Chem-X Consortium

Report: Digital Material ID for the Chemical Industry

Version 0.9 – November 2025

(prepared for external consultation)

Funded by the Federal Ministry of Economic Affairs and Energy
BMWE

Funded by the European Union
NextGenerationEU

Supported by:
Federal Ministry for Economic Affairs and Energy
on the basis of a decision by the German Bundestag

Participating partners

Chem-X participating partners:

BASF SE	Siemens
Cofinity-X	Spherity GmbH
Covestro Deutschland AG	Wacker Chemie
DAW	Catena-X e.V.
Henkel	Together for Sustainability (TfS) AISBL
Merck	Evonik
SAP SE	Sika Services AG

Date	Version	Submitted by	Reviewed by	Comments
10.11.2025	0.9	Adrian Von Mühlenen		

Table of Contents

1 Motivation

Today's life would not be the same without dedicated and specialised materials that keep us healthy, our food fresh, our clothes clean and durable and help us get transported. Chemicals are inputs for 95% of manufactured goods [1] and are, therefore, a key pillar for the economies of industrialised countries and for the sustainable transformation of our economy and society.

Since chemicals are manufactured on a large scale in many sites around the globe, a recurring question is how to identify them properly. Properly isn't the right term; a more precise term is uniquely, persistently, and scalable. And to answer this question, it is good to adopt at least two distinct views:

- the supply chain view with a strong focus on logistics, and
- the value chain view with a strong emphasis on product information.

Both are relevant to establishing a trusted exchange of chemical product information throughout the product lifecycle. This becomes more prominent in the green transformation as the linear extract-use-dispose system phases out and is replaced by a circular economy, keeping physical products in service as long as possible and applying relevant and viable R-Strategies [2].

Another aspect that must be mentioned is the efficiency potential that can be addressed using a unique digital MaterialID for chemicals in harmonising product information exchange through value chains, which is currently a patchwork of company-specific numbers or ambiguous material identifiers, such as the CAS (Chemical Abstract Service) number, resulting in recurrent information disruption. The MaterialID shall facilitate access to product information in the relevant process for multiple value chain actors, e.g., to ensure the right to sell while ensuring compliance. Unlike today's processes, where we establish trust in material information by manual work, as represented in Figure 1, the MaterialID shall provide a trust infrastructure and access to structured and machine-readable data sets so that the information exchange among the value chain partners can be automated, leveraging efficiency potentials by enhanced data quality, faster response times, etc.

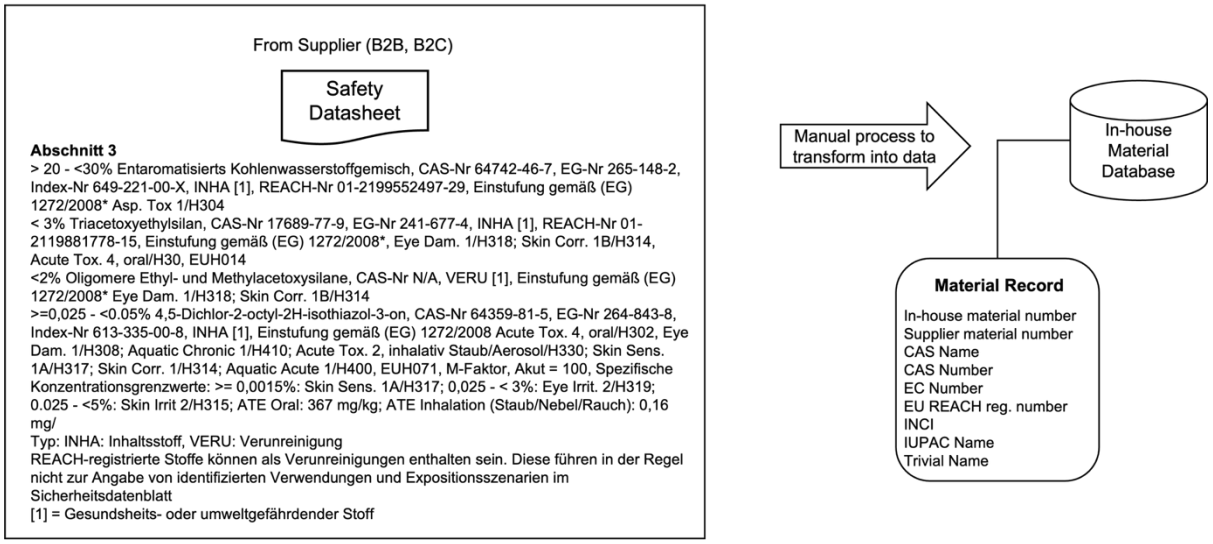

Figure 1 Today, product information exchange is document-centric, broken, and manual because of a lack of trust

1.1 Value Chain Communication

The chemical industry operates in a highly regulated environment, as some products can be harmful to humans, animals, and the environment if not handled safely. Therefore, product information communication in the value chain to economic actors is a key requirement for the right to operate and the right to sell chemical products. Such communication is mostly conducted using a document-based approach, e.g., with labels and safety data sheets (SDSs) required by [6, 7]. These documents use different, region and segment-specific identifiers for chemical products such as

- CAS Number – globally recognised numeric identifier for chemical substances
- EC Number – identifier assigned by the European Commission (EC) to substances for regulatory purposes. The EC Inventory comprises three individual inventories, EINECS, ELINCS and the NLP
- REACH Registration Number - identifier assigned by the European Chemicals Agency (ECHA) to substances registered under the REACH regulation
- UFI Number – unified formula identifier required for the notification of a hazardous mixture at a national poison center
- INCI Name – international identifier for cosmetic ingredients

This non-exhaustive list of identifiers for chemical products represents so-called speaking codes and provides human-readable information. The complication with such identifiers is the governance and maintenance across systems. Every so often, speaking codes do not meet the requirements laid out in sections 3.1 and 3.2. Hence, this report recommends including these identifiers in the digital material or product passport to foster compatibility with current business processes.

1.2 Out of Scope: Supply Chain Communication

Although out of scope, we shall briefly address identifiers that support global trade and are integrated in the backbone of many processes in international firms. These identifiers support the right to win by ensuring the delivery of the value in time and the quality expected by customers.

