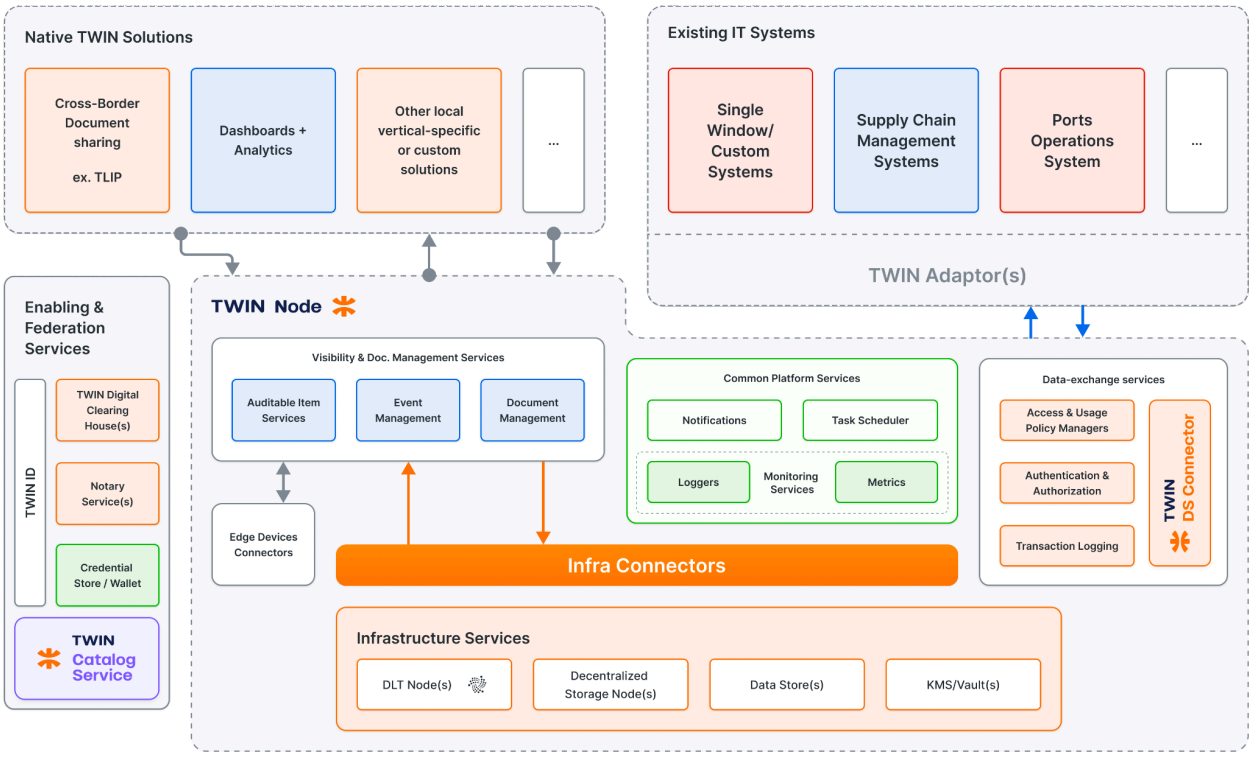


Figure 3 Anatomy of a TWIN Node and service categories

Different software services are classified under the following categories:

- **Enabling & Federation Services**, which realize the clearance, publication, and discovery of participants and the services they publish so that decentralized interactions can take place. Authorization policies, depending on each ecosystem's governance, might also apply to these services for security and privacy reasons.

  The *TWIN Catalog*, depicted in the figure above, is a key component of TWIN's architecture as it contains all the information about Participants, Service-Offerings, Data Resources, and their policies (represented using W3C ODRL).

- **Visibility Services,** They provide auditable digital representations of objects – digital twins – through their properties, relationships, business events (based on GS1 EPCIS 2.0 and its extensions) traceability data, and related resources (for instance, associated

documents or external data resources). Visibility Services are designed to be application-agnostic, relying on open standards, including Linked Data Vocabularies (schema.org, GS1, UN/CEFACT) and REST APIs.

- **Document Management Services** facilitate document storage (including multiple versions of the same document) document resolution, document traceability, authenticity, and attestation (possibly on-chain through NFT tokenization), data extraction, and document transformation, including multiple representations as per different industry standards (W3C VC, eInvoice, eBill of Lading, etc[23].). Document transfer, as per the Model Law on Electronic Transferable Records (MLETR) [UNCITRAL-MLETR], via IOTA DLT tokenization, is also under the scope of these services.

- **Data Exchange Services** facilitate data and document exchange between the different ecosystem participants. The main enabler on the TWIN Node side is the TWIN DS Connector, which exposes query and publish/subscribe REST endpoints.

- **Infrastructure (Software) Services** realize the software infrastructure needed for a TWIN Node to operate, namely, public, permissionless distributed ledger technology, object storage, data stores, and cryptographic key stores.

- **Infrastructure Connectors** are generic technical core components of the architecture that abstract away the specific interfaces of infrastructure services from the rest of the services present in a TWIN Node. As a result, there is loose coupling and improved flexibility concerning the underlying infrastructure. One noteworthy Infrastructure Connector is the *IOTA DLT Connector*, which is key for trust and data verification within a TWIN ecosystem.

- **Edge Connectors** are connectors that bridge the physical world of trade items with their corresponding digital twin. *Edge devices* (such as RFID readers, mobile scanners, and mobile sensors) are part of the physical infrastructure, and Edge Connectors enable data to be captured seamlessly and object presence to be recognized, recorded, and attested on TWIN. Additionally, accessibility to trade item information held by TWIN can be improved (for instance by reading or printing barcodes).

- **Common Platform Services** are general-purpose, reusable services that provide horizontal functions. Task scheduling, background tasks, notification delivery (messaging), metrics, and monitoring (telemetry) are some of the most noteworthy ones.

All TWIN software services offer REST APIs using JSON(-LD) as the data representation format. There is a high level of flexibility when deploying those services (packaged as Docker containers), from a monolithic deployment to a full micro-service split.

---

[23] A list of comprehensive key trade documents can be found at https://www.dsi.iccwbo.org/_files/ugd/8e49a6_9f8444133fc64fc9b59fc2eaaca2888e.pdf

In addition to the above-referred software infrastructure, a TWIN Node must execute within a hardware infrastructure that encompasses computing, storage, and networking resources. Such a hardware infrastructure might be virtualized (IaaS) and be offered by cloud providers in conjunction with PaaS (containerization, clusterization, i.e. Kubernetes, etc.) capabilities. Nonetheless, TWIN Nodes including the TWIN software infrastructure services (datastores, DLT, etc.), are also ready to be executed on-premise when required by organizations. In a nutshell, TWIN is not bound to any particular cloud provider or hardware platform. The deployment view of the architecture is out of the scope of this white paper and will be discussed in future documents.

TWIN Trust Framework

Additional and complementary definitions concerning this section can be found in the glossary.

Preliminary Concepts

According to Gaia-X[24], **Trust Frameworks** establish the rules that ensure minimum requirements are met for security, privacy, identification management, and interoperability through *accreditation and governance*. These operating **rules** provide a common framework for ecosystem participants, thereby increasing trust between them. The TWIN Trust Framework revolves around the following concepts:

- **Participant Identity:** A Decentralized Identifier (DID) plus other attributes related to a Participant.
- **Participant Attribute:** The identities of Participants in a TWIN Ecosystem rely on signed attributes, which can be requested and exchanged to gain individual trust from other participants. Participant Attributes might also be extracted from Verifiable Credentials which subject is the Participant itself.
- **Participant Credential:** A type of Verifiable Credential that attests Participant Attributes. For example, a Legal Entity Credential attests the attributes of a legal entity, such as legal name, registered domain, residence country, etc.
- **Trust Anchor:** A Participant (such as a Conformity Assessment Body) accredited to issue attestations about specific claims. How the accreditation of Trust Anchors works depends on each TWIN Ecosystem's rules. There can be even regular Participants, for example prominent organizations such as freight forwarders, that also play the role of Trust Anchors.

---

24 https://docs.gaia-x.eu/technical-committee/architecture-document/24.04/context/#gaia-x-trust-framework

- **Trust Anchor Credential:** A type of Verifiable Credential**,** it's purpose is to provide a machine-readable representation of the accreditation of a Trust Anchor for a specific scope, vocabulary or schema. There are several specializations: *Organization Trust Anchor Credential* is held by an organization that can onboard other Participants within the ecosystem, while an *Ecosystem Trust Anchor Credential is* held by an organization that is entitled to define the rules of a particular ecosystem.
- **TWIN Clearing House:** A decentralized compliance verification service that assesses Participants, Data Resources or Service-Offerings against predefined requirements. Upon successful validation, it issues a Compliance Credential.
- **Participant Compliance Credential:** A Verifiable Credential that attests that a Participant is compliant with the rules defined by a TWIN Ecosystem. Participants need a Compliance Credential to be registered in a TWIN Catalog.

Description

TWIN adheres to a **Trust Framework**, which enables the attestation of Participants' attributes and their seamless onboarding and interaction **without prior knowledge** among them. The final aim is to ensure that all Participants in a TWIN Ecosystem are adhering to the policy rules agreed between the Participants of the Ecosystem itself.

The Trust Framework revolves around the following rules:

- Participants are identified by a *W3C DID* held in a Credential Wallet, either directly controlled or kept in custody by a third party. Even though TWIN is not bound to any particular DID method, it provides off-the-shelf support for IOTA Identity[25], thus DLT infrastructure might act as a verifiable data registry.
- Participants' Attributes are attested by other Participants (**Trust Anchors**) through W3C Verifiable Credentials. Trust Anchors can be accredited by other Trust Anchors.
- Trust Anchors are defined by each TWIN Ecosystem. While there can be ecosystems with pre-defined, prominent Trust Anchors (for instance government agencies, private institutions, or banks, etc.), other ecosystems might be more lenient when it comes to attestation. For instance, an existing, compliant Participant might attest to the attributes of Participants it wants to interact with.
- Participants must be compliant with each ecosystem's rules. Once a Participant has been attested to possess certain attributes it must acquire a **Compliance Credential** through a TWIN Clearing House. A **TWIN Clearing House** must check for Compliance

[25] https://docs.iota.org/iota-identity/

as per the rules of each ecosystem. Compliance Credentials are the pass needed to appear under the TWIN Catalog.

Smart contracts are a good fit for the implementation of TWIN Clearing Houses. They guarantee clearance rules traceability, transparent onboarding processes, and immutability, enabling decentralization and seamless ecosystem governance.

- Ecosystem rules which include participation rules, schemas, vocabularies, etc. should be ideally registered on a **TWIN Registry** for traceability and immutability purposes, and be accessible to any TWIN Node and Clearing House.

  External Trust Service Providers (also playing the role of Trust Anchor) through their controlled trusted data sources are allowed to be part of the TWIN Trust Framework. Building on the concept of Gaia-X Notary[26], when these providers are not capable of issuing cryptographic material nor signing claims directly, then a TWIN Ecosystem can accredit one or more **TWIN Notaries** to do so.

  Example: The European Commission provides several APIs, including one to check the validity of EORI numbers. Unfortunately, those APIs are not returning Verifiable Credentials. A TWIN Notary service can be accredited by a TWIN ecosystem as the Trusted Data source for EORI validation and issue Verifiable Credentials to attest to EORI numbers.

- Compliance credentials and their evidence (also represented as Verifiable Credentials) are subject to **revocation**. As revocation lists are DLT registry entries, they can reach TWIN Nodes and be effective immediately. As a result, bad actors can be dismissed and offboarded from a TWIN ecosystem in a very efficient and effective manner.

Enabling and Federation Services

The Enabling and Federation services encompass:

- The **TWIN ID** Application service orchestrator with an accompanying UI intended for seamless onboarding of Participants and the Services they publish.
- The Credential Manager (**Wallet**) which receives, stores, presents, and manages Verifiable Credentials and cryptographic key material, possibly using a Key Management System.

