



**International
Standard**

ISO 20435

**Framework for representing
physical assets using tokens**

*Cadre pour la représentation des actifs physiques à l'aide de
jetons*

**First edition
2026-10**

Sample Document

get full document from standards.iteh.ai

Sample Document

get full document from standards.iteh.ai



COPYRIGHT PROTECTED DOCUMENT

© ISO 2026

All rights reserved.

This ISO publication is protected by copyright and is owned by ISO and/or its licensors.

The content of this ISO publication is provided under licence, not sold. Use is subject to the applicable licence terms issued by ISO, an ISO member body, or an authorized third-party distributor.

Except as required for implementation or expressly permitted by a separate licence, no part of this ISO publication may be reproduced, distributed, modified, used, or made available in any form or by any means – electronic or mechanical, including photocopying, scanning, recording, or posting on internal or external digital platforms.

Any use beyond the scope of the granted rights is prohibited and may result in legal action.

ISO copyright office
CP 401 • CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword	vi
Introduction	vii
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Overview	4
4.1 Background	4
4.2 Problems to address	4
4.3 Objective of the standard	5
4.4 Use case - digital product passport (DPP)	5
5 DID registry framework or reference architecture	7
5.1 Overview	7
5.2 DID registry framework	7
5.2.1 General	7
5.2.2 Data storage locations	8
5.3 Resolving the DID across multiple independent DID registries	8
5.3.1 General	8
5.3.2 Lookup registry	8
5.4 Tokenizing the DID data using NFTs	8
5.4.1 General	8
5.4.2 "Wrapping" the DID address in an NFT	8
5.4.3 NFT provides the DID registry encryption layer	9
5.4.4 Benefit: Ability to leverage advanced NFT features	10
5.5 pNFT minting sequence diagram	10
5.5.1 General	10
5.5.2 User interaction with inventory system	11
5.5.3 Data handling through middleware	11
5.5.4 Off-chain storage system interaction	11
5.5.5 Verifiable data registry and universal "Lookup"	12
5.5.6 Physical NFT (pNFT) creation	12
5.6 Alternate tokenization implementations	12
5.6.1 General	12
5.6.2 Data model in DID registry only implementation	12
5.6.3 Data model stored on-chain in the NFT layer	12
5.7 Framework conclusion	12
6 Physical asset identifier (PAI) generation method	12
6.1 Background and introduction	12
6.1.1 General	12
6.1.2 Rationale for hashing pre-existing universally unique identifiers	13
6.1.3 Harmonization with existing supply chain standards	13
6.2 DID generation method	14
6.2.1 General	14
6.2.2 DID generation method example	14
6.2.3 Use of alternate PAIs	14
6.3 Physical asset identifier (PAI) selection	14
6.4 PAI data object	15
6.5 Universal serial number (USN): a "DID URL shortening" method	15
6.5.1 General	15
6.5.2 USN shortening method	16
6.5.3 USN example	16
7 Asset data methods	16
7.1 Overview & general requirements	16