Identifiers used for Business Partners are:

- DUNS – International business entity identifier issued by Dun and Bradstreet
- LEI – International business entity identifier issued by the Global Legal Entity Identifier Foundation
- GLN – Global Location Number assigned to a physical location or entity issued by GS1

As for Materials following identifiers are used:

- EAN – International Article Number issued by GS1. Part of the GTIN specification
- DUNS – International business entity identifier issued by Dun and Bradstreet
- LEI – International business entity identifier issued by the Global Legal Entity Identifier Foundation
- GLN – Global Location Number assigned to a physical location or entity issued by GS1
- GTIN – Global Trade Item Number issued by GS1
- UPC – Universal product code issued by GS1. Part of the GTIN specification

For supply chain communication and related documents and messages, the non-exhaustive list of product, location, and organisation identifiers is essential to ensure seamless processes and integration of EDI-based protocols with CRM, ERP, PIM, and other business process-relevant systems and integrated in processes such as Order to Cash (OTC) or Purchase to Pay (P2P).

2 Objective

This report aims to outline the method and architecture for defining and structuring a digital MaterialID for chemical products.[1]

A digital MaterialID targets to identify a chemical product and, unlike known material identifiers such as CAS-Number, INCI Name, EC-Number, UFI Number, etc., provides a link from the physical product to its digital representation and its product information made available as a digital material passport (DMP) or digital product passport (DPP). The MaterialID shall be an opaque identifier with no significance, as outlined in the GS1 architecture principles [3]. Having said that, it becomes clear that the scope of the digital MaterialID is value chain communication —the business-value side that creates and delivers value to the value chain actors.

3 Requirements

In this section, we want to lay out the fundamental requirements from Chem-X viewpoint of an identifier that wants to link a physical chemical product to a digital representation of its product information represented in the digital material or product passport.

3.1 Technical Requirements

- Global Uniqueness – Ensure the identifier is distinct across all systems and domains. For example, there should be no duplicates or reused identifiers.
- Persistence – Ensures the identifier remains associated with one chemical product and unchanged over its validity or the product life cycle.
- Validity – Ensures the availability of the status (e.g. valid, invalid, revoked) of an identifier
- Integrity – Ensures the identifier is genuine and not altered or corrupted
- Scalability – Ensures the identifier can be issued in the required numbers in a timely manner
- Authenticity – Ensures the identifier's origin and legitimacy
- Privacy – Ensures the implementation of different visibility of the identifier

3.2 Business Requirements

- Regulatory Compliance – Ensures the identifier is compliant with regulations and standards
- Interoperability – Ensures the identifier is actionable (e.g. CRUD) in different systems

[1] Chemical products have many synonyms, such as material, chemicals, packaged goods, unpackaged goods, etc. For the sake of simplicity, we name them chemical products in this guideline. A stringent definition of these terms can be found in the

- Granularity – Ensures the identifier represents and addresses different granularity levels, such as model, batch, and item, following
- Sovereignty – Ensures that the control of the identifier is with the economic operator or its legal representative

4 Related Standards and Dataspaces

This chapter describes the existing Data Spaces, Regulatory, and Standards that are influencing the Chem-X Material / DMP / DPP Identifier.

4.1 EU DPP Framework Standards

CEN/CLC/JTC 24 draft standard proposes five identifier schemas:

- Web-enabled, structured path and query ID for products
- Identification Link (IL)
- Decentralised identifiers (DID) for products
- Product and group identification
- Digital Object Identifier (DOI) for a product has the biggest impact on the structure/semantics of a Material Identifier. As a standard proposal, the results of the prEN 18219:2025 [5] need to be considered.

4.2 Dataspaces

The number of available Dataspaces is growing; here, only a limited few will be considered. Catena-X as the most advanced, Manufacturing-X as they share different Material schemes, and IDSA as a non-X-Dataspace.

4.2.1 Catena-X

Catena-X uses a decentralised registry (like the AAS) to provide a unique identifier for a DPP in the form of a UUID, e.g.

`urn:uuid:123e4567-e89b-12d3-a456-426614174000`.

In Catena-X, a DPP includes additional identifiers for materials. The EU DPP registry must be used as a single point of contact/knowledge to create or resolve a DPP identifier.

4.2.2 Manufacturing-X

Manufacturing-X allows multiple identifier schemes for the DPP using a port concept. Example implementations are "Leo," "Hercules," and "Orion".

Leo uses the IEC 61406-2 ID Link concept to identify a DPP. In contrast, Hercules uses a UUID identification scheme in combination with the Data Space Protocol / Decentralised Claims Protocol based on an open-source EDC.

4.2.3 IDSA

The International Data Spaces Association (IDSA) recommends using the IEC 61406 standard for Unique Product Identification (UID) in industrial data spaces. However, more broadly and fundamentally, IDSA data spaces rely on a semantic and interoperable identifier scheme built around the following components:

- Decentralised Identifiers (DIDs)

    - (e.g., companies, services, connectors) in a
      Format: DID:<method>:<unique-id>
    - Purpose: To uniquely identify participants (e.g., companies, services, connectors) in a decentralised and verifiable way
    - Standard: Based on the W3C Decentralised Identifiers (DID) specification
    - Examples of DID methods used:
        - DID:web – Identifier based on HTTPS URLs
        - DID:indy – For identity based on distributed (indy) ledgers
        - DID:key – For identifiers based on cryptographic keys
- URI/URN/URL-based identifiers
    - Often used for data assets, contracts, and policies
    - Example: urn:ids:data:my-company.com:asset123
- UUIDs
    - For internal tracking and correlation within connectors or clearing houses.
- IEC 61406 family
    - Recommended for identifying physical products or assets in combination with their digital twins (especially in industrial or manufacturing settings).

4.3 Asset Administration Shell (AAS)

An Asset Administration Shell (AAS) is a standardised digital representation of an asset, such as a machine or component, used in Industry 4.0 for interoperability. It bundles all necessary information and functionalities of an asset into a structured digital model, consisting of modular "submodels," to enable secure and standardised data exchange between different systems. This provides a technological foundation for digital twins, allowing different companies and systems to communicate with each other seamlessly. [9] [10] [11] [12]

Key aspects of the AAS are:

- **Digital twin foundation:** The AAS serves as the technological foundation for the digital twin, providing a standard for describing and managing industrial assets.
- **Modular structure:** It uses submodels to structure the data, where each submodel describes a specific aspect of the asset, like its technical data, status, or capabilities.
- **Standardised information:** It provides a standard, machine-readable way to describe assets, their properties, and functions. This is crucial for enabling interoperability across different manufacturers and systems.
- **Interoperability:** The core goal is to enable seamless, standardised communication between different systems, software, and components in a connected industrial environment.