---

26 https://docs.gaia-x.eu/technical-committee/architecture-document/24.04/component_details/#gaia-x-trusted-data-sources-and-gaia-x-notaries

- The **TWIN Catalog**, a federated or sufficiently decentralized service that keeps a record of the different compliant Participants and the Services they publish.
- **Identity Service Providers** that can verify and attest the identity of Participants enabling KYC.
- **TWIN Notaries,** a service that, in collaboration with an external trust service provider, attests a Participant's specific attributes.
- The **TWIN Clearing House**, which checks the compliance of Participants and Services in accordance with the ecosystem's rules represented as records in the TWIN Registry

The interaction among these services is depicted by figure 4:

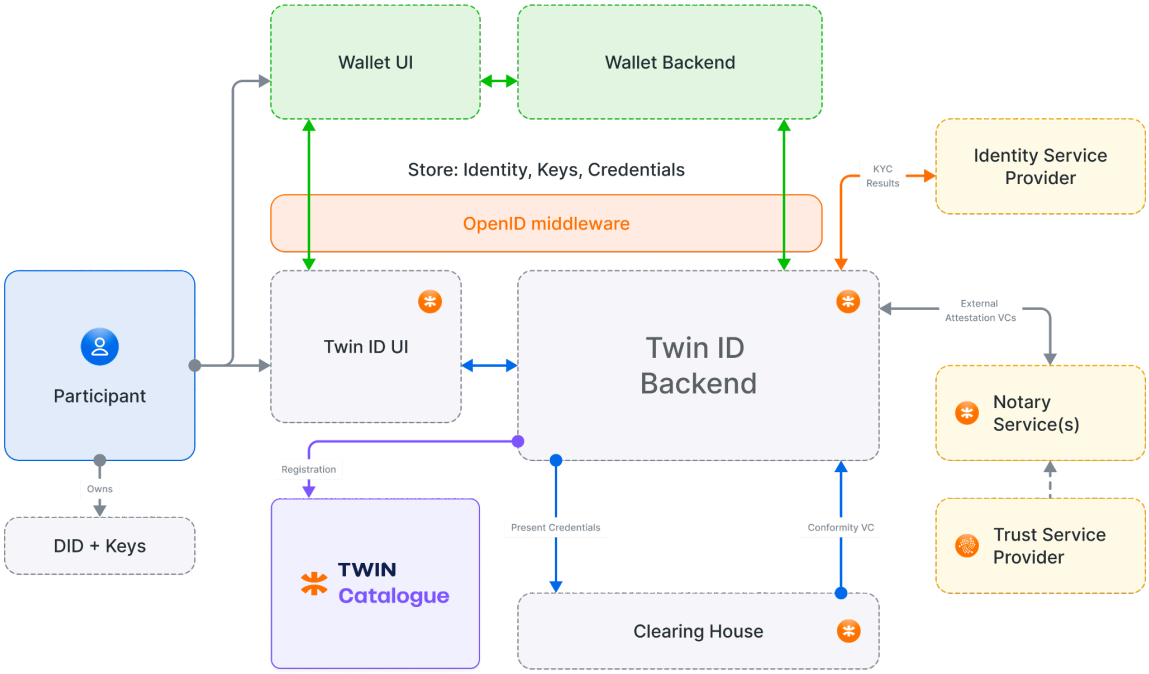


Figure 4 TWIN ID and onboarding overview

Participant Onboarding

To facilitate onboarding, TWIN aims at offering a TWIN ID Application, making it possible to obtain **Compliance Credentials** by directly using this tool to orchestrate the involved services described above. The figure above illustrates the process of Participant onboarding. Throughout the process, Participants can present evidence that will end up in a set of Verifiable Credentials signed by Trust Anchors (including Notaries), to attest to the Participant.

After storing Verifiable Credentials in a Wallet, they will be presented to the Clearing House, which will verify their compliance and issue a Compliance Credential once approved. Such a Compliance Credential is the ultimate proof that a Participant is entitled to be part of a TWIN Ecosystem.

The TWIN ID application can collaborate with **Identity Service Providers** enabling KYC Services. However, TWIN is not bound to a particular KYC process. While there can be formal KYC processes like those employed by banks or governments, there can also be lightweight ones, such as proof of ownership of a domain or email address.

From a technical perspective, the TWIN ID Application's Backend is the main orchestrator of the flow and one of the issuers of the Participant's credentials. First, it must generate a new DID (using IOTA APIs) and the corresponding key material, and then allow Participants to declare their attributes and (if evidence is needed) solicit verification to external identity providers. Additionally, TWIN Notary services can also play the role of Credential Issuers. To maximize interoperability, the interaction between TWIN ID and these external services should take place through standard **OIDC4VCI** (Open ID for Verifiable Credential Issuance) flows [OID4VCI].

Finally, once all the credentials needed are available and stored in the user's Wallet, they must be presented to the Clearing House. That process can be performed through a standard **OIDC4VP** (Open ID for Verifiable Presentations) flow [OIDC4VP], for the sake of interoperability. In this case, the TWIN ID backend will be playing the role of Verifier and mediator between the Wallet and the Clearing House. As a last step, if compliant, a new Credential will be issued and again stored in the Wallet following a standard OIDC4VCI flow.

Visibility Services

Terminology concerning this section can be found in the glossary.

Functional Overview

Visibility refers to the ability to fully understand and track the steps taken by an item (such as products, documents, and locations) along the value chain, thereby achieving transparency. This includes manufacturing, reuse, recycling, shipping, delivery, exportation, and import. Just as Participants' identities should be *discoverable, resolvable, and verifiable*, so too should item identifiers.

Visibility is a key enabler for traceability, optimization and efficiency. It enables Participants to always know where trade items are and where they come from, who has custody over them, when they will arrive and whether they are being transported properly. Visibility benefits businesses, consumers, governments and regulators in a wide variety of use cases such as compliance, provenance, authenticity/anti-counterfeiting or N-Tier traceability.

The final aim is to enable ecosystem Participants to capture and query information about their items of interest circulating within value chains. As a result, other Participants will be able to get access to that information on a need-to-know basis.

Auditable Item Services

The Auditable Item Services are composed of:

- The **Auditable Item Graph** (AIG) is a service that allows the creation of Auditable Item representations as a digital twin through its properties, relationships, and related resources (for instance, associated documents or external data sources), forming a graph.
- **Auditable Item Streams** (AIS) is a complementary service to the Auditable Item Graph, whose main functionality is to capture *Streaming Data* usually associated with an Auditable Item. Streaming data is emitted at high volume in a continuous, incremental manner with the goal of low-latency processing. Typically, organizations have thousands of data sources that simultaneously emit messages, records, or data (including location, event, and sensor data) that companies use for real-time analytics and visibility into many aspects of their business.

Figure 5 depicts the high level architecture and context within a TWIN Node of the Auditable Item Services. These services are wholly generic and application-agnostic, based on open standards (notably Linked Data Vocabularies from schema.org, GS1, and UN/CEFACT). These services primarily expose a REST API that can be consumed both by TWIN Native Solutions and by a TWIN DS Connector. Such a REST API exposes methods for creating and updating an Auditable iItem, and adding/removing alias IDs, resources, relationships, data streams, and so on. Auditable Item's property values, relationships, and resource identifiers along with their metadata are stored in a regular datastore (MySQL, DynamoDB, etc.).. Blob files are stored in a blob store. Data streaming is also facilitated by a Webocket interface.

The Auditable Item Services offer a subscription interface so that changes on Auditable Items of interest can be notified. For example, when a new document is added to an Auditable Item, other TWIN Nodes (via a TWIN DS Connector) can get notified.

Last but not least, the Auditable Item Services offer auditability to foreign clients that want to perform data verification. In other words, it can be verified that an item's data has not been tampered with, altered, or even to detect if a trade item has suffered any diversion. This is where the **DLT Connector** comes into play. Through this component, the AIG data is made verifiable through an object in the IOTA Ledger that represents a Data Integrity Proof [W3C-Data-Integrity]. That way, third parties can proceed independently to the verification of data.

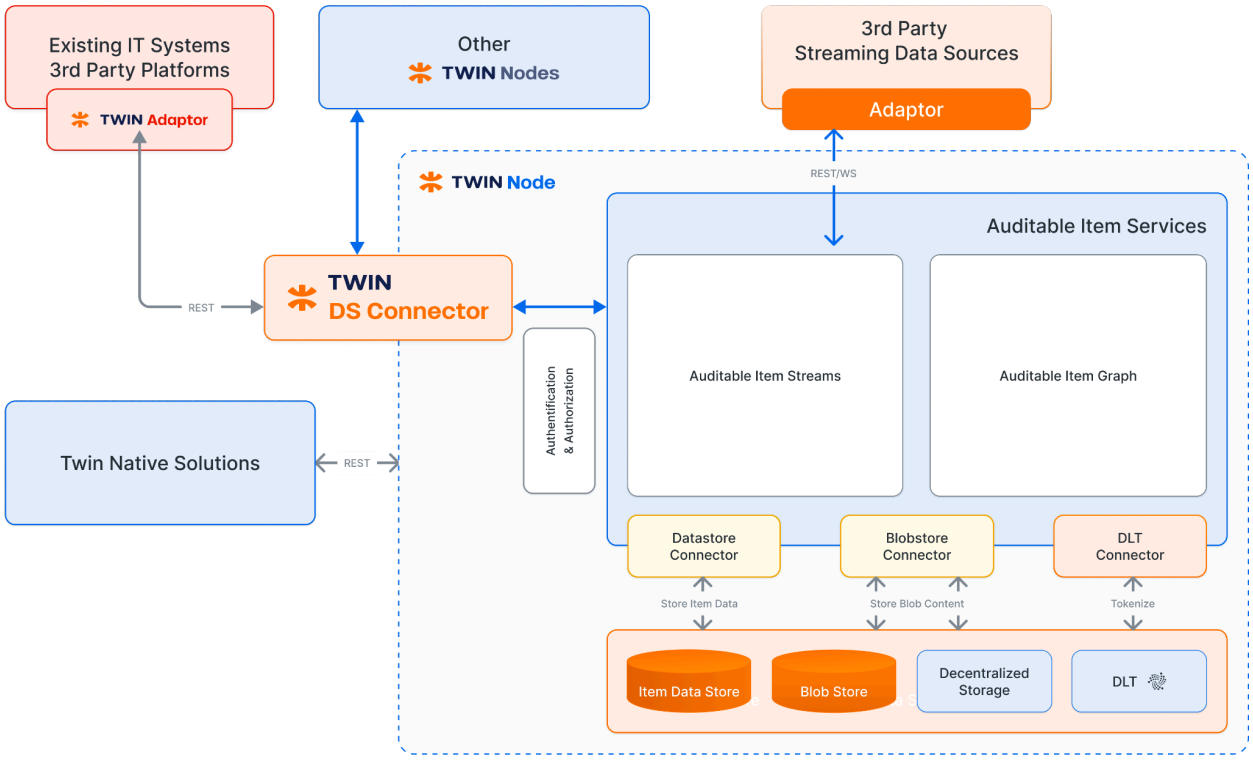


Figure 5 Auditable Item Services context diagram and functional overview

Auditable Item Graph

Figure 6 illustrates the information model behind the AIG Component. Following the W3C **Linked Data** recommendations and conventions, an item representation has: a semantic and unambiguous type(s), an identifier (which is a URI), and a set of fully qualified properties and relationships to other items (for instance, a parent-child relationship).

More specifically, the AIG information model has four fundamental elements:

- Auditable Items (Product, Consignment, Shipment, Document, etc.), which are identified by a URI, ideally a resolvable Digital Link [GS1-Digital-Link].
- Properties (for instance, weight, location, start date, etc.). A property's fully qualified name is a URI, usually imported from the UN/CEFACT, GS1 Web or schema.org vocabularies.
- Relationships (*is a, child of,* etc.), also uniquely identified by a URI.
- Associated Resources, also uniquely identified by a URI they can correspond to different assets related to an Auditable Item:
    - Blobs (for instance, an image depicting a product's photography)
    - Documents managed by the Document Management services (see below), which are also Auditable Items.
    - Data Streams, managed by the Auditable Item Streams service, with streaming data associated with the Item, for instance real time location data with a fine granularity level.
    - Extra Data Resources registered in the TWIN Catalogue that can be queried to obtain additional information, for instance time series data for product tracking offered by third party applications.

The main element (represented in Figure 6 by a rectangle) are items. These items should ideally be *serialized* elements (**instances**) in a value chain – for example, a part of an electronic device. Apart from its main Item ID (a URI), an item might be associated with other IDs named **Alias IDs**. This reflects the fact that, in a supply chain, different actors usually refer to the same trade item through different identifiers.

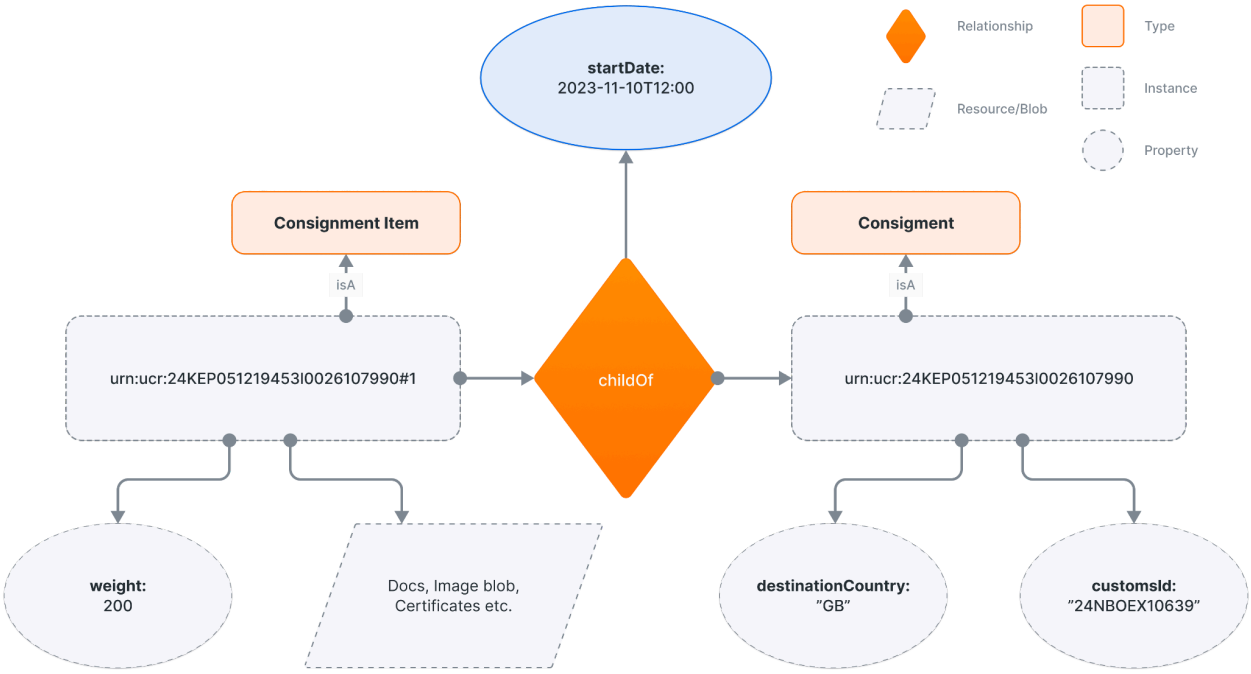
Every item has one or more **classes** (represented in Figure 6 by a rounded rectangle) (*isA* relationship), with "**Item**" being the default. Items can have **properties** (represented by an oval) – for example, the weight of the part, or the location of the part in a warehouse – and associated documents stored as blobs (represented in Figure 6 as a quadrilateral), generalized as the item's **resources**.