7.2	Types of asset data objects	17
7.3	Hashing method selection	17
7.3.1	Technical background	17
7.3.2	SHA-256 is the default hashing algorithm	17
7.3.3	Storing asset data history	17
7.3.4	Use of a non-binary hash tree approach	18
7.4	Encryption of data objects	18
7.5	Data object metadata	18
7.6	Quantum agility	19
7.7	Hash tree method – details	19
7.8	Snapshots and version identifiers	20
7.9	Hash tree generation and updating example	20
7.9.1	Overview	20
7.9.2	Initial minting of a pNFT	20
7.9.3	Remove data object A and re-mint the pNFT	21
7.9.4	Replace data object B with D	21
7.9.5	Hash tree generation and updating example conclusion	22
7.10	Hash tree explanation using a spreadsheet model	22
7.10.1	General	22
7.10.2	Snapshot 1: Initial minting	22
7.10.3	Snapshot 2: Deletion of data object A	22
7.10.4	Snapshot 3: deletion of B and addition of D	23
7.10.5	Snapshot 4: modification of metadata for object D	23
7.11	Justification for hash tree model	24
7.12	Hash tree storage location	24
7.13	Document size and computational considerations	24
7.14	Document management	24
7.15	Asset data permanence	24
8	Data objects and metadata	24
8.1	Overview	24
8.1.1	General	24
8.1.2	Schema and ontology	25
8.1.3	Default minimum viable schema to enable the transport layer	25
8.2	Alternative schema identification	25
8.2.1	General	25
8.2.2	Examples of schema identification	25
8.3	Data object types, schemas, metadata, attributes	26
8.3.1	General	26
8.3.2	Global attributes	26
8.3.3	System-level data object types	26
8.3.4	Mandatory system-level data object types	26
8.3.5	Optional system-level data object types	27
8.3.6	Optional business-level data object types	28
8.3.7	Traceability system integration	31
8.3.8	Designating permanent data objects	31
8.4	Metadata format	31
8.4.1	Ordering and required attributes	31
8.4.2	Use of structured data	31
8.5	Conclusion	32
9	Physical layer verification	32
9.1	Introduction	32
9.2	Resolving physical asset identifier (PAI) conflicts	32
9.2.1	General	32
9.2.2	Resolving ambiguity between “part number” vs “model”	32
9.2.3	Handling inconsistent identifiers for the same asset	33
9.2.4	Handling missing identifiers	34
9.2.5	Handling colliding identifiers	35
9.3	Documenting data extraction methods	36

	9.3.1	General	36
	9.3.2	Retrieval methods	36
	9.3.3	Manual data entry	37
10		DID method scheme	37
	10.1	General	37
	10.2	Overview of DID roles and components	37
	10.3	DID document and metadata	38
	10.4	DID generation method requirements	39
	10.5	DID format and syntax	39
	10.6	Standardized DID and API operations	39
	10.6.1	General	39
	10.6.2	Resolve DID	40
	10.6.3	Register DID	40
	10.6.4	Update DID	41
	10.6.5	Deactivate DID	41
11		Trust anchors and legalities	41
	11.1	General	41
	11.2	Natural person identification	42
	11.2.1	Digital credential requirements	42
	11.2.2	Trust anchor requirements	42
	11.3	Machine/software identification requirements	42
	11.3.1	Software interaction signing	42
	11.3.2	Trust anchor validation	42
	11.4	Issues and considerations	42
	11.4.1	Maturity of SSI/decentralized identity standards	42
	11.4.2	Maturity of trust anchor standards	42
	11.4.3	Legal ownership framework	42
	11.5	Current domain-specific implementation	42
	11.5.1	Role of trade and membership associations	42
	11.5.2	Authority requests for device ownership	43
	11.6	References to ISO/TR 23644	43
12		Encryption, privacy and cybersecurity	43
	12.1	Overview	43
	12.2	DID authentication and encryption options	43
	12.3	Data transfer methods for encrypted pNFTs	44
	12.3.1	General	44
	12.3.2	Off-chain re-encryption method	44
	12.3.3	Keystore transfer method	44
	12.3.4	Implementation considerations	44
	12.4	Encryption methods	44
	12.4.1	Data object encryption	44
	12.4.2	Optional individual encryption	44
	12.5	DID and USN generation security considerations	44
	12.6	Privacy considerations	45
	12.6.1	Hashing and privacy	45
	12.6.2	User responsibility	45
	12.6.3	GDPR and privacy regulations	45
	12.7	Cybersecurity best practices	45
	12.8	Limitations and user responsibilities	45
	12.8.1	Limitations of the standard	45
	12.8.2	User responsibilities	45
	12.9	References to DID method specification	45
	12.10	Security conclusion	45
13		Conclusion	45
		Bibliography	47

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 307, *Blockchain and distributed ledger technologies*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

This document outlines a framework for representing physical assets by means of tokens. The standard is neutral on the choice of distributed ledger technology (DLT). This document introduces the universal serial number (USN), which is a standardized identifier derived algorithmically from existing asset identifiers. It also outlines methods for securely encoding physical asset data using decentralized identifiers (DIDs), creating a standardized and verifiable framework that enables seamless transfers across different systems.