- **Lifecycle management:** An AAS can accompany a product throughout its entire lifecycle, from manufacturing to its use in operation.
- **Examples of assets:** An asset can be a single piece of equipment like a sensor, a complex machine, or even an entire factory.

The AAS supports the following standardised identifier types:

- IRI (Internationalised Resource Identifier):
  Example:

  ```
  urn:example.org:asset:12345
  ```

- IRDI (International Registration Data Identifier): Commonly used in ECLASS and IEC 61360 CDD (Common Data Dictionary) standard
- Custom (Short/Local). Locally unique identifiers (less preferred for interoperability).

4.4 Decentralised Identifier (DID)

Decentralised Identifiers (DIDs) are globally unique identifiers defined by W3C, designed for cryptographically verifiable, privacy-preserving identity data. A DID resolves to a DID document containing public keys, verification methods, and optional service endpoints. DID methods specify where/how that document is obtained.

DID:web is one such method that says: host the DID document at a predictable HTTPS URL under your domain. It's frequently highlighted in DPP/Digital Identity discussions as the "lightweight, non-DLT" option alongside methods based on distributed ledger technologies, such as DID:ethr and DID:ebsi. It combines the developments from Web3.0 with the robustness and scalability of Web2.0. For a deep dive in DID:web, please refer to 0.

5 Granularity levels

There is a separation into two dimensions of granularity. First is related to the production time, second is related to packaging

Production timing can be separated into

- General data, which is timing independent → Model
- several goods produced in a specific time range → Batch
- A single item produced to a specific time → Item

The second dimension is packaging; there is a split into

- Packaged goods
- Unpackaged goods

5.1 Model – Batch - Item

5.1.1 Model Level

The model level describes the product in a generic form – independent of any specific manufacturing instance or batch. It represents a master data view of the product.

Typical contents are, for example.

- Product name and category (e.g., epoxy resin type XY123)
- Chemical composition/formulation
- Hazard classifications and safety data
- Application areas
- Standards and certifications (e.g., REACH registration)
- Packaging specifications
- Environmental profiles based on standardized models (e.g., generic carbon footprint)

Use case

- Ideal for regulatory compliance, product development, sales, and marketing.

Frequency of data changes

- Relatively low

Required data volume

- Low to medium

5.1.2 Batch Level

The batch level relates to a specific production lot or batch produced under defined conditions within a certain time frame.

Typical contents

- Date and place of production
- Source of raw materials and suppliers (for that batch)
- Process parameters (e.g., reaction temperature, mixing time)
- Lab results and quality inspections
- Traceability of materials and precursors
- Batch-specific carbon footprint and energy use
- Events such as deviations or rework

Use case

- Essential for quality assurance, audits, traceability in case of complaints or recalls, and sustainability reporting.

Frequency of data changes

- Medium to high, depending on whether required with each batch

Required data volume

- Medium

5.1.3 Item Level

Serialized items are relevant for value chain communication irrespective of the similarity to supply chain operations. The item level pertains to a specific physical unit or uniquely identifiable article (e.g., container, drum, or packaging unit). It is less common in the chemical industry but relevant for high-value or safety-critical products. If a serialized item is not available or required, it can refer to a product, e.g., a packed unit (100g plastic box of a chemical). An item can have an external identifier, for example, a UPC or GTIN.

Typical contents

- Unique serial number or RFID tag
- Packaging unit (e.g., 1,000 L IBC container)
- Delivery and logistics data (e.g., transport temperature)
- Status information (e.g., opened, used, returned)
- Lifecycle data for reuse or recycling

Use case

- Relevant for logistics and inventory management of high-value and safety-critical products, specialized customer needs, or closed-loop systems.

Frequency of data changes

- (High) frequency

Required data volume

- High

5.1.4 Conclusion on the representation of different granularities

Considering Chem-X as a consolidated proposal for future standardization throughout B2B and B2C relationships in the chemical industry, the consortium creates a common foundation to balance individual party needs and manageable workflow complexity.

Chem-X proposes to work wherever possible on Model-Level and recommends drilling deeper into Batch- respectively Item-Level only on a non-avoidable exception basis.

5.2 Packed and Unpacked Goods

5.2.1 Packaged Goods

Packaged goods are chemical substances or mixtures that are contained in individual units or transport packaging, such as drums, canisters, IBCs (Intermediate Bulk Containers), or bags.

Examples:

- A 25 kg bag of sodium hydroxide pellets
- A 200-liter drum of solvent
- A 1,000-liter IBC container filled with polyurethane precursor

Typical Use Cases

- Distribution to end customers, easier handling and transport, storage in warehouses, and compliance with labelling and transport regulations.

5.2.2 Unpackaged Goods

Unpacked goods are chemicals that are transported or stored in bulk without discrete packaging units. Often moved via pipelines, tank trucks, rail tankers, or silos.

Examples

- Liquid methanol delivered via tank truck
- Bulk sulfuric acid stored in on-site tanks
- Powdered materials conveyed pneumatically into silos

Typical Use Cases

- Industrial-scale production inputs, on-site processing, and cost-efficient high-volume transport.

5.2.3 Conclusion on the level of packaged and unpackaged goods

Chem-X needs to deal with both scenarios: packed and unpacked goods. In the event of unpacked goods (materials), a digital product passport will focus on all required information based on the material only.

Considering packed goods/items, two majorly independent positions need to be consolidated into basically one (sales) item. For transparency reasons, Chem-X recommends treating both positions separately and handling them via two individual digital product passports. A separation of passports reduces complexity in data creation and maintenance and reduces the need for updates for the holistic (packed) good in case of a data correction on just one of the involved positions.

6 Format of the Material Identifier

The term material identifier represents an identifier of a DMP / DPP which can be issued on model, batch, or item level. The identifier can be formatted using different schemas as per prEN 18219:2025 [5]. This chapter compares different suggestions out of the Chem-X consortia.