Items can be related to other items, and these **relationships** are depicted by a diamond in Figure 6. For example, in international trade, a *Consignment*[27] – related to a business agreement between a seller and a buyer – may be split into multiple *Consignment Items*[28] for delivery or customs purposes. From an information management perspective, this translates as a single Auditable Item of type "Consignment" with a "parentOf" relationship, with multiple Auditable Items of type "Consignment Item". Conversely, each *Consignment Item* has a "child Of" relationship with its parent *Consignment*.

Relationships can also have properties. A typical example is the date from which the "child Of" relationship applies, corresponding to the date the consignment was prepared.

Items can also represent trade documents that may have relationships among them and among the trade items they reference. For example, a *Customs Declaration* can point to a *Commercial Invoice* and a *Bill of Lading* might reference items formerly referenced by one or more *Custom Declarations*.

Another important aspect (auditability), is the ability to store different versions (change sets) of an Item – its Object History – as it undergoes change, such as additions or removals of properties, relationships, etc.). This allows for tracing the object's state over time.



[27] https://vocabulary.uncefact.org/Consignment

[28] https://vocabulary.uncefact.org/ConsignmentItem

Figure 6 *Information model of the Auditable Item Graph*

Last but not least, the Auditable Item Graph supports the concept of Item Views. An Item View allows the definition of projections of Auditable Items to hide certain properties, relationships or resources. For instance, in the context of data exchange policies, an Item View allows sensitive item properties that should not be accessed by certain Participants to be filtered.

Event Management

The **Event Management** Service enables the storage, retrieval, querying, subscription, and timestamping of **key value chain events – TWIN Events –** related to Auditable Items. These events encompass traceability and business events and can be applied to a wide variety of value chain ecosystems. In international trade, multiple stakeholders often need advance information about consignments, including their nature, location, transport route, and conditions. These data points can be transmitted as signals, represented as TWIN Events, as part of the data exchange between different TWIN Nodes. Key TWIN Events may include health checks, departure or arrival times corresponding to locations, entry and exit records for ports, document availability, and other critical logistics details.

Another case is supply chain traceability from manufacturing to distribution and retail being those steps captured and timestamped through supply chain events that can be disclosed on a need basis.

Figure 7 illustrates the context of the Event Management Service:

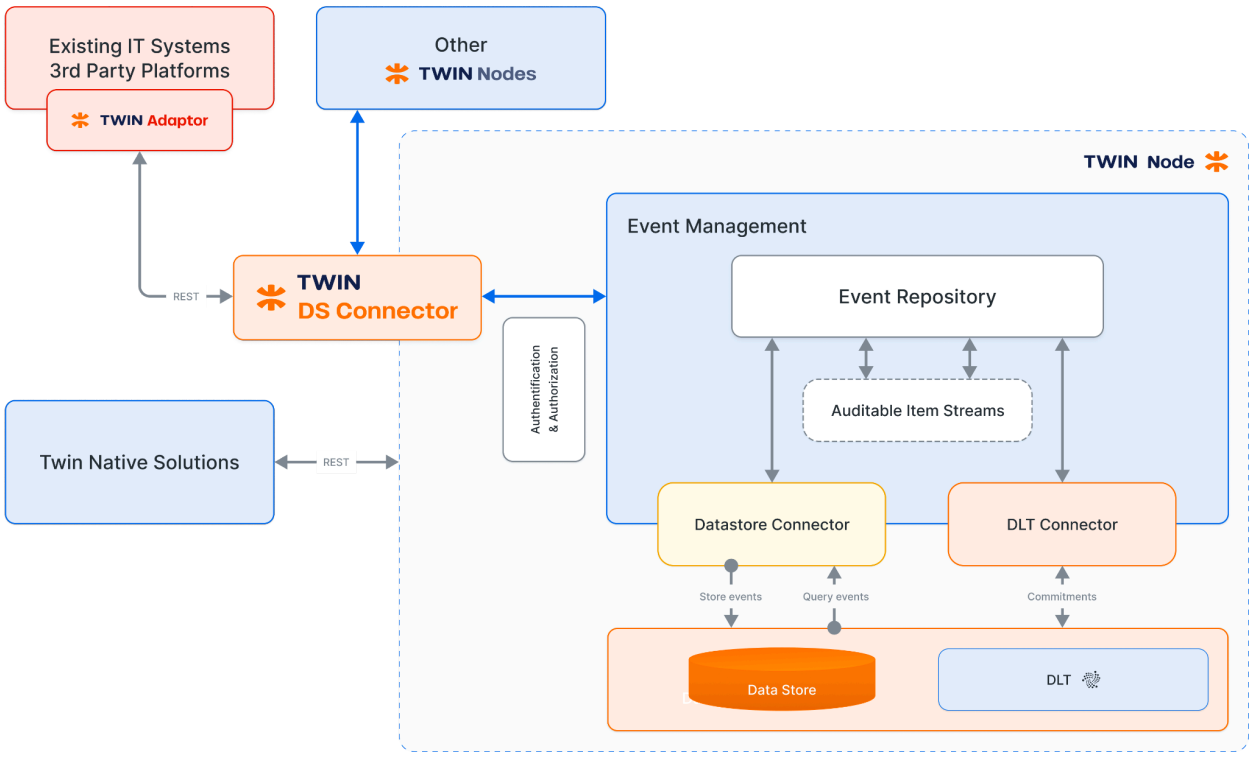


Figure 7 *Event Management Service context diagram and functional overview*

There are two main components involved:

- The **Event Repository** is in charge of exposing the fundamental REST API endpoints that allow TWIN Events to be captured (including syntax validation and indexation) for later retrieval. This component is also responsible for supporting standard API definitions, including the GS1 EPCIS 2.0 REST APIs[29].
- The *Auditable Item Streams Service* offers the backend capability of grouping events concerning the same item under an Auditable Item Stream, facilitating the discovery of Auditable Item's Events, timestamping and auditability (through DLT), streaming and publish/subscribe features.

As with the rest of Visibility Services, the Event Management Service is datastore agnostic. TWIN Events arrive through REST requests generated by authorized TWIN Native Solutions or through the TWIN DS Connector. As TWIN Events are an essential data exchange item, many of them will come from existing IT systems or other TWIN Nodes.

[29] https://ref.gs1.org/standards/epcis/openapi.json

As a baseline, the Event Management Service supports the **GS1 EPCIS Linked Data Model**[30] for TWIN Event representation (JSON-LD). On top of that, two different flavours of TWIN Event representation are supported:

- Full **GS1 EPCIS 2.0** representation for more complicated visibility- and traceability-oriented use cases where business transactions take a prominent role.
- Minimal Event representation, which is a subset of EPCIS 2.0 plus some additional extensions, and which comprises a minimalistic representation more suitable for transport and international trade use cases.

  Concerning APIs supported, TWIN aims at being fully compliant with EPCIS 2.0 REST APIs as specified by GS1, while supporting both Event representations described above. Those APIs allow capturing events, querying events and subscribing to events.

Several characteristics of how TWIN Events are managed are aimed at increasing trust in the ecosystem:

- TWIN Events are **immutable** by definition. Once an Event has been disclosed to other Participants it cannot be changed. In fact, Events are always **appended** and never deleted. If an Event proves to be erroneous, a further Event with an error declaration must be appended.
- Critical business Events can be linked to **proofs** that timestamp or attest for the legitimacy of an Event i.e. that it has not been faked and its real occurrence time. TWIN advocates two types of proofs for Events:
  - DLT Commitments attest the existence of one or more Events at a particular time. That feature is provided by the Auditable Item Streams Service.
  - Physical Device Events can attest the physical presence of an item at a particular location (see Edge Connectors)

The following are the minimal data points captured by an Event in TWIN (all have a standard representation in the GS1 EPCIS Linked Data Model):

- Event identifier, a URI that is constructed, for immutability, via a hash of the canonicalized representation of the event's data points.
- Event type(s), represented by a URI, which provides a semantic, unambiguous categorization of the event.
- Targeted item or items (**what**), identified by a URI.

[30] https://ref.gs1.org/epcis/

- Timestamp of when the event physically occurred (**when**).
- The timestamp when the event was recorded (for example, recorded digitally after its physical occurrence)
- A DID Identity of the Participant registering the event (**who**).

Figure 8 shows a TWIN Event, that corresponds to an inspection performed over a target trade item, performed at a particular business location (such as a warehouse or port) and originated by a Participant identified by a DID (for example, the agent performing the inspection).

	Event ID	ni:///sha-256;f12640477da404f845f5e4a2d4071fdecda7cb1af6fc0fd89462654cf2b94f43?ver=CBV2.0
What	Event Type	Visibility
	Target	https://id.gs1.org/01/09521987654327/21/202301
When	Observed at	2024-09-12T15:00:03.321Z
	Recorded at	2024-09-12T 15:05:03.321Z
When	Location	2024-09-12T 15:05:03.321Z
Who	Actor	did:iota:0xb62afcd0150d048ea0679af61d28d0eb1ad1b969f411b03997194df232b27383
Why	Business Step	Inspecting

Figure 8 *Conceptual overview of a TWIN Event*

Additional data points are also possible as per the GS1 EPCIS 2.0 standard and further extensions, such as:

- Physical location (represented by geocoordinates or by an encoded location) of the event (**where**)
- Read point (usually represented by an encoded location) that gives precise details of the location of the event (for example, a specific door in a warehouse).

- Environmental conditions of the capturing place, such as temperature or humidity
- Identity and/or other details of the device that served to capture the event (**how**). A URI.
- Business process or business transaction involved (**why**).
- Details of the reported business process such as completion status, start date and end date.
- Participants concerned: generator (rapporteur) of the event, actor or actors involved
- Other items involved, such as child items or attached sensors.
- Objects related to the event, such as trade documents involved.
- Target item specific properties at the time of capture, for instance, temperature, weight, etc.
- Other event-specific

Document Management Services

Definitions referenced in this section can be found in the glossary.

Functional Overview

Trade documents are an integral data exchange asset in trade and value chain ecosystems. In fact, different interactions critical among businesses, government and consumers involve **key trade documents**:

- *Business to government (B2G) and government to government* (G2G): Clearance of goods at borders requires the availability and authenticity of essential documents (such as certificate of origin, health certificate, and export or import customs declaration).
- *Business to business (B2B)*: key documents are bills of lading or commercial invoices that can be the subject of upper-level ecosystems such as *trade finance*.
- *B2G, B2B and Business to Consumer (B2C):* Value chain ecosystems and Digital Product Passports rely on documents like product certifications [UN/CEFACT-Prod-Certificate] issued by auditors (for example, eco-labels), test reports issued by manufacturers, product specifications and manuals, bills of materials to facilitate recycling operations, verifiable evidence of compliance with ESG Regulations, and so on.

Note the distinction between two different classes of trade documents:

- *Pure, native eDocuments* (ePhyto, eInvoice, etc.) are represented using a semi-structured, machine-readable format (XML, JSON, CSV, etc.). If they include a digital signature, their authenticity and integrity can be ensured through cryptographical methods. In fact, recent legislation, for instance the *UK Electronic Trade Documents Act*[31], in alignment with the MLETR, provides for certain electronic trade documents, including electronic bills of lading, to be accorded the same legal status as their paper equivalents, if they meet certain relevant criteria.

- *Scanned, generated, plain documents*, a digital version of a paper document resulting from a scanning or rendering process, usually saved in PDF format. Even though they can be read by AI-based automation tools, they are not ready for processing using simple techniques and are error and fraud prone. Normally, they do not include any signature, thus their verification requires human intervention.

From the point of view of trade document management, there are two key roles:

- **Issuer** (*issuerParty*[32] as per UN/CEFACT), an accredited entity (government agencies, conformity assessment bodies, regulators, auditors, accredited organizations, etc.) who supplies a trade document to an interested party. For instance a Chamber of Commerce issues Certificates of Origin (CoO). Traditional issuance methods rely on hand-made signatures and official stamps for authenticity.

- **Holder** (*senderTradeParty*[33] as per UN/CEFACT), a Participant who sends and presents a trade document issued by an issuer. For instance the exporter in the case of a CoO. There are trade documents where the issuer and holder role can be played by the same entity, for instance an exporter that presents a commercial invoice in order to obtain export permits.