The framework enables comprehensive tracking of physical assets throughout their lifecycle, offering significant environmental advantages. Additionally, this framework enables tokenization in initiatives such as digital product passports (DPP).

The framework includes the following key components:

- A DID generation method: How to transform the existing identifiers of any physical asset that has a serial number into a standard reproducible DID format called a USN.
- Physical asset data model: How to combine data objects about a physical asset into a standard provable structure, using a hash tree format.
- DID method scheme with standardized application programming interface (API) endpoints: To allow the digital representation to be transportable across independent DID registries.
- Business document classification: The minimum viable semantics that allow disparate systems to recognize the purpose (and legal requirements) of data objects.
- Physical layer verification: How to use trust anchors to verify and tie information about the real-world object to its digital representation as per ISO/TR 23644.

Sample Document

get full document from standards.iteh.ai

Sample Document

get full document from standards.iteh.ai

Framework for representing physical assets using tokens

1 Scope

This document establishes a digital ledger technology (DLT) agnostic, decentralized identifier (DID) framework for representing physical assets using tokens. This includes:

- A DID generation method: An algorithmic data method for generating DIDs from assets with immutable unique identifiers, e.g. serial numbers.
- A cryptographic method to tie asset data objects to the DID: An algorithmic hash tree data method for transferring a set of asset data objects that are cryptographically tied together, agnostic to any specific DLT or blockchain system.
- A DID method scheme: A DID method scheme to enable DID registry interoperability, so the digital representation can be stored, resolved or transferred to any compliant DID registry.
- Real world trust anchor processes: Processes for utilizing off-chain trust anchors to establish proof of real-world human and machine generated events and information that tie a real-world asset to its digital representation.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

W3C, Verifiable Credentials Data Model v2.0, W3C Recommendation 15 May 2025 <https://www.w3.org/TR/vc-data-model/>

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

3.1

asset

anything that has value to a stakeholder

[SOURCE: ISO 22739:2024, 3.1]

3.2

asset data object

data object (3.4) containing specific information about a physical asset

Note 1 to entry: Information may include documents, structured data, verified credentials or other information representing attributes, events or states of the asset within a distributed ledger system.

3.3

asset data set

collection of *data objects* (3.4) that comprehensively represent the information pertinent to a physical or digital *asset* (3.1)

Note 1 to entry: This may include historical, operational and identification data.

3.4

data object

individual unit of data related to a physical *asset* (3.1) or its digital representation

Note 1 to entry: This data can be structured or unstructured and can include documents, images, structured data or other digital content.

3.5

decentralized identifier

DID

identifier that is issued or managed in a decentralized system and designed to be unique within a context

Note 1 to entry: Decentralized identifiers are used in systems that do not rely on central registration authorities.

[SOURCE: ISO 22739:2024, 3.18]

3.6

DID registry

verifiable data registry (3.24) that provides the storage, resolution and management of *decentralized identifiers (DIDs)* (3.5), ensuring that DIDs are accessible and verifiable across different systems and platforms

3.7

digital asset

asset (3.1) that exists only in digital form or that is the digital representation of another asset

[SOURCE: ISO 22739:2024, 3.21]

3.8

digital product passport

DPP

digital document containing the lifecycle data of a product from manufacturing to end of life, to support transparency, conformity and sustainability practices

3.9

digital representation of a physical asset

digital format encapsulating all essential data and attributes of a physical asset, enabling it to be uniquely identified, managed and tracked within a digital ecosystem

3.10

distributed ledger technology oracle

DLT oracle

service that updates a distributed ledger using data from outside of a DLT system

Note 1 to entry: DLT oracles can be used by smart contracts to access data from sources external to the DLT system.