6.1 Functional Comparison of DID:web vs. UUID as Material Identifier

Both technologies, DID:web, UUID, or even a combination of both can be used for material identification. So, the comparison of these different technologies makes only sense in the context of material identification and cannot be used as a standalone technology comparison.

Therefore, the following comparison aims to clarify the different functions both technologies can serve in future dataspace architectures, not as one-to-one comparison of existing technical standards.

6.1.1 Overview

Both technologies have distinct characteristics and use cases, serving different functions.

	DID:web	UUIDv4
Type	Decentralised digital identifier (W3CDID Method)	128-bit unique identifier(RFC 4122)
Purpose	Identity/authentication in decentralised and web systems	Object/resource unique identification
Example	DID:web:example.com:user:alice	550e8400-e29b- 41d4-a716-446655440000
Typical Use case	Identification of an entity, resolving a DID Document to provide access to additional services, cryptographic operations and data providers	Unique identification of data, entities, etc.

6.1.2 Authenticity and Verifiability

DID:web

- Each DID resolves to a DID document hosted on a specific web domain, containing cryptographic public keys and service endpoints.
- Enables verification of identity via public-key cryptography.
- Changes to identity data are traceable and managed by DID owners, not third parties

UUID

- No built-in support for authentication or cryptographic verification.
- Used solely for uniqueness; anyone with a UUID can assert ownership—there's no inherent proof.

6.1.3 Non-Repudiation

DID:web

- Signed transactions and interactions are possible, providing strong non-repudiation.
- Changes to identity (such as key rotation) can be traceable in public documents.

UUID

- Lacks auditability or non-repudiation features. If leaked or guessed, anyone can use it; no proof-of-origin.

6.1.4 Confidentiality and Privacy

DID:web

- Can expose minimal info via its public DID document, but keys (rather than personal data) are public.
- Privacy depends on the hosting/management of the DID document and key practices.
- Not suitable for storing confidential data directly—only for referencing or authenticating entities.

UUID

- Versions like UUIDv1 can reveal timestamp and MAC address (potentially privacy-leaking).
- Version 4 (random) offers better privacy but is still just a random, static identifier.

6.1.5 Resistance to Guessing/Enumeration

DID:web

- Identifiers are as strong as the web endpoints and DNS naming (e.g. DID:web:company.com:resource). Security relies on domain management and HTTPS
- If enumeration is possible on a hosting server, sensitive associations could be listed.

UUID

- Random UUIDv4 is highly resistant to guessing; probability of collision or prediction is negligible.
- Older or deterministic versions (like UUIDv) can be more predictable and less secure.

6.1.6 Authorization Use

DID: web

- Designed for authentication, federated trust, and (optionally) decentralised attestation scenarios.
- Used in protocols that check cryptographic proof using keys from the DID document.

UUID

- Never rely on UUIDs for authorization or access control alone.
- Attackers can simply guess or enumerate valid UUIDs if no cryptographic authentication is required.

6.1.7 Key Management

DID:web depends on the secure management of private keys, while UUIDs require no key material.

6.1.8 Revocation

DID:web allows revoking or rotating keys via document updates; UUIDs can’t be “revoked,” only made obsolete with system rules.

6.1.9 Decentralisation

DID:web is built on the Decentralised Identifier (DID) framework, which aims to reduce reliance on a central authority for identifier creation and management. However, the DID:web method specifically stores DID documents on web servers under domain names and therefore still depends on centralised infrastructure, namely DNS and web hosting. This means its decentralisation is limited compared to DID methods based on blockchain or fully peer-to-peer networks.

A UUID (Universally Unique Identifier) is not inherently decentralised or centralised—it is a 128-bit value generated locally by any system that follows the standard, with no coordination or registration required. While UUIDs are unique and can be generated independently, they offer no features to manage or resolve the identifier beyond the creating system. There is no decentralised or centralised control mechanism; UUIDs are static and stand-alone.

6.1.10 Control

DID:web gives control to the entity managing the domain: whoever owns and operates the relevant web domain can create, update, and revoke DID documents and the cryptographic keys within. This allows entities to control their digital identifiers and manage credential rotation or revocation, but that control is reliant on the continued ownership and security of the DNS domain and web server. Ultimate control lies with the domain administrator; if the domain registration is lost or compromised, so is control over the associated DID:web identifiers.

Manufacturer has control over details of identifier online / at runtime

NO OTHER scheme can offer this level of control COMBINED with shared schemas AND SEMANTIC INTEROPERABILITY with all other schemas mentioned in chapter 4.

UUID offers no ongoing control—once generated, a UUID cannot be updated, revoked, or managed. Control is limited to the act of creation; anyone can generate a UUID, but there is no built-in way to prove or transfer ownership, nor to coordinate updates or revocations. There is also no mechanism for cryptographic proof of control.

6.1.11 When to Use: Functional Purpose

DID:web offers:

- Verifiable, decentralised identity is crucial.
- Cryptographic proof-of-control and cross-domain trust needed.
- Compliance with W3C/DID standards is required for interoperability or self-sovereign identity.

UUID offers:

- Only uniqueness (not security or identity) is required.
- Simplicity, distributed generation, and scale are critical and identities are not externally exposed.

6.1.12 Summary of functional comparison

Criteria	**DID:web**	**UUID**
Uniqueness	Web domain-based, globally unique	Practically unique (esp. v4)
Verifiability	Public-key cryptography, DIDdocument	Not verifiable, static only
Non-repudiation	Strong (cryptographic signatures)	None
Authorization/Proof	Yes (cryptographic), not just obscurity	No (do not use for access control)
Privacy risks	Minimal with best practice	v1 exposes time & MAC; v4 is private
Management Complexity	Higher (key storage, doc hosting)	Lower (no infra/key management)
Revocability	Yes (update doc or keys)	No

Decentralisation	Limited—depends on DNS and web servers (centralised infrastructure)	Not decentralised or centralised; locally generated
Control	Domain owner controls, can update & revoke via DID document	Only creation control; static, immutable, no management

All things considered, DID:web offers substantial IT security, with built-in cryptographic authentication, identity proofs, and interoperability for decentralised digital identity. It should be considered wherever digital identity or verifiable identity control is required, as DID:web provides security, trust, and auditability at scale.