Additionally there is a third role, the **Verifier** (*recipientTradeParty*[34] as per UN/CEFACT). Verifier is an entity that receives and verifies a trade document. The verification process implies checking document authenticity, consistency and validity. For instance, a customs system that receives a CoO needs to verify it in order to apply reduced tariffs.

Description and Functionalities

TWIN **Document Management** services allow the storage and retrieval, on a need basis, of **multi-versioned**, **multi-format** *electronic* trade documents ensuring *data availability, data*

[31] https://www.legislation.gov.uk/ukpga/2023/38/contents

[32] https://vocabulary.uncefact.org/issuerParty

[33] https://vocabulary.uncefact.org/senderTradeParty

[34] https://vocabulary.uncefact.org/recipientTradeParty

sovereignty, *data auditability and tamper-proofness*. The Document Management services are ready to deal with both PDF-like, scanned, plain documents and native eDocuments.

Even though the backoffice processes that concern the issuance of documents are out of scope of TWIN, a TWIN Node helps to transition from scanned, generated documents to native eDocuments. In fact through a TWIN Node, a Participant, playing the role of document issuer, can announce (through an Event emitted by the corresponding IT system) the issuance of a key trade document (materialized for instance as a PDF) concerning a Trade Item. Once known by a TWIN Node, this new document can be bound to an Auditable Item, and, later, to facilitate verification by Participants fetching the document, a **data integrity proof** can be created on behalf of the document issuer. As a result, plain documents are turned into eDocuments enabling the automation of document verification through digital means.

Figure 9 shows a context diagram of the Document Management services. At the top there are different functional blocks related to the main functionalities offered (described above), all of them exposed as REST endpoints. At the middle layer is the Auditable Item Graph service as TWIN manages trade documents as Auditable Items, enabling seamless traceability and auditability. At the lower level the different infrastructure services (including DLT) that constitute the fundamental substrate.

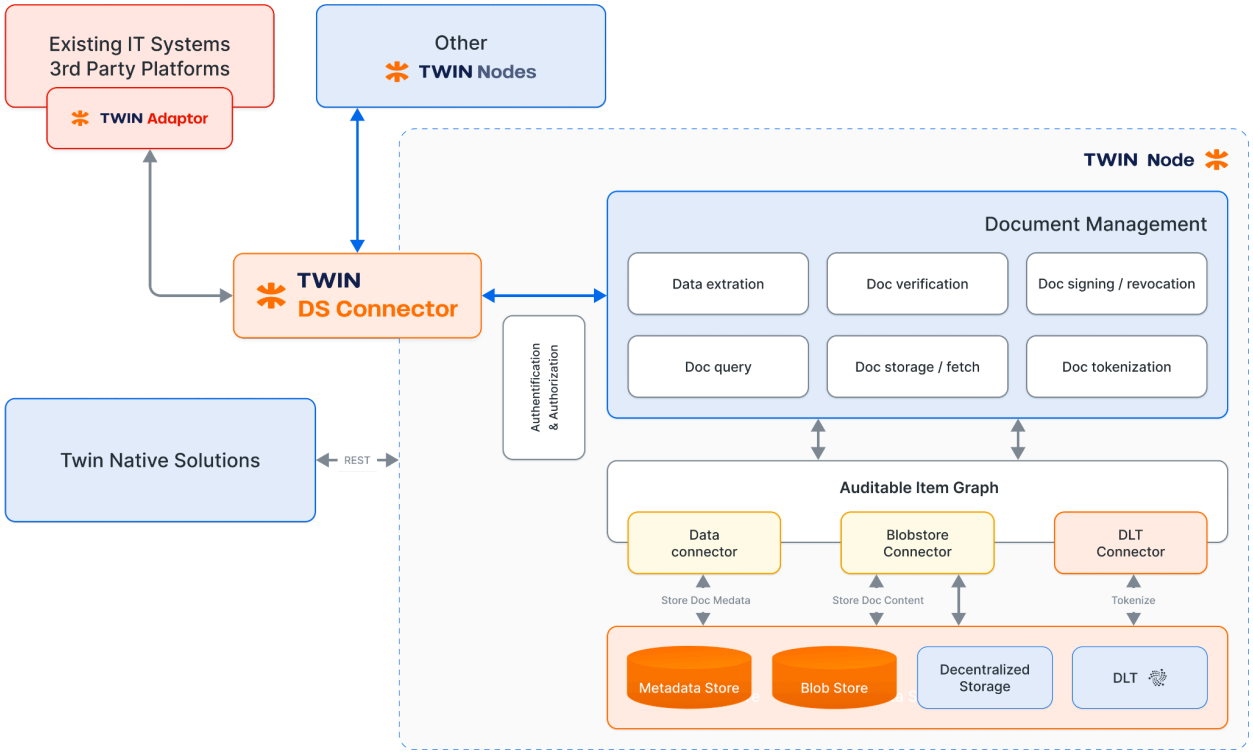


Figure 9 *Document Management services context diagram and functional overview*

There are two options for **storing a document's content**:

- The document's content is stored *at the source* (usually an issuer's or holder's external IT system), while the Document Management services at a TWIN Node only keep metadata properties (see below) and a digital fingerprint that prevents tampering.

  Typically, an external IT system storing document content will be wrapped as a **Data Resource**, and published to the *TWIN Catalog*, enabling other Participants to fetch (and verify) documents on a need-to-know basis (provided data exchange policies are matched).

- The document's content and metadata are stored *at the TWIN Node*, typically when the Participant lacks sufficient storage – such as a small trader. In this case, the document can be stored in a blob store managed by the Node or in a decentralized storage system (typically IPFS). If stored in a decentralized system, it may be encrypted to ensure that only authorized Participants can access it, following predefined sharing policies that govern encryption key distribution.

A TWIN Node can store various metadata properties related to eDocuments (**document metadata properties**) through an Auditable Item bound to the document. This flexible approach follows Linked Data models, enabling the use of vocabularies such as UN/CEFACT or schema.org. Figure 10 provides an illustrative example.

Name	Tag	Description
Details	Document ID	urn:docId:337:b0ff65af9768c9a24b9579c953c8a856b5f3e197b265af3e662f0c572e23f923
	Document Type	unece:DocumentCodeList#851
	Revision Number	2
	Item Referred	https://id.gs1.org/01/09521987654327/21/202301
Content	Content size	5671
	File Format	application/xml
	Content Locator	urn:fs-blob:7df6bdb4cb31ad118c9dfb3053f8cd671330e9538bfe03027c1cd5ec7c268d9d
Timestamps	Issued at	2024-09-12T 15:05:03.321Z

Name	Tag	Description
	Created at	2024-09-12T 15:05:03.321Z
Party	Issuer party	did:iota:0xb62afcd0150d048ea0679af61d28d0eb1ad1b969f411b03997194df232b27383
	Sender party	did:iota:0xd7258832d2c578426f2d33ce320cf485b3707ae99b90fdcf25ca5b60b30381c3
Proof	Fingerprint	c6b6f54aecdec6f37de08ae4a2375eceb1d69115c28c2738c915587362714d8c

Figure 10 *Document metadata example*

Although TWIN is not limited to a specific set of metadata properties, the following are the most essential trade document metadata properties:

- Document identifier (URI). This is equal to the Auditable Item ID that represents the document on a TWIN Node.
- Document type code (as per the UN/CEFACT document code list[35]).
- Content MIME type (XML, PDF, JSON, etc.).
- Content length (byte number).
- Content locator, a URI that points to a blob that contains the document's content.
- Issuer Identity (DID).
- Revision number (multiple document revisions can be stored and fetched)
- Digital Fingerprint (a hash to prevent tampering when the document remains at the source)
- Timestamps:
    - Creation (date and time when the document was registered on a TWIN Node).
    - Revision (date and time when a document revision was registered on a TWIN Node).

[35] https://vocabulary.uncefact.org/DocumentCodeList

    - Issuance (date and time when the document was issued).

Other metadata properties:

- **The (Auditable) Trade Item(s)** referred **to** by this trade document (URI). However, there can be trade documents that, initially, might not refer to a specific Trade Item. For instance, a veterinary inspection result that is performed over poultry. Later, it might be needed to associate the original veterinary inspection with a food shipment that contains such poultry's meat.
- **Document description**: a textual description of the document.
- **Revised Document:** the **URI** of the previous document version that this document updates.
- **Holder Identity (DID).**
- **Data integrity proof** (can be pre-created or created on demand when a document is fetched).
- **Validity period.**
- **Document status**, including revocation status (a link to a location where a verifier can check to see if a document has been revoked).
- Other properties (see UN/CEFACT *Document*[36] class and schema.org *DigitalDocument*[37] class).

A TWIN Node is ready to interface with deployed **Data Extraction applications** (actually TWIN App instances) that apply to two different scenarios:

- **eDocuments:** TWIN Document Management services are agnostic to specific document standards (ePhyto, eInvoice, etc.). As a result, a data extraction TWIN A may be required to automatically process the information contained within an eDocument.
- **Plain documents:** In this case, data extraction can be performed on PDF-like documents using OCR or other AI-driven automations. The goal is to obtain a canonical, machine-readable version of the document, which can be converted into an eDocument if required, using a **data transformation TWIN App**.

In both scenarios, the final purpose of data extraction is:

[36] https://vocabulary.uncefact.org/Document

[37] https://schema.org/DigitalDocument

- To capture relevant document metadata properties (such as validity period, issuance timestamp, or signatures) so that they can be properly processed by business processes.
- To capture additional data about associated trade item(s) and its journey while also checking for consistency in order to detect fraud or suspicious activities.

Document fetching is a simple query operation, subject to data exchange policies and exposed by a TWIN Node via a REST API. To retrieve a document, it is necessary to know either its identifier or type code[38]. Alternatively, the document's identifier can be discovered through its referred Auditable Item(s). The result of a document fetching operation includes the document's metadata along with the latest revision of its content. The content can either be transmitted directly to the client or provided as a reference to its location in decentralized storage. There can be multiple copies of a document if the data exchange policies allow different nodes to retain documents. As it happens with other Auditable Items, Documents can also be constrained by "Item Views" in order not to disclose sensitive data points.

Document/Revision addition is a simple operation exposed through a REST API. The client needs to provide the document's:

- Metadata
- Fingerprint or signature.
- Content in case the document needs to be stored in a TWIN Node.
  A TWIN Node is responsible for ensuring consistency within metadata properties across revisions. Other consistency checks can be performed by upstream, application-specific services.

Document signing can be subject to the following scenarios:

- **Pre-Signed Document (Verified Signature)**
  If a document (whether a plain PDF-like file or an eDocument) is already signed by the issuer, whose signature can be verified by a TWIN Node or a TWIN App), no further action is required. This is the simplest scenario, as the TWIN Node only verifies the existing signature.
- **Unsigned or Unverified Signature**
  If a document lacks a signature or has one that cannot be verified by a TWIN Node, the Node can sign it on behalf of the Participant, who can either be the issuer (higher trust level) or the holder (lower trust level). Since the TWIN Node does not directly manage signing keys, it must interact with a Wallet that holds the relevant keys to complete the signing process..

[38] https://vocabulary.uncefact.org/documentTypeCode

A document's signature can be stored as part of its metadata properties, following the W3C Data Integrity Proof Recommendation.[39]Alternatively, the signature can be calculated on demand when another Participant requests the document.

Document verification occurs when TWIN Nodes or external systems, via TWIN Adaptors, exchange documents. This process ensures that the disclosed fingerprint matches the original or that the original signature can be verified.

Document timestamping and auditing follow the same mechanisms used for the Auditable Item Graph, as documents within a TWIN Node are represented by an Auditable Item.

Document tokenization involves binding a trade document to a Non-Fungible Token (NFT) on-chain via a DLT Connector. While the document's content and metadata remain on a TWIN Node, its immutable entry on a distributed ledger enables electronic record transfers, following the recommendations of the MLETR legislation. This capability is envisaged for eBills of Lading, eInvoices, promissory notes, etc, bringing life to Trade Finance ecosystems. This feature is being developed and tested at time of writing, and we are planning to report on our results and vision in future whitepapers.

Readers may wonder about the role and relevance of W3C Verifiable Credentials (VCs) standards in trade documents [UN/CEFACT-VC-Trade]. Simply put, VCs are also eDocuments that follow a particular W3C-defined data model with clear semantics. In addition, like other eDocuments or TWIN-signed plain documents, they can be cryptographically verified for authenticity and integrity using data integrity proofs. Bottom line, when a Participant adds a new trade document represented as a VC, a TWIN Node can act as a VC verifier, extracting data from such a VC,. Alternatively, a TWIN Node can also be a VC issuer, on behalf of a Participant, when transforming a trade document into a VC as required by other services..

Data Exchange Services

Definitions useful to understand this section can be found in the glossary section for Data Spaces.

Functional Overview

Data Exchange services are enablers for data exchange among Participants and imply:

- **Publication to the TWIN Catalog** of Service Offering(s), incarnated by the TWIN Data Space Connectors, and Data Resources, incarnated by TWIN Adaptors, so that discovery is enabled.