[SOURCE: ISO 22739:2024, 3.32]

3.11

lookup registry

decentralized system or service that stores and manages the resolution of digital identifiers across multiple registries, ensuring the correct linking and retrieval of asset data and digital representations

3.12

non-fungible

not capable of mutual substitution among individual units

Note 1 to entry: The individual units can be *digital assets* (3.7), e.g. *tokens* (3.20).

3.13

non-fungible token

NFT

token (3.20) that is non-fungible

[SOURCE: ISO 22739:2024, 3.64]

3.14

physical asset identifier

PAI

unique identifier for a physical asset, derived algorithmically, using identifiers affixed to the asset such as serial numbers, model or manufacturer data

3.15

physical asset token

PAT

digital token that represents a physical asset within a blockchain or distributed ledger system

Note 1 to entry: PATs are designed to track ownership, authenticity and provenance of the physical asset throughout its lifecycle. Depending on the implementation, a PAT is often realized as an NFT but can also be fungible or semi-fungible based on the asset's characteristics and requirements.

3.16

physical NFT

pNFT

physical asset token (3.15) implemented as a *non-fungible token* (3.13), representing a unique physical asset within a blockchain or distributed ledger system

Note 1 to entry: The pNFT purports to bind the digital representation of the asset to its physical counterpart, ensuring traceability and authenticity.

3.17

root hash

single hash value at the top of the hash tree that results from consecutively hashing pairs of child node hashes until a single hash remains

Note 1 to entry: This hash represents the entirety of the data stored in the tree. Any change in the data blocks at the leaves of the tree causes a change in the root hash, thus providing a quick way to verify whether any data has been altered.

3.18

semantic layer interoperability

ability of systems to use shared schema and ontologies to ensure that the content of exchanged data is consistently understood and processed across different platforms in a verifiable manner

3.19

snapshot

unique historical version of an *asset data set* (3.3), minted into a *physical non-fungible token (pNFT)* (3.16) at a point in time

Note 1 to entry: A snapshot serves as a single source of truth for the state of the asset at a point in time. Due to the gas and storage costs of re-minting an NFT, off-chain systems typically make intermediate data changes to an off-chain copy of the snapshot, only re-minting the pNFT as necessary for communication with external systems.

3.20

token

asset (3.1) that represents a collection of entitlements

3.21

transport layer interoperability

capacity of systems to exchange data seamlessly and verifiably across a network, without interpreting or modifying the content, regardless of differing underlying technologies or protocols

3.22

universal serial number

USN

shortened, universally unique identifier generated from the *physical asset identifier* (3.14) using cryptographic hashing

Note 1 to entry: The USN is intended to simplify identification while maintaining uniqueness across systems.

3.23

verifiable credential

digital document issued by a trusted authority that contains claims about an individual, organization, or object

Note 1 to entry: Verifiable credentials (VC) are cryptographically secure, tamper-evident and can be verified electronically. VCs enable the holder to prove information to a verifier without revealing unnecessary personal details, using a mechanism that ensures the integrity and authenticity of the claims presented.

[SOURCE: W3C Verifiable Credentials]

3.24

verifiable data registry

system for creating, verifying, updating, and deactivating of *decentralized identifiers* (3.5)

Note 1 to entry: A verifiable data registry can also be used for other cryptographically-verifiable data structures such as *verifiable credentials* (3.23).

[SOURCE: W3C Verifiable Credentials]

4 Overview

4.1 Background

This document aims to enable traceability throughout an asset's lifecycle. For example, in an initial use case focused on the electronics recycling sector, the framework facilitates tracking of asset authenticity, the status of data erasure and the recoverable materials value at the recycler.

Early attempts to develop decentralized approaches to asset lifecycle tracking were hampered by basic interoperability issues due to a lack of standards for modelling physical asset data into a standard tokenizable structure.

4.2 Problems to address

Absence of a standard universal identifier: Current systems lack standardized methods for assigning universally recognized identifiers to physical assets, complicating their integration and traceability across different platforms.