UUID on its own serves function for ensuring uniqueness at scale, not for security or authentication. Therefore, it should not be used as a substitute for access control or cryptographic identity verification. Typically, requirements met by UUID are the need for simple, non-security-critical identifiers.

6.2 DID:web method specific identifier

A DID consists of 3 parts,

1. the did URI scheme identifier, (did)
2. the identifier for the DID method (web)
3. the DID method-specific identifier.

The third part is split up into company- and material identifier.

A resolver, like the Universal-Resolver will use the method specific identifier to fetch the DID Document from this location.

Example:

```
DID:web:company.org:1234567890
```

will be resolved to a DID Document, which must be available at:

```
https://company.com:1234567890https://company.org/1234567890/did.jso
n
```

6.2.1 Material DID vs Business Partner based DID

Chem-X offers a central Business Partner identifier service, which provides a DID:web for a business partner. Instead of issuing an own DID for every material identifier, this DID can be used as a base for a Material DID by adding the material identification as suffix. A material would reuse the Key Material of the Business Partner DID.

The downside of this approach is a centralised DMP/DPP resolver as the did document would be associated with a centrally provided Business Partner DID.

Example Material DID based on Business Partner DID of Cofinity-X

```
DID:web:portal-backend.beta.cofinity-
x.com:api:administration:staticdata:DID:BPNL0000000ZZZZZ:MATERI
AL-IDENTIFIER
```

The example mentioned above requires the resolving of the DID document:

```
https://portal-backend.beta.cofinity-
x.com/api/administration/staticdata/did/BPNL0000000ZZZZ/
MATERIAL-IDENTIFIER /did.json.
```

This can be resolved by providing either a centralised registry or proxy component which forwards the request to the corresponding local economic operator service.

The issuing of an own Material DID would allow the economic operator to provide there own services following the w3c standard.

6.2.2 GLN vs Domain Name as DID:web company identifier

In Chem-X a company is identified by the Business Partner Number which can reference the GLN.

As a resolver will use the company identifier in an URL to resolve the DID Document, the GLN cannot be used. So the company domain must be used.

6.2.3 UUID vs HASH as DID:web material identifier

The material identifier of a DID:web:companyIdentifier:materialIdentifier can be formatted in different ways, like UUID, Hash, or a salted Hash.

The following table will compare the three options with each other.

	UUIDv4	Hash	Salted Hash
example	DID:web:company.org:be2b4e24-dcdb-4e80-a157-fd93df892a3e	DID:web:company.org:747d945963e24986e2c75a05898d502c78510635c8ceb0e7cf36e4b4	DID:web:company.org:3c6678a668c5195cb6623098ace361d024835f8aadc8f7f9fd1f2d8c
Online/Offline	Online	Offline / Online	Online
predictable	no	yes	no
lengths	32 digits	Depends on algorithm	Depends on algorithm
Verifiable structure	Yes	Length only	Length only
Authentication / validity check	Online	Offline	Online
Collision resistant	Depends on algorithm	Depends on algorithm	Depends on algorithm

The UUID is the preferred way for material identification. It is easy to calculate provides a high collision resistance. Hashes can be used in a case of an offline number verification.

7 Conclusion

This report is based on a discussion of design choices based on four major requirements:

1. Compatible with existing and future standards or regulations
2. Using existing technology
3. Serving the functional demands of the chemical industry with its unique role at the centre of multiple manufacturing value chains
4. Assigning a maximum of control over material identifiers to the manufacturer itself.

While there are more established material identifier schemas than DID:web for other industrial applications – at least outside the chemical industry - we propose that the key advantage of DID: web-based designs is the high level of control a manufacturer receives over details of the identifier at publication and during deployment. In addition, the design supports semantic interoperability by integrating other identifiers into the DID document, addressing the unique challenge of the chemical industry at the centre of so many manufacturing value chains.

A DID:web based material identifier can use a UUIDv4 as identifier. The UUID is managed locally by the economic operator or a DPP provider. A Hash based identifier should be used primarily in offline scenarios, as it has the risk of predictable identifier. The combination of the company identifier, the local material identifier, and a salt would provide a secure basis for a unique hash. A unique identifier can be used as basis to generate a cryptographic key.

The attributes of the proposed material identifier laid out in 3.1. are summarised in Figure 2

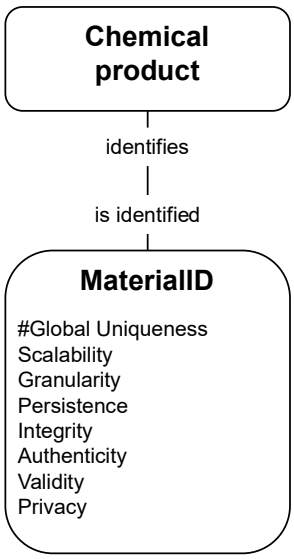

Figure 2 MaterialID and its attributes

8 Glossary

Term	Definition	Note to source
CAS Number	CAS (Chemical Abstracts Service) Number. A globally recognized numeric identifier for chemical substances	
Chemical products	a manufactured good whose principal functional or structural components are one or more chemical substances, mixtures, or REACH articles produced, transformed, or combined through chemical processes. Synonyms are chemicals, materials, (un)packaged goods	Chem-X Material Declaration Guideline
CRM	A Customer Relation Management System, short CRM, is a ICT system to manage and structure the business relationship and interaction with the customers of an economic operator.	
CRUD	Create, Read, Update, Delete action done on dedicated	
Digital Material Passport (DMP)	A structured digital record that contains detailed information about – and not limited to - a product's lifecycle, materials, components, and sustainability attributes. It focuses on intermediate materials which may not be subject to regulation, but whose data are required to enable the issue of regulated Digital Product Passports (DPPs). DMPs are designed to interoperate with one or more DPPs.	Chem-X Sustainability Guideline
Digital Product Passport (DPP)	A structured digital record that contains detailed information about a product's lifecycle, materials, components, and sustainability attributes. It focuses on a regulated final product in the value chain. Both its information content and technical requirements follow regulatory requirements and/or standards delegated by the legislator to designated standardization bodies.	Chem-X Sustainability Guideline
DUNS	Data Universal Numbering Systems by Dun & Bradstreet to identify global business entity or organization	
Economic Actors	An economic actor is any organization or individual that performs a commercial, regulatory, or operational function within the lifecycle of a physical product.	
ECHA	European Chemical Agency	ECHA
EC Number	Identifier assigned by the European Commission (EC) to substances for regulatory purposes. The EC Inventory comprises three individual inventories, EINECS, ELINCS and the NLP	ECHA
EDC	Eclipse Dataspace Connector	
EDI	Electronic data interchange protocol is a set of standards to enable automated machine to machine information exchange between legal entities, e.g. purchase orders, invoices, shipping notices, etc.	
EINECS	European Inventory of Existing Commercial chemical Substances	ECHA
ELINCS	European List of Notified Chemical Substances	ECHA
ERP	Enterprise Resource Planning is an ICT system helping organizations streamline their core business processes such as order to cash (OTC) or purchase to pay (PTP)	
GTIN	Global Trade Item Number issued by GS1. It is a set of specifications and a standard family ISO/IEC 15495	
GLN	Global Location Number is an identifier for a location or an entity in a business network issued by GS1	