[39] https://www.w3.org/TR/vc-data-integrity/

- **Vocabularies**: TWIN uses the Gaia-X Vocabulary[40] when describing Services and Data Resources. To describe policies, TWIN uses the W3C ODRL Vocabulary[41], expressed as Linked Data.
- **Policy management**, so that Participants can declare unambiguously which data is shared to whom (*permissions*) and under which terms and conditions (*data usage policies*). Policies are linked from Service Offering or Data Resource descriptions.
- **Authentication and authorization services** so that Participants can authenticate against a TWIN Node when requesting data (or documents) or subscribing to data. Afterwards, authorization can be checked through the Policies already declared and found on the Catalog.
- **Data Exchange protocol** implemented by a TWIN DS Connector. This protocol, in alignment with the IDSA Data Space Protocol[42], defines a control plane and a data plane.

  TWIN Adaptor protocol, a subset of the Data Exchange protocol, typically exposed by external IT systems through Data Resources that are used to retrieve data (particularly trade documents) kept at the source.
- **Transaction logging** (optional) to provide an auditable framework for data exchange transaction observability so that there is a digital notary that has the last word in case of dispute. As a TWIN Node includes a DLT Node (i.e. anIOTA Node), this is a differential functionality in our roadmap.

To support the understanding of the concepts defined above, Figure 11shows a functional overview of the architecture that describes in detail how Data Exchange Services play together. It can be observed that data exchange happens through the Data Plane of the Data Exchange Protocol implemented by TWIN DS Connectors. As the Data Space Connectors are just the means to obtain data, they need to delegate on the Visibility and Document Management services to persist it. On the other hand, TWIN DS Connector Apps implement custom functionality that might depend on particularities of each ecosystem. As anticipated, a data exchange can only happen on behalf of compliant Participants registered on the TWIN Catalog and if the corresponding policies are met.

[40] https://w3id.org/gaia-x/development

[41] https://www.w3.org/TR/odrl-vocab/

[42] https://docs.internationaldataspaces.org/ids-knowledgebase/dataspace-protocol

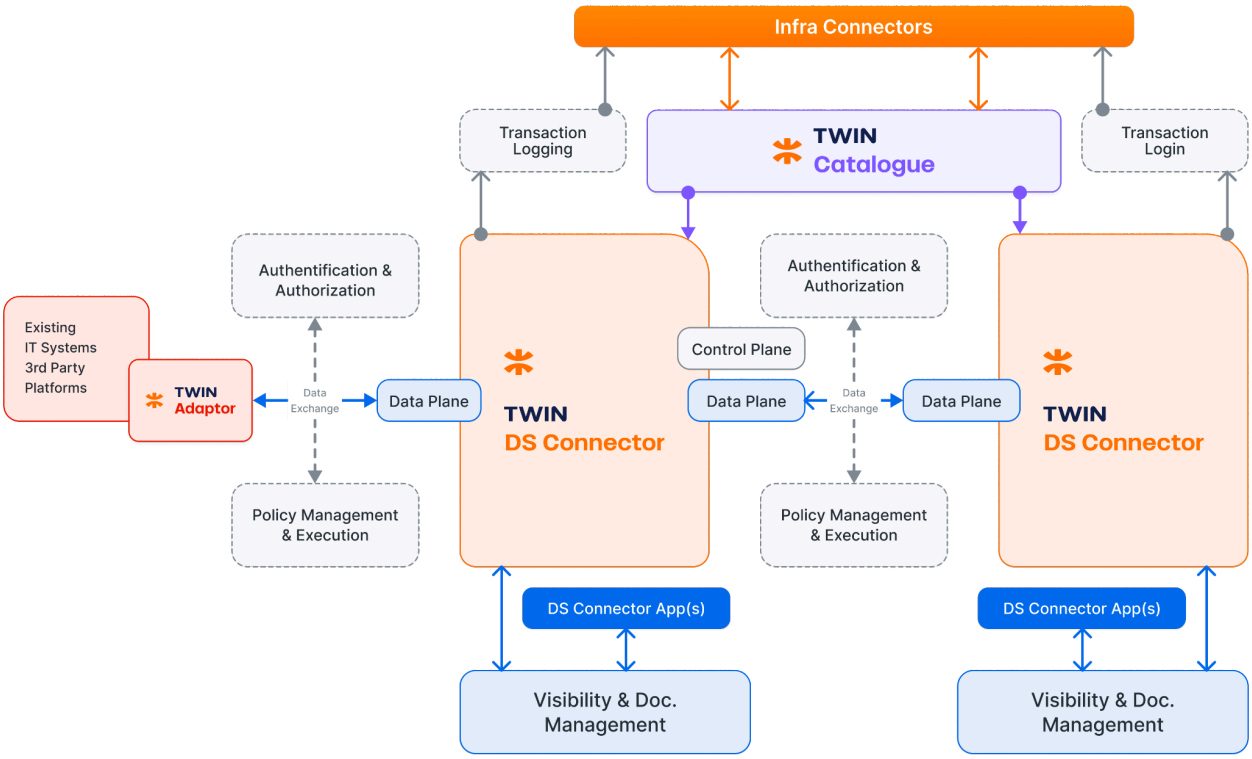


Figure 11 *Data Exchange Services architecture overview*

Service Publication and Discovery

The **TWIN Catalog** is a decentralized service intended for the publication by compliant Participants (Data Providers) of metadata about the services and resources they expose (*Service Offering* descriptions or *Data Resource* descriptions, expressed as Verifiable Credentials[43]). Later, other Participants (Data Consumers) can query the TWIN Catalog to discover services or resources of their interest and perform data exchange.

Each TWIN Node can declare multiple Service Offerings or Data Resources, particularly the ones incarnated by the TWIN DS Connector service instance. Additionally, other services – such as the Auditable Item Graph (AIG) and Document Management – can be aggregated to define further offerings.

A *Service-Offering Credential* contains different metadata (expressed using the Gaia-X Vocabulary) that describes a service and its policies. The same applies for Data Resources.

43 https://docs.gaia-x.eu/technical-committee/identity-credential-access-management/24.07/credential_format/

An example of the metadata needed to describe a Service Offering[44] is provided below:

Name	Tag	Description
Details	Service Offering ID	https://my-offerings.example.org/service1
	Provision Type	public
	Description	TWIN Node Data Space Connector
	Name	Data Space Connector
Privision	Provided by	did:iota:0xb62afcd0150d048ea0679af61d28d0eb1ad1b969f411b03997194df232b27383
	Aggregation of resources	http://twin-nodes.example.org/node1/aig-query http://twin-nodes.example.org/node1/document-query http://twin-nodes.example.org/node1/event-subscription
	Terms and conditions	url: https://tcs.example.org/1234 hash: 0x56A123
	Data account export	format type: application/jsonrequest type: API
Timestamps	Endpoint	Url: https://my-twin-node.example.org/dataspace-connector formal description: https://openapi.example.org/twin-data-space-connector
Party	Service Policy	See service policy description

Figure 13 Data exchange service metadata expressed using the Gaia-X Vocabulary

Like Participants, *Service Offerings* (or *Data Resources*) must undergo **compliance** checks by a TWIN Clearing House. If they meet the ecosystem rules, a *Service Offering Compliance*

[44] https://docs.gaia-x.eu/ontology/development/classes/ServiceOffering/

Credential[45] is issued. This Credential must then be presented to the TWIN Catalog for final service onboarding.

Policy Management

Policies attached to Service Offerings or Data Resource descriptions – represented using W3C ODRL – allow Providers to set rules regarding:

- The informational resources (documents, Auditable Items, Events, etc.) they want to share. These are usually expressed as conditions of the resource's properties, such as "all items of type 'Consignment' whose destination country is Great Britain".
- The Consumers (Participants, Services) that can get access to the shared resources. These can be enumerated by ID (DID, URI, etc.) or through conditions that the Consumer's Attributes must meet. For instance, "all Participants whose headquarters are in Kenya and whose role corresponds to a 'government border agency'".
- Certain environment conditions (optional) concerning the operational, technical, or situational environment in which the information access occurs. For example, the time of day in which the data exchange can take place.
- The terms and conditions (optional), for instance if the data or documents shared can be retained or archived by a Consumer.

These rules are associated with an action (*read, modify, annotate*, etc. as per ODRL.). In data exchange processes the usual action will be "read". An example of a Policy can be found below (Figure 14).

45 https://docs.gaia-x.eu/technical-committee/identity-credential-access-management/24.07/credential_format/#gaia-x-compliance-inputoutput

Name	Tag	Description
Details	Policy ID	https://my-policies.example.org/policy1
	Provision Type	Agreement
	Profile	https://twindev..org/odrl:profile:01
	Description	Agree to share consignment details whose destination country is UK with UK Border Force Participant
Who	Assigner	did:iota:ebsi:0xb62afcd0150d048ea0679af61d28d0eb1ad1b969f411b03997194df232b27383
	Assignee	did:iota:ebsi:0x3edd589d510d58c211237c79755314d81c228b8bd95559f9ad35911736b3a4aa
Timestamps	Target	type: Consignment
	Action	read
Contidionts	Destination Country	unece:CountryId#GB

Figure 14 Policy structure example

Regarding the services in charge of managing and enforcing Policies, TWIN adheres to Gaia-X, NIST and OASIS recommendations, dividing it into the following services:

- The **Policy Execution Point** (**PEP)** is responsible for delivering the final *permit/deny* outcome to a client service. The client service submits a request context to the PEP, describing the nature of the request (the target resource, the identity of the requester, etc.). The PEP then forwards this request context to the Policy Decision Point (PDP) for evaluation.
- The **Policy Decision Point** (**PDP**) determines whether a requesting party should be granted access to a protected resource, such as an Auditable Item or trade document. The decision is performed by examining the access request, the attributes of the requesting identity offered by a Policy Information Point (PIP) – and comparing them

against the corresponding resource's policies, which are obtained through the Policy Access Point (PAP).

- **The Policy Access Point** (**PAP**) is a service that enables Participants to manage policies, including creation, update, deletion, storage and publication. This service is offered by a TWIN Node off-the-shelf.

  The **Policy Information Point (PIP)** supplies Identity Attributes necessary for the PDP to make access control decisions. This role can be fulfilled by various entities, including the **TWIN Catalogue**. Additional attributes may be disclosed through the **SD-JWT** [IETF-SD-JWT-2025] used for authentication.

A functional view of the policy management architecture is depicted below (Figure 15):

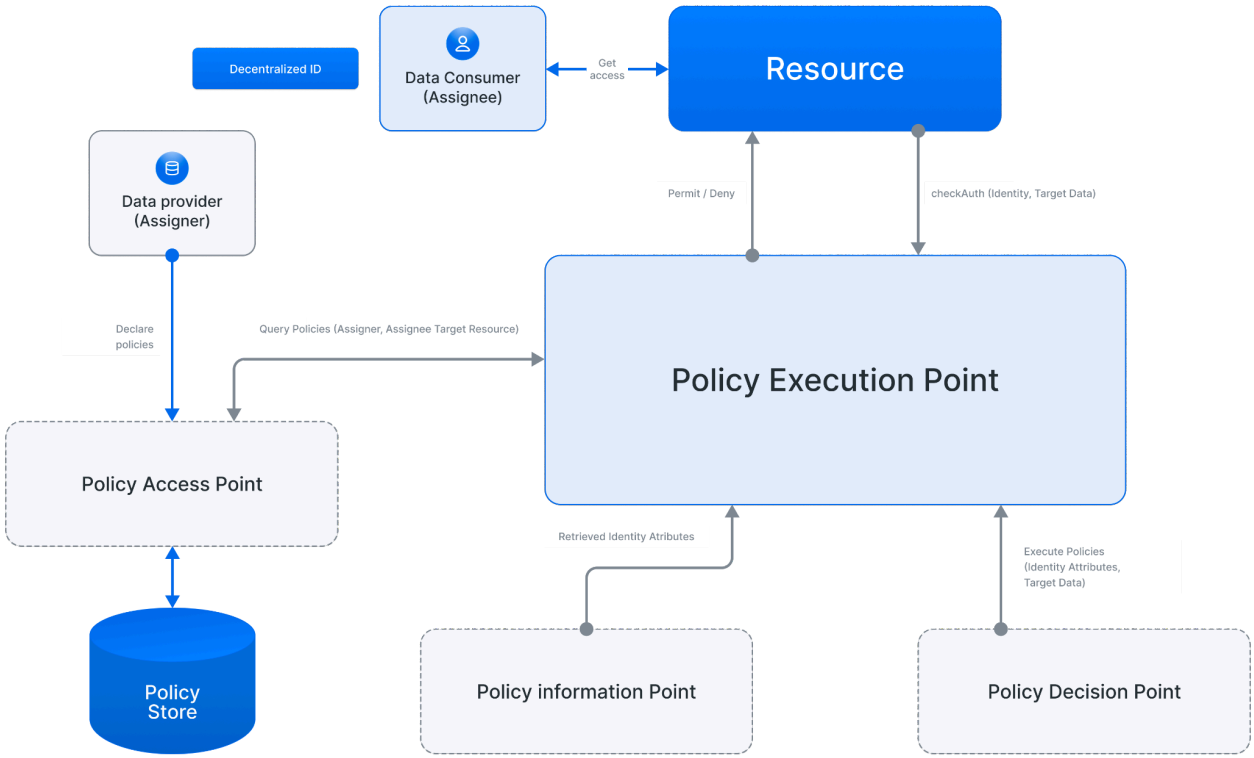


Figure 15 Functional view of the policy management architecture in TWIN

Authentication and Authorization

To perform data exchange processes, TWIN DS Connectors must first determine who wants to perform a certain action (for instance, who wants to fetch a trade document) i.e. *authentication*. Authentication is achieved using a (SD-)JWT token, which the requesting party must present to

prove, at a minimum, control over a specific identity (DID). Once the Identity is verified through a verifiable registry (such as the DLT, the Policy Decision process can take place, permitting or denying the request (*authorization*).