Lack of a standard asset data method: No common framework exists for transforming physical asset data into a secure digital form that can be tokenized, while maintaining verifiable links to the physical counterparts.

Lack of methods to bind digital representations to real-world assets: There is a need to establish methods to cryptographically tie real-world documents and events to their digital representations.

4.3 Objective of the standard

This document aims to resolve these issues by defining methods for generating unique identifiers and structuring asset data for transportability across disparate systems, whether DLT or otherwise, ensuring the data remains verifiable and linked to real-world events. The primary focus is on serialized assets, with provisions for extending the framework to other asset classes through future modifications. This document provides methods for user-defined NFTs to interact with supply chain systems that control physical assets. These methods enable tokenization of the physical asset data, facilitating its transfer across different technological platforms.

While the standard is agnostic regarding the form of governance for implementation, it provides the necessary structures for implementing governance, as per ISO/TS 23635. Decisions about how to create and manage a specific system are governance issues and are beyond the scope of this document. For example, the document says the name of the manufacturer should be included in generating the USN. Some systems can use the company's tax ID number, instead. A system for tracking livestock may use some number string generated by using a facial recognition algorithm.

4.4 Use case - digital product passport (DPP)

A DPP is a structured digital record that provides comprehensive data about a product's composition, origin, sustainability, compliance and lifecycle events, including ownership transfers, maintenance records and end-of-life disposal instructions to support circular economy initiatives. DPPs contain essential details such as raw material sources, manufacturing certifications and environmental data. DPPs aim to improve transparency, sustainability and accountability by enabling better resource tracking, reparability, recycling and compliance with environmental standards.

[Figure 1](#) illustrates a series of use cases for tracking an electronics product across its lifecycle using a DPP. The DPP is a digitalized set of information that accompanies physical products throughout their lifecycle, enhancing transparency for consumers and facilitating compliance with regulatory requirements.

This use case diagram implements the DPP using an NFT, connecting to a DID registry as an oracle service, to interact with the systems managing the physical asset.