Term	Definition	Note to source
IDSA	International Dataspace Association	
INCI Name	International Nomenclature Cosmetic Ingredient Name – international identifier for cosmetic ingredients	
IRDI	The international registration data identifier (IRDI) is an internationally unique identifier for a data element used, e.g. in the IEC common data dictionary (CCD).	
IRI	Internationalized Resource Identifier	
LEI	Is a Legal Entity Identifier issued by the Global Local Entity Identifier Foundation (GLEIF) under the direction of the G20 and the Financial Stability Board (FSB)	
NLP	No-Longer Polymers	ECHA
PIM	Product Information Management	
REACH	REACH stands for Registration, Evaluation, Authorization and Restriction of Chemicals	ECHA
SDS	Safety Data Sheet. Regulatory required document [] [] to ensure save handling, use, storage and disposal of chemical products	
Supply chain communication	The “logistics” side – moving goods, money, and information from supplier to customer. Typically handled by electronic formats such as EDI (electronic data interchange)	-
UFI Number	Unified formula identifier required for the notification of a hazardous mixture at a national poison center	ECHA
UPC	Universal product code issued by GS1. Part of the GTIN specification	
URI	Uniform Resource Identifier a unique sequence of characters that identifies an abstract or physical resource such as a webpage, e-mail-address, etc.	
URL	Uniform Resource Locators as defined in RFC 1738	
URN	Uniform Resource Name is a URI that uses the URN scheme.	
UUID	Universally Unique Identifier is 128-bit number identifier normally generated by random numbers	
Value chain communication	The “businessvalue” side – creating and delivering value to the endcustomer. Essentially delivering product information such as quality or technical information, sustainability information, etc.	

9 Bibliography

[1] A. Gambarin and H. Galloway, "The Global Chemical Industry: Catalyzing Growth and Addressing Our World's Sustainability Challenges," The International Council of Chemical Associations (ICCA), 2019.

[2] J. Potting, M. Hekkert, E. Worrell and A. Hanamaaijer, "Circular Economy: Measuring Innovation in The Product Chain," PBL Netherlands Environmental Assessment Agency, The Hague, 2017.

[3] *Regulation (EC) No 1272/2008 of the European Parliament and of the Council of 16 December 2008 on Classification, Labelling and Packaging (CLP) of Substances and Mixtures,* Official Jounal of the European Union, 2008.

[4] Globally Harmonized System of Classification and Labelling of Chemicals (GHS), New York and Geneva: United Nations, 2023.

[5] *Regulation (EC) No 1907/2006 of the Europan Parliament and the Council of 18 December 2006 concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH),* Official Jounal of the European Union, 2006.

[6] A. Osborne, D. Buckley and H. Barthel, "GS1 Architectural Principles," GS1, June 2022. [Online]. Available: https://ref.gs1.org/architecture/principles/. [Accessed 6 November 2025].

[7] *Regulation (EU) 2024/1781 of the European Parliament and the Council of 13 June 2024 establishing a framework for setting of ecodesign requirements for sustainable products,* Official Jounal of the European Union, 2024.

[8] *prEN 18219:2025 Digital product passport - Unique identifiers,* DIN, 2025.

[9] C. Diedrich, "Asset Administration Shell," 17 January 2024. [Online]. Available: https://www.i40.ovgu.de/i40/en/Asset+Administration+Shell.htm. [Accessed 10 November 2025].

[10] J. Neidig, A. Orzelski and S. Pollmeier, "Asset Administration Shell Reading Guide," Industrie 4.0, Berlin, 2022.

[11] M. Benndorff, Asset Administration Shell – Industry 4.0's Standard for Connected Assets, [Online]. Available: https://soffico.de/en/use-cases/asset-administration-shell.

[12] F. Schloz, "How the Asset Administration Shell Is Shaping the Future of Digital Twins," 08 Mai 2024. [Online]. Available: https://www.mhp.com/en/insights/blog/post/asset-administration-shell. [Accessed 10 November 2025].

[13] "Decentralized Identifiers (DIDs)," W3C, [Online]. Available: https://w3c.github.io/did/. [Accessed 27 October 2025].

[14] M. Sporny, D. Longley, M. Sabadello, D. Reed, O. Steele and C. Allen, "Decentralized Identifiers (DIDs) v1.0," 19 July 2022. [Online]. Available: https://www.w3.org/TR/did-1.0/. [Accessed 27 October 2025].

[15] "DIF Universal Resolver," [Online]. Available: https://dev.uniresolver.io/. [Accessed 27 October 2025].

[16] K. Hamilton-Duffy, R. Grant and A. Gropper, "Use Cases and Requirements for Decentralized Identifiers," W3C, 17 March 2021. [Online]. Available: https://www.w3.org/TR/did-use-cases/. [Accessed 27 October 2025].

[17] "Decentralized Identifiers (DIDs) v1.0," 19 July 2022. [Online]. Available: https://www.w3.org/TR/did-1.0/#did-resolution. [Accessed 27 October 2025].

[18] "did:web Method Specification," W3C, 31 July 2024. [Online]. Available: https://w3c-ccg.github.io/did-method-web/. [Accessed 2025 October 2025].