TWIN Data Space Connector

As described throughout this document, the fundamental TWIN services described – **Auditable Item Graph, Event Management, and Document Management** – expose APIs that facilitate the full lifecycle management of various objects, such as trade items, TWIN Events, data streams, and trade documents).

In addition, a TWIN Node exposes a **Data Space Connector**, a specialized service designed for data exchange within trade ecosystems. The Data Space Connector is responsible for two key functions:

- Receiving "events of interest" (acting as a sink). These are activity reports generated by other Data Space Connectors or TWIN Adaptors, which act as a source. Examples of such events include the creation of a consignment, the addition of a trade document, or the finalization of an inspection.

  The W3C Activity Streams [W3C-Activity-Streams] standard is the fundamental data model and representation format for expressing "activity or events of interest". An "event of interest" is modelled as an **Activity**[46] object represented using JSON-LD. Each Activity object includes information on the generator and actor of the Activity (typically a Participant), the type of action[47] (e.g. "Add", "Request", "Create") and the associated **object** and **target** (e.g. a *Document*[48] linked to a *Consignment*). An object could also be a TWIN Event.

- Processing received Activity objects and collaborating with the fundamental services of a TWIN Node to react appropriately. These reactions may include:

  - Creating new objects in the target TWIN Node, such as Auditable Items or TWIN Events.
  - Updating existing Auditable Items in the target TWIN Node.
  - Retrieving object's data from the Data Space Connector of the Activity's actor, if necessary and permitted by policy (e.g., for verification purposes).

[46] https://www.w3.org/TR/activitystreams-vocabulary/#dfn-activity

[47] https://www.w3.org/TR/activitystreams-vocabulary/#activity-types

[48] https://vocabulary.uncefact.org/Document

- Delivering derived “events of interest” (modelled as *Activity* objects) to other TWIN Nodes via their corresponding target Data Space Connectors, effectively transforming the original sink Data Space Connector into a source Data Space Connector.
- Sending other notifications to external IT systems, TWIN Applications, or other relevant entities.

In technical terms a TWIN DS Connector offers:

A. REST endpoint for receiving Activity objects. This is part of the **Data plane**.

B. One or more REST endpoints that expose an interface for querying objects managed by a TWIN Node, such as trade items, documents, or TWIN Events. This is part of the **Data plane** and offers a pull transfer[49]. The data retrieved is represented using JSON-LD or derivatives such as NGSI-LD [ETSI-NGSI-LD] that allow a convenient representation of property graphs.

C. REST endpoint that allows different kinds of parties (such as Participants, other TWIN Nodes, or external applications) to subscribe to “events of interest”.

   Matching ”events of interest” will be represented as Activity objects and delivered via a Web hook (an HTTP POST request to a recipient). This is part of the **Control plane**. Typically the recipient will be the endpoint for receiving Activity objects of another TWIN DS Connector. Therefore, Activity objects are used to both receive “events of interest” and to send “events of interest” in TWIN Data Spaces.

   Obviously, a subscription is also subject to Policy enforcement, i.e. only those parties which can get access to certain data can actually subscribe to such data.

Figure 16 describes the data model of a subscription:

Name	Tag	Description
Details	Subscription ID	urn:x-subscription:6e8ffe0b5e5ac9f50723a4f99d5fa7719f0e93fd02d7465a5f42916ad5fd263c
	Type	Subscription

[49] https://docs.internationaldataspaces.org/ids-knowledgebase/dataspace-protocol/transfer-process/transfer.process.protocol#id-1.1.2-data-transfer-types

Name	Tag	Description
	Description	Subscribe to the availability of Phytosanitary certificates of Consignments destination UK
	Date Created	2024-10-02T14:19:26.413Z
Who	Subscriber	did:iota:ebsi:0xb62afcd0150d048ea0679af61d28d0eb1ad1b969f411b03997194df232b27383
Notification	Recipient ID	https://tlip-nodes.example.org/uk-borderforce-1
Object	Type	Document
	Business Step	Document issuance
	Document Type	unece:DocumentCodeList#851
Target	Type	Consignment
	Destination Country	unece:CountryId#GB

Figure 16 Subscription to a TWIN Data Space Connector

A subscription includes key details such as the subscriber Party (in this case, a Participant identified by a DID), the event of interest (e.g. document issuance of phytosanitary certificates), the items of interest (e.g. Consignments destined for the UK), and the recipient, identified by a URI. Since the recipient is specified by an ID, notifications are delivered to the final endpoint registered under that ID in the TWIN Catalog.. However, notifications can also be delivered to a bare endpoint (i.e. to a REST service that is not incarnated by a TWIN Node nor registered on the TWIN Catalog).

Notification delivery requires authentication by the corresponding TWIN Node, referencing the matching subscription including the expected subscriber. TWIN Nodes will ignore events that do not match these criteria, such as notifications sent to unknown Participants or to those not authorized to use the Node.

TWIN recognizes that one size does not fit all and that different ecosystems may require unique formats or custom reactions to Activities propagated through a Data Space Connector. To

address this, the **TWIN DS Connector App**, aligned with the International Data Spaces architecture, aims to allow the integration and deployment of complementary applications inside a Data Space Connector. These applications provide services on top of the generic data exchange processes, such as services for data processing, data format alignment, and data exchange protocols.

TWIN Adaptor

A TWIN Adaptor must implement at least the query interface (as described in point B here, and also known as the TWIN Adaptor Protocol) of a Data Space Connector). Typically, it is registered as a Data Resource in the TWIN Catalog and can be queried by authorized TWIN Nodes to provide data or documents by interfacing with an external system.

In addition, a TWIN Adaptor must also function as a **bridge** between an external system and a TWIN Node. This bridge propagates “events of interest” to the TWIN DS Connector when specific business workflows occur externally, such as the issuance of trade documents or the creation of new items.

Nonetheless, external systems may choose to implement an Adaptor with the full Data Space Connector interface (TWIN Data Exchange Protocol). This reinforces that it is not necessary to fully deploy a TWIN Node to participate in a TWIN Ecosystem .

Infrastructure Services

Definitions related to this section can be found in the glossary of terms.

Infrastructure software services provide the essential substrate that enables the functionality of a TWIN Node. Essentially, they include:

- Datastores (SQL or NoSQL).
- Blobstores i.e. large binary object stores (to store images, documents, etc.).
- Key Management Services (KMS) and Secret Management systems (like *Hashicorp Vault*[50]) to store encrypted information, particularly keys, with a high degree of security.

[50] https://www.vaultproject.io/

- Distributed Ledger Technology (IOTA) as a verifiable registry with code execution (smart contracts) capability at Layer 1 (Move Virtual Machine[51]) and Layer 2 (Ethereum Virtual Machine[52]).

TWIN is developing the following software components, which are key to keep a level of agnosticism concerning infrastructure services:

- **TWIN Datastore Connector**: A software component intended to store and query data/metadata concerning the entities managed by a TWIN Node (Auditable Items, Documents, TWIN Events, Participant Registrations, etc.).
- **TWIN Blobstore Connector**: A software component intended to store and fetch documents (trade documents, product certificates, etc.) managed by a TWIN Node.
- **Secret Management Connector** or *Vault Connector*: A software component intended to store secrets encrypted, manage their lifecycle (rotation, revocation, etc.), and to control access to them. It is concerned with secrets needed by the different systems within TWIN, including those kept in custody, such as the keys of a Participant or service.
- **TWIN DLT Connector:** A software component intended to settle transactions (with or without smart contract intervention) or to read entries from a distributed ledger for data traceability, verifiability or timestamping purposes.

TWIN offers a DLT Connector for IOTA, a Vault Connector for Hashicorp Vault, a blobstore connector for IPFS[53] and S3[54], and multiple flavours of datastore connectors, including DynamoDB[55] and ScyllaDB[56] for maximum data scalability.

DLT and TWIN

TWIN fully exploits the four key characteristics of a public, permissionless DLT:

- **Transparency**, the append-only ledger is auditable by the whole network.
- **Immutability**, as data cannot be easily tampered with.

---

[51] https://docs.iota.org/developer/iota-101/move-overview/

[52] https://evm.iota.org/

[53] https://ipfs.tech/

[54] https://aws.amazon.com/s3/

[55] https://aws.amazon.com/dynamodb/

[56] http://scylladb.com/

- **Traceability and nonrepudiation**, because each network participant cryptographically signs each transaction issued in the immutable ledger.
- **Decentralized execution** of immutable instructions, i.e., smart contracts.

In addition, the rise of decentralized applications (dApps) has created a need for standardized methods of representing information on DLTs. One of the most widely used approaches is *token* representation, where information recorded on a DLT represents a specific right, such as ownership of an asset, access to a service, or receipt of payment, etc. Fungible tokens are commonly used for second-layer cryptocurrencies, including stablecoins, as they maintain uniform value and interchangeability. In contrast, Non-Fungible Tokens (NFTs) are utility tokens designed to represent and transact with unique tangible or intangible assets on DLTs. Unlike fungible tokens, each NFT is distinct and non-interchangeable.

The five key DLT features explained above are applied to TWIN through the IOTA DLT as follows:

- The Ledger plays the role of a Verifiable Registry, avoiding the need of trusted central entities, facilitating among others:
    - identity (DID) registration, resolution, verification and traceability.
    - credential revocation lists stored on-chain as bitmap strings.
    - as a helper for snapshotting and bootstrapping of enabling and federation services, namely the TWIN Catalog and TWIN Registry functionalities.
    - Trust anchor registration on-chain including traceability of their public Verifiable Credentials.
    - TWIN Clearing House functionalities (through smart contracts and NFTs).
- Objects managed by TWIN can be made auditable, improving Participant trust in traceability. Each critical event or relevant change is immutably recorded and timestamped on the Ledger, ensuring transparency and verifiability.
- The Ledger facilitates dispute resolution, recording transactions within a TWIN ecosystem, such as data exchange transactions..
- Key trade documents that are transferable records (BoL, invoice, etc.) managed by TWIN can be tokenized through an NFT on the Ledger, enabling the transfer of the ownership, rights and obligations.
- Luxury items tracked by TWIN can be tokenized as NFTs, facilitating product authentication, brand image, customer engagement, and so on.

In a nutshell, dApps built with TWIN leverage the verifiability of information stored on the distributed ledger and authentication mechanisms based purely on cryptographic primitives.

The operational models can vary:

- Each TWIN Participant may have their own ledger account owning the different assets and funding gas fees of each DLT transaction.
- TWIN Nodes can be delegated by Participants to have control and ownership over certain assets, including those that allow funding transactions..

TWIN also supports hybrid approaches where a TWIN Node can sponsor transactions using an IOTA Gas Station, while Participants remain the actual asset owners. Furthermore, some TWIN Nodes may also function as a DLT Validator, earning validation fees. The final setup may depend on business, subscription or operational models, a topic outside the scope of this whitepaper.

Edge Devices and Connectors

Edge devices deal with automatic identification and data capture (AIDC). They play an important role: bridging the physical world of trade items with their corresponding digital twin, represented as an Auditable Item. On one hand, as physical resources, Edge Devices are owned and operated by Participants and can form part of the underlying infrastructure. In cases where compliance tracking is required, they may even be onboarded through **Compliance Credentials** to verify their compliance status or device credentials.

On the other hand, through their **Edge Device Connector**, these devices can be characterized as Data Resources, providing events and data of interest to a TWIN Node. For example, an RFID Reader can report that a set of trade items have been read at a particular location. The Edge Connector can listen to the Reader's low level events (device events) and transform them into higher-level events (TWIN Events), recording them on a TWIN Node. Afterwards, the corresponding Auditable Items will be updated and new TWIN Events registered on the Event Repository, identifying the source as the Reader in question, etc. Additionally, DLT-based event notarization, could be used to certify whether an item was physically in the possession of its claimed owner.

This architecture is not limited to RFID Readers but can be extended to **mobile sensors, scanners, printers**, and other **Edge Devices**, enabling seamless integration into the **TWIN ecosystem**.

To validate this architecture, initial experiments were conducted by the IOTA Foundation in collaboration with Zebra Technologies using the **FX9600 RFID Reader**[57]**.** This device incorporates the Zebra IoT Connector[58], a software that enables applications to be built that leverage the Reader's capabilities without having to develop specific software to be run on the

[57] https://www.zebra.com/gb/en/products/rfid/rfid-readers/fx9600.html

[58] https://www.zebra.com/gb/en/software/rfid-software/iot-connector.html

device itself. The Zebra IoT Connector supports Web Hooks (or MQTT) for data transmission. For instance, when a reading cycle begins and several RFID tags are detected, a JSON payload will be sent through a Web Hook (HTTP POST) with the details of the tags read (EPC, TID, etc.). That is a Tag Data Event that could be transformed into another Event by the corresponding TWIN Edge Connector that reacts to the Webhook notifications. Finally, TWIN Events will be registered in a TWIN Node via an Edge Device Connector that will have to authenticate itself on behalf of the Edge Device or on behalf of the Device's owner.