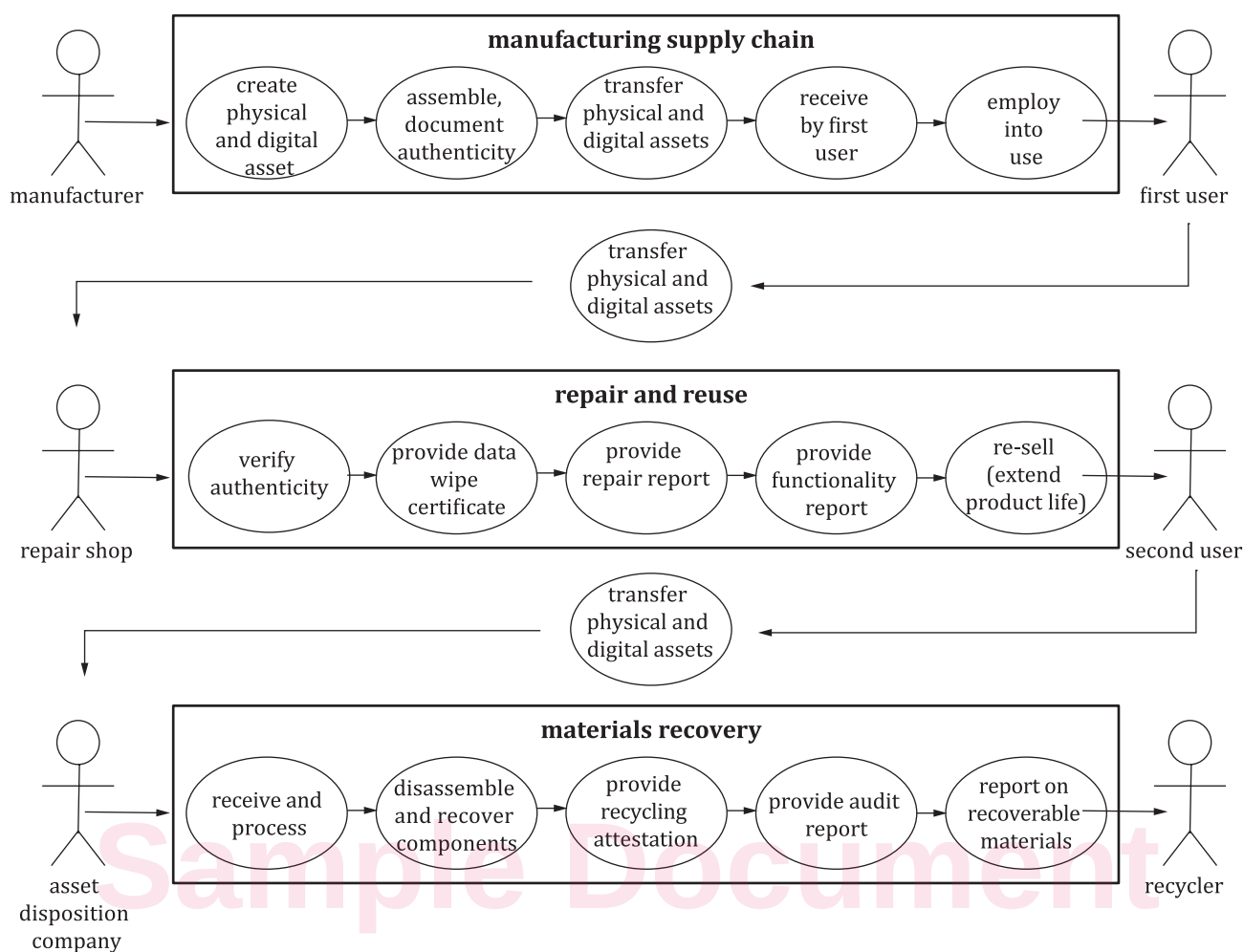


Figure 1 — Use case diagram: digital product passport (DPP) for tracking asset lifecycle

The use cases shown in [Figure 1](#) are divided into three primary lifecycle phases: manufacturing supply chain; repair and reuse; and materials recovery. Each integrates with the DPP for event recording and validation.

Manufacturing supply chain: The asset's journey through creation, transfer, reception and employment is immutably recorded by the associated NFT, immutably capturing provenance and other relevant details. This process outlined in the diagram aligns with a NIST publication "Supply Chain Traceability: Manufacturing Meta-Framework^[6]" for consistency with emerging industry standards for traceability.

Repair and reuse: The asset's authenticity is checked; maintenance, service, repairs and the exchange of components are recorded for verification; and the status of data included on the asset is recorded. Proving that sensitive data was destroyed with a "data wipe certificate" is critical for privacy and to prevent data breaches. All these items are crucial for secondary market transactions.

Materials recovery: At the end-of-life stage, assets are responsibly decommissioned, components are removed for reuse and recovery, and the reclamation of commodity materials such as gold, copper and rare-earth elements is documented. The recycling process is authenticated using W3C Verified Credentials, by industry trust anchors such as SERI,^[7] a standards body responsible for the methods used by electronics recycling facilities.

The use case diagram underscores the transparency and accountability facilitated by decentralized ledgers. It enables real-time DPP updates through a DID registry, with NFT re-minting safeguarding record integrity, visible to authorized actors throughout the lifecycle of an asset.

While this model technically enables governance frameworks, with accommodations for authorities and regulatory bodies for compliance and verification, it does not prescribe any specific governance structure.

5 DID registry framework or reference architecture

5.1 Overview

[Figure 2](#) illustrates a reference architecture for supply chain systems that implement this document. The data model outlined in [Clause 5](#) and [Clause 6](#) is a prerequisite to ensure transport layer interoperability of the data.