[19] M. Sporny, D. Longley, D. Chadwick and I. Herman, "Verifiable Credentials Data Model v2.0," W3C, 15 May 2025. [Online]. Available: https://www.w3.org/TR/vc-data-model-2.0/. [Accessed 27 October 2025].

[20] "Asset Administration Shell," 17 June 2024. [Online]. Available: https://de.wikipedia.org/wiki/Asset_Administration_Shell. [Accessed 10 November 2025].

Annex: Decentralised Identifiers (DIDs) Deep Dive

DID stands for Decentralised Identifier and is a W3C Standard . The Abstract defines the functionality, design, and scope: "Decentralized identifiers (DIDs) are a new type of identifier that enables verifiable, decentralised digital identity. A DID refers to any subject (e.g., a person, organisation, thing, data model, abstract entity, etc.) as determined by the controller of the DID. In contrast to typical, federated identifiers, DIDs have been designed so that they may be decoupled from centralised registries, identity providers, and certificate authorities. Specifically, while other parties might be used to help enable the discovery of information related to a DID, the design enables the controller of a DID to prove control over it without requiring permission from any other party. DIDs are URIs that associate a DID subject with a DID document, allowing trustable interactions associated with that subject. Each DID document can express cryptographic material, verification methods, or services, which provide a set of mechanisms enabling a DID controller to prove control of the DID. Services enable trusted interactions associated with the DID subject. A DID might provide the means to return the DID subject itself, if the DID subject is an information resource such as a data model. This document specifies the DID syntax, a common data model, core properties, serialised representations, DID operations, and an explanation of the process of resolving DIDs to the resources that they represent." The DID basic representation is shown in Figure A1: 3 and the basic overview of its architecture in Figure A2: 4.

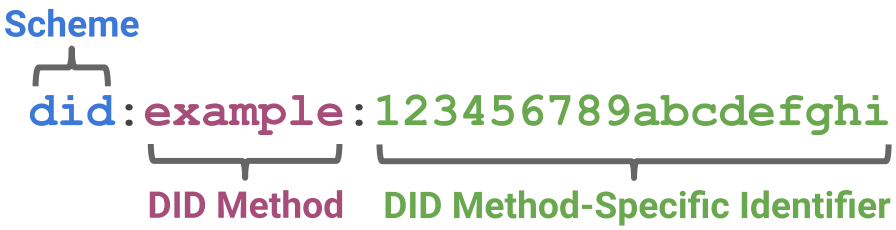

Figure A1: 3A DID consists of a schema, a method, and an identifier, separated by columns

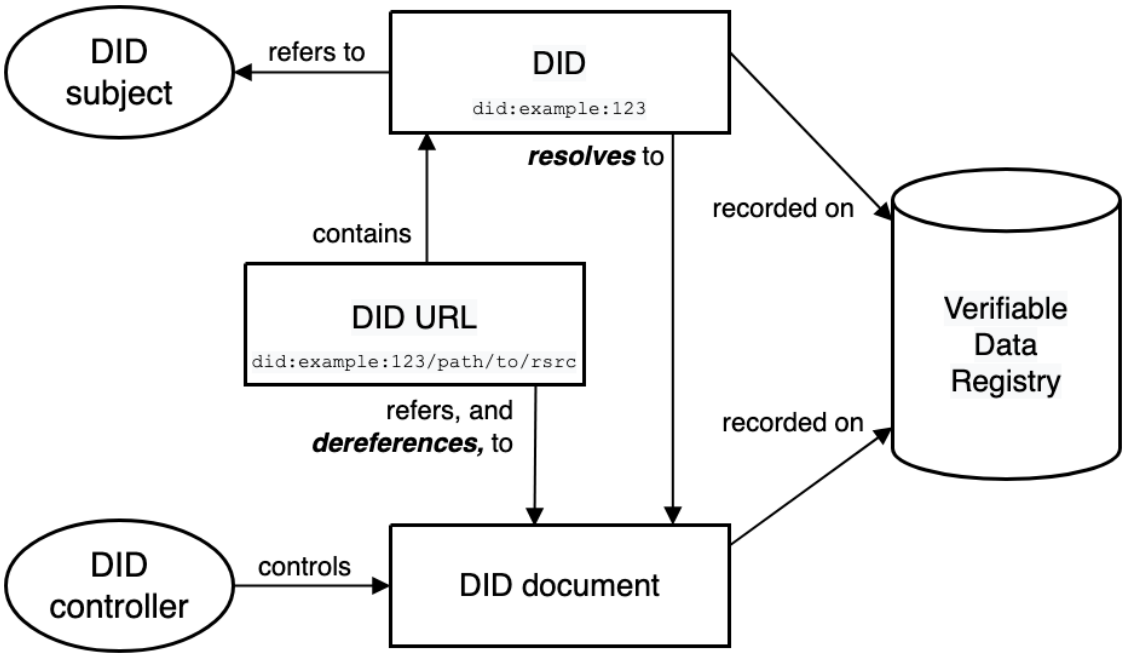

Figure A2: 4 Basic overview of the DID architecture

A.1 DID Controller

The W3C standard defines a DID controller as an entity that is authorized to change the content of a DID Document. Typically, the DID Controller is mentioned as a controller entity on the DID document itself, but it is an optional property. The DID method determines the authorization process of a DID Controller. It is possible to delegate the control or share the responsibility of a DID Document to/with a 3rd party. W3C documentation describes the DID Controller as "An entity that has the capability to make changes to a DID document. A DID might have more than one DID controller. The DID controller(s) can be denoted by the optional controller property at the top level of the DID document. Note that a DID controller might be the DID subject."

A.2 DID Subject

The subject of a DID is the entity associated with the DID, so in other words, a DID Subject is the entity identified by a DID and described by a DID document. Anything can be a DID subject: person, group, organization, physical thing, digital thing, logical thing, etc. A DID subject can have multiple identifiers for different purposes, or at different times. The assertion that two or more DIDs (or other types of URI) refer to the same DID subject can be made using the alsoKnownAs property.

A.3 AlsoKnownAs

A DID subject can have multiple identifiers for different purposes, or at different times. The assertion that two or more DIDs (or other types of URI) refer to the same DID subject can be made using the alsoKnownAs property. This property is optional, but if available of type URI.