A similar architecture can be put in place with other Edge Devices such as mobile sensors, scanners, printers, etc.

Common Platform Services

The following services offer cross-cutting functionalities to other services within a Node:

- **Telemetry**, which includes **logging** and **metrics** functions. Logging involves keeping a log of events that occur within the different TWIN software services, such as problems, errors or information on current operations. Metrics relate to the quantitative measures used to evaluate the performance and efficiency of the various software components.A TWIN Node exposes Open Telemetry[59] interfaces so that it can be easily monitored using Promotheus and Grafana.
- **Background Tasks:** A service that allows to schedule asynchronous tasks that have to be executed immediately or at a scheduled time.
- **Messaging:** A service that can deliver notifications through different messaging channels (SMS, email, etc).
- **Local User Management:** This is an internal service within a Node that allows the creation of different user or service accounts **internal** to a Node. Those accounts are not visible to other Nodes.

Local User Management and Policies

It is important to differentiate between local user management and Participant management through the TWIN Catalog. A Participant or Service instance registered on the Catalog might interact with any TWIN Node by proving her Identity through a (SD-)JWT token generated through a Credential Wallet. Depending on the services offered through the Catalog, their

[59] https://opentelemetry.io/

policies and the Participant's attributes, the Node will either respond with data or documents or will deny the request.

Additionally, to interact with a specific Node, a Participant may own additional user or service accounts added by a Node operator. For instance, a Participant may have deployed multiple TWIN Native solutions, and each of these client services may have their own service account in their Node. Going further, there can be clients of a TWIN Node that are not even registered on the TWIN Catalog because they are private Data Producers behind the façade of a Node. Local user or service accounts will not be visible to other Nodes, instead being purely local.

Concerning authentication, a TWIN Node could play the role of resource server within OpenID Connect and enable local authentication of clients together with an OpenID Provider. Concerning authorization, there might be local policies associated with each account that dictate local rules for the use of the Node services by the authorized Participants. Policies can be described and executed as already described for Data Exchange Services.

Glossary

The following definitions have been adapted (and sometimes taken literally) from different sources cited at the end of this Whitepaper.

Technology-related

Identity and Credentials

- **Attribute Service Provider:** A type of Trust Service Provider with the role of collecting, creating, checking or sharing pieces of information that describe something about a Participant. Attribute Service Providers can share their attributes with relying parties and Identity Service Providers, subject to rules of obtaining Participant's agreement being followed.
- **Certificate Authority:** The entity in a Public Key Infrastructure (PKI) that is responsible for issuing public-key certificates and exacting compliance to a PKI policy. Also known as a Certification Authority.
- **Credential:** A set of one or more claims made by an issuer.
- **Credential Dataset** defines the data (claims) about a subject that is to be included in a Credential.
- **Credential Format:** A Data Model used to create and represent Credential information. This format defines how various pieces of data within a Verifiable Credential are organized and encoded. TWIN supports both JWT and JSON-LD (using the W3C VC Data Model).
- **Credential Manager:** A synonym for "Credential Wallet".
- **Credential Issuer** (or Issuer): An entity that issues Verifiable Credentials.

- **Credential Status List:** A mechanism used by a Verifiable Credential issuer where a verifier can check to see if a credential has been suspended or revoked.
- **Credential Wallet**: An entity used by the Holder to request, receive, store, present, and manage Verifiable Credentials and cryptographic key material.
- **Decentralized Identifier** (DID:. A type of entity identifier that is globally unique, resolvable with high availability, and cryptographically verifiable. DIDs are used to identify Participants within a TWIN Ecosystem.
- **Holder:** An entity that receives Verifiable Credentials and has control over them to present them to the Verifiers as Presentations.
- **Identity:** A set of attributes related to an entity.
- **Identity Service Provider:** A type of Trust Service Provider with the role of proving and/or verifying Participant's identities. They can do this using online (for instance through a Trusted Data source) or offline channels, or a combination of both. An Identity Service Provider can be a public or private sector organization (for instance, a bank).
- **Key Management System:** A system for the management of cryptographic keys and their metadata (e.g., generation, distribution, storage, backup, archive, recovery, use, revocation, and destruction). An automated key management system may be used to oversee, automate, and secure the key management process.
- **KYC:** Know your Customer. It is a process intended to verify the identity of new Participants. There can be multiple mechanisms and providers of KYC services.
- **Party Credential:** A Verifiable Credential that attests the attributes of a Service-Offering, Data Resource or Participant.
- **Public Key Infrastructure:** A way to implement secure electronic transactions over insecure networks, such as the internet. It's used to authenticate identities for the purposes of data encryption and signing.
- **Relying Party (or Verifier):** A role an entity performs by receiving one or more Verifiable Credentials, optionally inside a Verifiable Presentation for processing. A TWIN Node might play this role when processing requests issued by other TWIN Nodes.
- **Trust List:** Collection of trusted certificates used by Relying Parties to authenticate other certificates.
- **Trust Service Provider:** A role performed by an external entity to the TWIN ecosystem by offering identity verification or attribute attestation.
- **Verifiable data registry:** A role a system might perform by mediating the creation and verification of identifiers, keys, and other relevant data, such as verifiable credential

schemas, revocation registries, issuer public keys, and other rules. Example verifiable data registries include trusted databases, decentralized databases, government ID databases, and distributed ledgers. Often there is more than one type of verifiable data registry utilized in an ecosystem.

- **Verifiable Credential:** A tamper-evident credential that has authorship that can be cryptographically verified. Verifiable credentials can be used to build **verifiable presentations**, which can also be cryptographically verified.
- **Verifiable Presentation:** A tamper-evident container of data derived from one or more verifiable credentials, issued by one or more issuers, that is shared with a specific verifier by a holder.
- **Verifier:** An entity that requests, receives, and validates Presentations.

Data Spaces

- **Authentication:** The process of verifying the identity of a requesting party, as a prerequisite to allowing access to resources.
- **Authorization:** The process of verifying whether a requesting party is allowed to access resources (Data Resource, Service instance, etc.).
- **Creator:** Also known as *Data Producer*, the Creator generates data, e.g. by generating data such as from a sensor or accessing data in backend IT systems. In international trade an exporter filling out an export declaration is playing the role of “Data Producer”.
- **Data** here is synonymous with Data Asset, i.e. content exposed for exchange by a Participant acting as a Data Provider.
- **Data Sovereignty:** The ability of a natural or legal person to exclusively and sovereignly decide concerning the usage of data as an economic asset.
- **Data Exchange:** Data exchange takes place in the vertical cooperation between organizations to support, enable or optimize value chains and supply chains.
- **Data Resource:** Description of an object in a TWIN Ecosystem, that may be aggregated in a service (i.e. an offering made by a Provider) or exist independently of it, and which manages certain data of interest to the ecosystem Participants. It is characterized by endpoints and access rights. There can be different types of Data Resources, for instance, resources wrapping a data set, IoT device data, etc., document Resources (exposing an endpoint to get access to issued trade documents or supply chain certificates, etc.).

- **Operator:** Providers that have been approved by the ecosystem governance to operate Federation Services and the Federation, which are independent of each other. There can be one or more Operators per type of Federation Service.
- **Policy:** A group of one or more Rules that concern Services or Resources.
- **Policy Enforcement:** System functionality intended to execute policies so that Providers or Consumers are ensured to meet the rules associated with Services or Data Resources.
- **Rule:** An abstract concept that represents the common characteristics of Permissions, Prohibitions, and Duties.
- **Service-Offering:** A set of Data Resources, which a Provider aggregates and publishes as a single entry in a TWIN Catalog**.** A Service-Offering is consumed through a *Service instance* whose endpoint and access rights are declared through a Service-Offering Credential.
- **Service-Offering Credential:** A type of Party Credential, in alignment with Gaia-X principles, a Service Offering description attested by its Provider, that follows the corresponding TWIN Schema, and whose claims are validated by the TWIN Clearing House**,** thus producing the corresponding Service-Offering Compliance Credential.
- **TWIN Schema:** A JSON Schema or SHACL JSON-LD aimed at validating different data elements within TWIN (Items, Credentials, Events, etc.). TWIN Schemas aim at alignment with Gaia-X by using the same Vocabulary and structure (but with extensions when needed).
- **TWIN Registry:** A verifiable data registry that captures Trust Anchors, TWIN Schemas and Ecosystem (participation) Rules which are key to comply within a TWIN Ecosystem. For decentralization purposes TWIN aims at a DLT-based (IOTA) implementation.
- **TWIN App:** Self-contained, self-descriptive software package that can be distributed via different package managers and deployed to extend the functionality of a TWIN Node.
- **TWIN App Provider:** The developer or distributor of a TWIN App.
- **Vocabulary** ontologies, reference data models, or metadata elements that can be used to annotate and describe participants, datasets, usage policies, apps, services data sources etc.

DLT

- **Asset:** A representation of value.

- **Content addressable storage:** A way to store information so it can be retrieved based on its content, not its name or location.
- **Decentralized Storage:** A mechanism for storing data, split into small pieces, across multiple computers or nodes connected to a P2P network like the InterPlanetary File System (IPFS) protocol.
- **Decentralized Storage Node:** A Node participating in a Decentralized Storage system.
- **Decentralized System:** A distributed system wherein control is distributed among the persons or organizations participating in the operation of the system.
- **Distributed Ledger**: A type of ledger that is shared, replicated, and synchronized in a distributed and decentralized manner.
- **DLT Commitment**: A record stored by an application on a Distributed Ledger that enables to prove data stored externally has not been tampered. A DLT commitment can also be used for timestamping purposes.
- **DLT Node**: device or process that participates in a distributed ledger network.
- **Fingerprint:** A cryptographic hash of the content of an object (file, document) that allows integrity checking.
- **NFT:** (Non-fungible token) an entirely unique digital representation of an asset.
- **Timestamping:** A timestamp proves that a message existed prior to some point in time. Timestamping, also known as notarization, is the act of creating a timestamp.
- **Public distributed ledger system**: A distributed ledger system which is accessible to the public for use.
- **Permissionless distributed ledger system**: A distributed ledger system where permissions are not required to maintain and operate a node.
- **Smart Contract:** A program written on the distributed ledger system which encodes the rules for specific types of distributed ledger system transactions in a way that can be validated, and triggered by specific conditions.

Domain specific

Value Chains

- **Automatic Identification and Data Capture (AIDC):** The automated process of identifying and capturing data about trade items facilitating tracking, processing, and inventory processes. AIDC technologies include different variants of barcodes, QR Codes, smart cards, biometrics, RFID, NFC or even machine learning/deep learning techniques.
- **Auditable Item:** A Trade Item whose history is explicitly captured by an information system. Each historical state's fingerprint of an Auditable Item can be recorded on a Distributed Ledger for timestamping purposes, enabling actors to perform external data verification.
- **Auditable Item Graph:** A graph in which vertices correspond to Auditable Items and edges to relationships among those Auditable Items (child of, parent of, etc.).**Global Trade Item Number (GTIN)** A Trade Item identifier scheme for which GS1 is the authority. The GTIN can be used to identify types of products at any packaging level (e.g. consumer unit, inner pack, case, pallet).
- **Circularity:** An economic model that aims to minimize environmental impact by reducing waste and maximizing reuse. A useful conceptual reference is the "9R framework[60]" (*refuse, rethink, reduce, reuse, repair, refurbish, remanufacture, repurpose, recycle and recover*).
- **Digital Link:** A Trade Item Identifier encoded as a persistent URL that when resolved leads to machine readable information about the concerned item. A GS1 Digital Link is a Digital Link that encodes a GS1 EPC.
- **Digital Product Passport:** A structured collection of product related data with predefined scope and agreed data management and access rights conveyed through a unique identifier and that is accessible via electronic means through a data carrier. The intended scope of the DPP is information related to sustainability, circularity, value retention for re- use, remanufacturing, and recycling.
- **ESPR Regulation:** *Ecodesign for Sustainable Products Regulation (EU)*. A framework of environmental sustainability requirements for European goods, making mandatory a Digital Product Passport for certain products on the EU market. Under the framework of the EU Green Deal, the European Commission has adopted the Ecodesign for

[60] EC "Categorization System for the Circular Economy", March 2020, available at https://circulareconomy.europa.eu/platform/sites/default/files/categorisation_system_for_the_ce.pdf .

Sustainable Products Regulation (ESPR) in 2024. The overall aim of the regulation is to reduce the lifecycle environmental impacts of products through efficient digital solutions.