The underlying framework is designed to accommodate any asset class, emphasizing its broad applicability across various industries. Currently, the focus is on serialized physical assets with unique immutable identifiers, e.g. electronic devices with serial numbers. Future developments can expand this applicability by introducing methods to generate unique identifiers for asset classes that currently lack visible identifiers.

5.2 DID registry framework

5.2.1 General

At the centre is the independent DID registry, which stores verifiable digital information about physical assets. This registry is essential for linking the physical asset to its digital counterpart and serves as a DLT oracle service to allow the physical asset token (PAT) to connect to the real world.

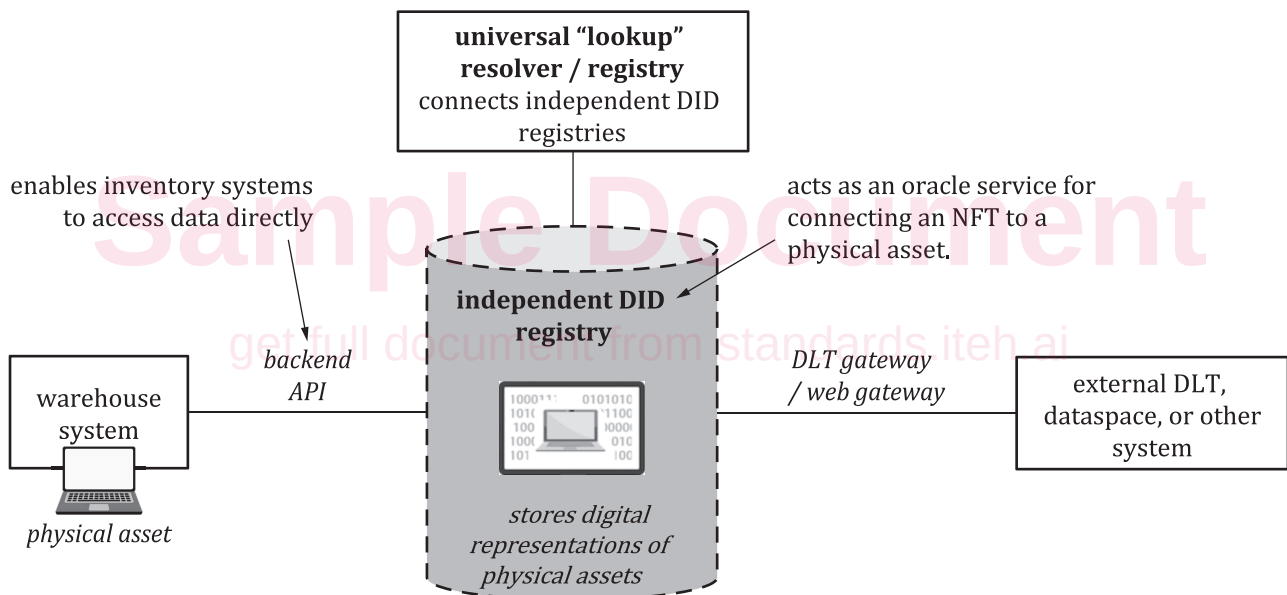


Figure 2 — DID registry reference framework for supply chain implementations

The “warehouse system” refers to an inventory system in a warehouse that is connected to the DID registry via a backend API. These systems have direct connections to the physical assets and already contain data about the asset which can be algorithmically restructured (per [Clause 6](#) and [Clause 7](#)) to tokenize it.

The DID registry is connected to an external DLT gateway or web gateway, so that external systems, like other blockchains, dataspaces or supply chain management systems, can access the DID registry data directly. The standardized data model ensures transport layer interoperability across various existing supply chain systems. This DID method approach uses DLT technology for data verification and interoperability, without the need for a third party, but it does not truly tokenize the digital representation of the physical asset.

The DID registry acts as a DLT oracle service so the digital representation can be tokenized by “wrapping” the DID address in an NFT. Thus, the DID registry address becomes a primitive building block for pNFTs, and consequently, pNFTs can become a database primitive for tokenizing physical assets inside of supply chain systems.