- **FSMA Regulation:** *Food Safety Modernization Act (US FDA)* A regulation for the way foods are grown, harvested and processed. It includes several rules such the Preventive Controls rules for Human and Animal Food, the Produce Safety rule, and the Foreign Supplier Verification Programs (FSVP) rule.
- **Supply Chain:** All upstream activities and processes of the value chain of the product, up to the point where the product reaches the end-user (customer).
- **Supply Chain Event:** Data record concerning one or more Trade Items to enable visibility, within organizations as well as across an entire ecosystem of Participants. It helps answer the questions “what, when, where, why and how” of Trade Items, enabling the capture and sharing of key information such as status, location, movement and chain of custody.
- **Trade Item:** Items that represent pProducts or services that are priced, ordered or invoiced at any point in the supply chain. From an information management point of view, Trade Items are represented by a descriptive Digital Twin that captures their type, properties and relationships with other items.
- **Trade Item Identifier:** A collection of alphanumeric characters that can be used to identify a Trade Item. A GS1 Electronic Product Code (EPC) is a Trade Item Identifier represented using the GS1 identification scheme.
- **Trade Document:** Written, printed or electronic matter that is referenced and concerns a Trade Item. From an information management perspective, trade documents can have multiple representations, JSON-LD documents, PDF, XML, etc. Often trade documents carry key information referring to its concerned Trade Item.
- **Traceability:** According to the United Nations Global Compact and Business (UNGC), traceability is the ability to identify and trace the history, distribution, location and application of products, parts and materials, to ensure the reliability of sustainability claims, in the areas of human rights, labor (including health and safety), the environment and anti-corruption.
- **Value Chain[61]:** All activities and processes that are part of the life cycle of a product, as well as its possible remanufacturing.

[61] See also https://www.cisl.cam.ac.uk/education/graduate-study/pgcerts/value-chain-defs

International Trade

- **Airway Bill** The Air Waybill (AWB) is a critical air cargo trade document that constitutes the contract of carriage between the shipper and the carrier (airline).
- **Bill of Lading:** A trade document with contractual value, issued to the shipper which confirms the carrier's receipt of the cargo, acknowledging goods being shipped or received for shipment and specifying the terms of delivery (as one of the evidences of the contract of carriage). The Bill of Lading is usually prepared based on shipping instructions, including cargo description, given by the shipper on forms issued by the Carrier and is the title to the goods and can be a negotiable document. Bill of lading is historically a nautical term but does get used for other forms of transport (air, train, or truck shipments), which concern other similar documents such as the airway bill and CMR (road transport).
- **Buyer:** The Participant to whom goods are sold services as stipulated in a sales order contract.
- **Carrier:** The Participant who provides transport services.
- **Certificate of Origin** A trade document that attests the country of origin/originating status of a Trade Item. It is an attestation that can be used to claim the Trade Item satisfies the applicable origin criteria.
- **Commercial Invoice** A trade document that contains a demand of paying (concerning a Shipment) made from the invoice issuer (the invoicer, usually the Seller) to the invoicee (usually the Buyer).
- **Consignment:** A separately identifiable collection of Trade Items to be transported or available to be transported from one **consignor** to one **consignee** in a supply chain via one or more modes of transport where each consignment is the subject of one single transport contract.
- **Customs Declaration:** A trade document whereby a Participant indicates in the prescribed form and manner the request to place Trade Items under a customs procedure (outward Export or inward Import procedures). There must always be an Export and an Import customs declaration and these are made in the countries of dispatch and receipt, typically the declarations are made by different parties.
- **Export Declaration:** A type of Customs Declaration. The export declaration is made by the seller/despatcher of the goods or their customs agent. It is submitted to gain authorisation for the goods to leave a country and is mainly focussed on compliance (e.g. any standards that the goods might need to meet, any restrictions that apply to exporting particular types of goods, or the country that the goods are being sold/moved to).

- **Exporter:** The Participant who makes the export declaration, or on whose behalf the export declaration is made, and who is the owner of the goods or has similar rights of disposal over them at the time when the declaration is accepted.
- **EUDR** *Regulation on Deforestation-free Products (EU).* Rules to guarantee that the products EU citizens consume do not contribute to deforestation or forest degradation worldwide.
- **Freight Forwarder:** The Participant, on behalf of a shipper, undertaking the forwarding of goods by provision of transport, logistics, formalities services, etc. by liaising with Carriers.
- **Import Declaration**: A type of Customs Declaration. The import declaration informs goods compliance procedures for the receiving country and will be made by the buyer/receiver of the goods. There is also a financial element for an import declaration should customs import duty or sales tax apply.
- **Importer:** The Participant who makes, or on whose behalf a customs clearing agent or other authorized person makes, an import declaration.
- **MLETR Regulation** *Model Law on Electronic Transferable Records (United Nations)*. It aims to enable the legal use of electronic transferable records both domestically and across borders. The MLETR applies to electronic transferable records that are functionally equivalent to transferable documents or instruments.
- **Packing List:** A trade document. It provides the exporter, international freight forwarder, and ultimate consignee with information about a Consignment, including how it's packed, the dimensions and weight of each package.
- **Phytosanitary Certificate** A trade document that attests the necessary sanitary and phytosanitary measures have been taken for the protection of human, animal or plant life or health.
- **Seller:** The Participant selling goods or services as stipulated in a sales order contract.
- **Shipment:** A shipment is an identifiable collection of one or more trade items (available to be) transported together from the seller (original consignor/shipper), to the buyer (final/ultimate consignee). A Shipment may form part or all of a Consignment or may be transported in different Consignments. It is a synonym for Trade Delivery.
- **SPS regulations** Sanitary and Phytosanitary regulations — government standards to protect human, animal and plant life and health, to help ensure that food is safe for consumption.
- **Trade Finance** It represents the financial instruments and products that are used by companies to facilitate international trade and commerce. It makes it possible and easier for importers and exporters to transact business through trade.

- **Transferable documents or instruments** are paper-based documents or instruments that entitle the holder to claim the performance of the obligation indicated therein and that allow the transfer of the claim to that performance by transferring possession of the document or instrument. Transferable documents or instruments typically include bills of lading, bills of exchange, promissory notes and warehouse receipts.
- **UCR:** *Unique Consignment Reference*[62], a reference number, applied to all international goods movements for which Customs control is required, with the following characteristics: used only as an access key for audit, consignment tracking and information, reconciliation purposes; unique at both national and international level; applied at consignment level; issued as early as possible in the international transaction.

[62] https://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/ucr.aspx

References

[CIRPASS] CIRPASS Project. DPP in a nutshell. URL: https://cirpassproject.eu/dpp-in-a-nutshell

[GS1-Standard] GS1 General Specifications Standard. Release 24. URL: https://ref.gs1.org/standards/genspecs/

[GS1-EPCIS] GS1. EPCIS standard. Version 2.0. URL: https://ref.gs1.org/standards/epcis/2.0.0/

[GS1-Digital-Link] GS1. Digital Link standard. URI Syntax. Version 1.5.0. URL: https://ref.gs1.org/standards/digital-link/uri-syntax/

[DCSA-Shipping-Glossary] Digital Container Shipping Association (DCSA). Shipping Glossary. URL: https://dcsa.org/standards/shipping-glossary

[EC-ESPR] European Commission. REGULATION (EU) 2024/1781 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 June 2024. Establishing a framework for the setting of ecodesign requirements for sustainable products. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401781

[EC-Deforestation] European Commission. REGULATION (EU) 2023/1115 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 May 2023. Making commodities and products associated with deforestation and forest degradation available on the Union market

and as exports from the Union. URL:
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1115

[ETSI-NGSI-LD] ETSI GS CIM 047 V1.1.2 (2024-12). Context Information Management (CIM);

NGSI-LD API. URL:
https://www.etsi.org/deliver/etsi_gs/CIM/001_099/009/01.08.01_60/gs_CIM009v010801p.pdf

[EU-Data-Spaces] European Commission. COMMISSION STAFF WORKING DOCUMENT of January 2024. Common European Data Spaces. URL:
https://ec.europa.eu/newsroom/dae/redirection/document/101623

[US-FSMA] 'FDA Food Safety Modernization Act'. PUBLIC LAW 111–353—JAN. 4, 2011. URL:
https://www.govinfo.gov/content/pkg/PLAW-111publ353/pdf/PLAW-111publ353.pdf

[Gaia-X] Gaia-X Consortium. What is Gaia-X?. URL: https://gaia-x.eu/what-is-gaia-x/

[Gaia-X-Architecture] Gaia-X Consortium. Gaia-X Architecture Document v24.04. URL:
https://docs.gaia-x.eu/technical-committee/architecture-document/24.04/

[Gaia-X-Credentials] Gaia-X Consortium. Gaia-X Identity, Credential and Access Management Document v24.07 . URL:
https://docs.gaia-x.eu/technical-committee/identity-credential-access-management/24.07

[IDSA-RAM-4] International Data Spaces Association. Reference Architecture Model v4.
https://docs.internationaldataspaces.org/ids-knowledgebase/ids-ram-4

[ITU-T-DLT] ITU-T Focus Group on Application of Distributed Ledger Technology. Technical Specification FG DLT D1.1 Distributed ledger technology terms and definitions. URL:
https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d11.pdf

[OIDC4VCI] OpenID Foundation. OpenID for Verifiable Credential Issuance. Draft 15. December 2024. URL: https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html

[OIDC4VP] OpenID Foundation. OpenID for Verifiable Presentations. Draft 23. December 2024. URL: https://openid.net/specs/openid-4-verifiable-presentations-1_0.html

[IEFT-SD-JWT-2024] Fett, D., Yasuda, K., and B. Campbell, "Selective Disclosure for JWTs (SD-JWT)", Work in Progress, Internet-draft, draft-ietf-oauth-selective-disclosure-jwt-14, 15 November 2024, URL: https://datatracker.ietf.org/doc/html/draft-ietf-oauth-selective-disclosure-jwt-14

[UN/CEFACT-BSP] United Nations Economic Commission for Europe. Centre for Trade Facilitation and Electronic Business. (UN/CEFACT). Buy–Ship-Pay (BSP) Reference Data Model. Summary presentation. URL: https://unece.org/fileadmin/DAM/cefact/brs/BuyShipPay_BRS_v1.0.pdf

[UN/CEFACT-Rec49] UN/CEFACT. Draft Recommendation No. 49 - Transparency at Scale. URL: https://unece.org/sites/default/files/2024-07/ECE-TRADE-C-CEFACT-2024-06E_0.pdf

[UN/CEFACT-VC-Trade] UN/CEFACT. White Paper eDATA Verifiable Credentials for Cross Border Trade. September 2022. URL: https://unece.org/sites/default/files/2023-08/WhitePaper_VerifiableCredentials-CrossBorderTrade_September2022.pdf

[UN/CEFACT-Prod-Certificate] UN/CEFACT. White Paper on Digital Product Conformity Certificate Exchange. October 2023. URL: https://unece.org/sites/default/files/2023-10/WhitePaper_DigitalProductConformityCertificateExchange.pdf

[UNCITRAL-MLETR] United Nations Commission on International Trade Law (UNCITRAL). Model Law on Electronic Transferable Records. (MLETR). URL: https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/mletr_ebook_e.pdf

[UNTP] UN/CEFACT. United Nations Transparency Protocol (UNTP). Technical specification. URL: https://uncefact.github.io/spec-untp/docs/about

[W3C-Activity-Streams] Activity Streams 2.0. 23 May 2017. W3C Recommendation. URL: https://www.w3.org/TR/2017/REC-activitystreams-core-20170523/

[W3C-Data-Integrity] Verifiable Credentials Data Integrity 1.0. W3C Candidate Recommendation. 26 January 2025. URL: https://www.w3.org/TR/vc-data-integrity/

[W3C-DID-Core] Decentralized Identifiers (DIDs) v1.0. Core architecture, data model, and representations. 19 July 2022. W3C Recommendation. URL: https://www.w3.org/TR/2022/REC-did-core-20220719/

[W3C-JSON-LD] JSON-LD 1.1. A JSON-based Serialization for Linked Data. 16 July 2020. W3C Recommendation. URL: https://www.w3.org/TR/2020/REC-json-ld11-20200716/

[W3C-VC-DATA-MODEL] Verifiable Credentials Data Model v1.1. 3 March 2022. W3C Recommendation. URL: https://www.w3.org/TR/vc-data-model-1.1/

[W3C-ODRL-22] ODRL Information Model v2.2. 15 Feb 2018. W3C Recommendation. URL: https://www.w3.org/TR/2018/REC-odrl-model-20180215/

[WCO-Guidelines] World Customs Organization (WCO). Guidelines on certification of origin. https://www.wcoomd.org/-/media/wco/public/global/pdf/topics/key-issues/revenue-package/guidelines-on-certification.pdf

[WCO-Instruments] World Customs Organization (WCO). Instruments and tools. URL: https://www.wcoomd.org/en/topics/facilitation/instrument-and-tools.aspx

[WCO-Handbook] World Customs Organization. WCO Handbook on Inward and Outward Processing Procedures. URL: https://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/instruments-and-tools/tools/wco-handbook-on-inward-and-outward-processing-procedures/pc_handbook.pdf

[WTO-Sanitary] World Trade Organization (WTO). Agreement on the Application of Sanitary and Phytosanitary Measures. URL:

https://www.wto.org/english/docs_e/legal_e/15sps_01_e.htm

[WTO-Glossary] World Trade Organization (WTO). Glossary of terms. URL: https://www.wto.org/english/thewto_e/minist_e/min99_e/english/about_e/23glos_e.htm#ag

[WTO] World Trade Organization (WTO). Technical Information on Rules of Origin. URL: https://www.wto.org/english/tratop_e/roi_e/roi_info_e.htm

TWIN

twin.org

TWIN Whitepaper

Trade Worldwide Information Network

Seamless Trading for All