A.4 DID - Method

A definition of how a specific DID method scheme is implemented. A DID method is defined by a DID method specification, which specifies the precise operations by which DIDs and DID documents are created, resolved, updated, and deactivated. It also documents all implementation considerations related to DIDs as well as Security and Privacy Considerations.

Chapter 8 of the DID standard describes a DID Method as a definition of how implementers can realize the features described by this specification. DID methods are often associated with a particular verifiable data registry. New DID methods are defined in their own specifications to enable interoperability between different implementations of the same DID method.

- DID:key
- DID:web
- ledger-based
- comparison DID Methods

A.5 DID scheme

The formal syntax of a decentralised identifier. The generic DID scheme begins with the prefix DID: as defined in DID Syntax. Each DID method specification defines a specific DID method scheme that works with that specific DID method. In a specific DID method scheme, the DID method name follows the first colon and terminates with the second colon, e.g., DID:example:, DID:web, DID:web:managed-identity-wallet.preprod.cofinity-x.com:BPNL000005551C9G. Note that the path is an optional parameter that resolves to a path on the web-domain where the did.jason document is expected to be returned.

The ABNF Rules of a DID are:

did = "DID:" method-name ":" method-specific-id method-name = 1*method-char method-char = %x61-7A / DIGIT method-specific-id =(*idchar ":") 1*idchar idchar = ALPHA / DIGIT / "." / "-" / "_" / pct-encoded pct-encoded = "%" HEXDIG HEXDIG

A.6 DID Document

The DID Document contains information associated with the entity (the object), which is identified by the DID. Typically, the expressed information can be associated to verification methods or services. Additionally, a generic section is foreseen in the DID Document.

Services determine how to interact with the DID Subject, as verification methods typically provide cryptographic public keys to be used for verification.

DID Document properties

Property	**Required?**	**Value constraints**
id	yes	A string that conforms to the rules of the DID Syntax.
alsoKnownAs	no	A set of strings that conform to the rules of RFC3986 for URIs.
controller	no	A string or a set of strings that conform to the rules of the DID Syntax.

Property	Required?	Value constraints
verificationMethod	no	A set of Verification Method maps that conform to the rules in Verification Method properties, such as cryptographic public keys, which can be used to authenticate or authorize interactions with the DID subject or associated parties.
authentication	no	expression of the relationship between the DID subject and a verification method for this relation. An example of a verification relationship is authentication with a verification method cryptographic public keys.
assertionMethod	no	
keyAgreement	no	
capabilityInvocation	no	
capabilityDelegation	no	
service	no	A set of Service Endpoint maps that conform to the rules in Service properties.

A.7 Verification Method

A set of parameters that can be used together with a process to independently verify a proof. For example, a cryptographic public key can be used as a verification method with respect to a digital signature; in such usage, it verifies that the signer possessed the associated cryptographic private key.

"Verification" and "proof" in this definition are intended to apply broadly. For example, a cryptographic public key might be used during Diffie-Hellman key exchange to negotiate a shared symmetric key for encryption (keyAgreement). This guarantees the integrity of the key agreement process. It is thus another type of verification method, even though descriptions of the process might not use the words "verification" or "proof."

A.8 Properties

Property	Required?	Value constraints
id	yes	A string that conforms to the rules of the DID URL Syntax.
controller	yes	A string that conforms to the rules of the DID Syntax.
type	yes	A string.
publicKeyJwk	no	A map representing a JSON Web Key that conforms to [RFC7517]. See definition of publicKeyJwk for additional constraints.
publicKeyMultibase	no	A string that conforms to a [MULTIBASE] encoded public key.

When a controller property (see) is present in a DID document, its value expresses one or more DIDs. Any verification methods contained in the DID documents for those DIDs should be accepted as authoritative, such that proofs that satisfy those verification methods are to be considered equivalent to proofs provided by the DID subject.

The DID controller has its own DID that is different from the DPP/DMP identifier. It implies that we use verification methods and relationships.

A.9 DID Service endpoints

Means of communicating or interacting with the DID subject or associated entities via one or more service endpoints. Examples include discovery services, agent services, social networking services, file storage services, and verifiable credential repository services. To summarize, a service is a service endpoint network address, such as an HTTP URL, at which services operate on behalf of a DID subject.

Endpoint Properties

Property	Required?	Value constraints
id	yes	A string that conforms to the rules of [RFC3986] for URIs.
type	yes	A string or a set of strings.
serviceEndpoint	yes	A string that conforms to the rules of [RFC3986] for URIs, a map, or a set composed of a one or more strings that conform to the rules of [RFC3986] for URIs and/or maps.

A.10 DID References

The DID standard does not foresee a direct property to reference another DID document.

The “alsoKnownAs” property should lead to a set of URIs as stated by the W3C Standard , therefore it might be used to build a relationship between DID. This functionality can also be realized using the service section, either via direct usage or indirect as part of the result of a custom service (e.g. DPP).

Option1:

Utilize the optional DID property “alsoKnownAs” to refer to the same subjectID (i.e. MaterialID) from another EOP, who creates it’s own DID. That implies we must have DID methods, that support DID Documents (basically all methods beyond DID:key). Those references in DID documents would be publicly visible, as the DID should be publicly resolvable and a resolver returns the same DID document regardless of who is asking.

Option2:

Services in the DID document could be for example a presentation service for credentials (that are identified by a DID) such as a DPP or DMP. Services presenting DMP/DPP credentials can be seen as protected resource, thus requiring authorization of the requestor (think of Oauth2) in order to get access to confidential parts of the DMP. Sensitive information would then only be presented (or selectively disclosed) to authorized requestors.
References to DIDs from other EOPs or the other DMPs of the same EOP would then be part of the Credential payload and could also be fields relevant to selective disclosure.

A.11 DID resolution / DID resolver

The process that takes as its input a DID and a set of resolution options and returns a DID document in a conforming representation plus additional metadata. This process relies on the "Read" operation of the applicable DID method. The inputs and outputs of this process are defined by the W3C as follows

- resolve: the resolve function accept the DID and resolution options as input and return the DID Document as key-value pairs (a map) in a representation that conforms to the VC data model and is serialized with on of the media-types application/did+json; application/did+cbor or application/did+ld+json
- resolveRepresentation: the resolvePresentation function has the same input as the resolve function, accepting a DID and resolution options, but the return value is a byte stream of the DID Document formatted in the corresponding representation.

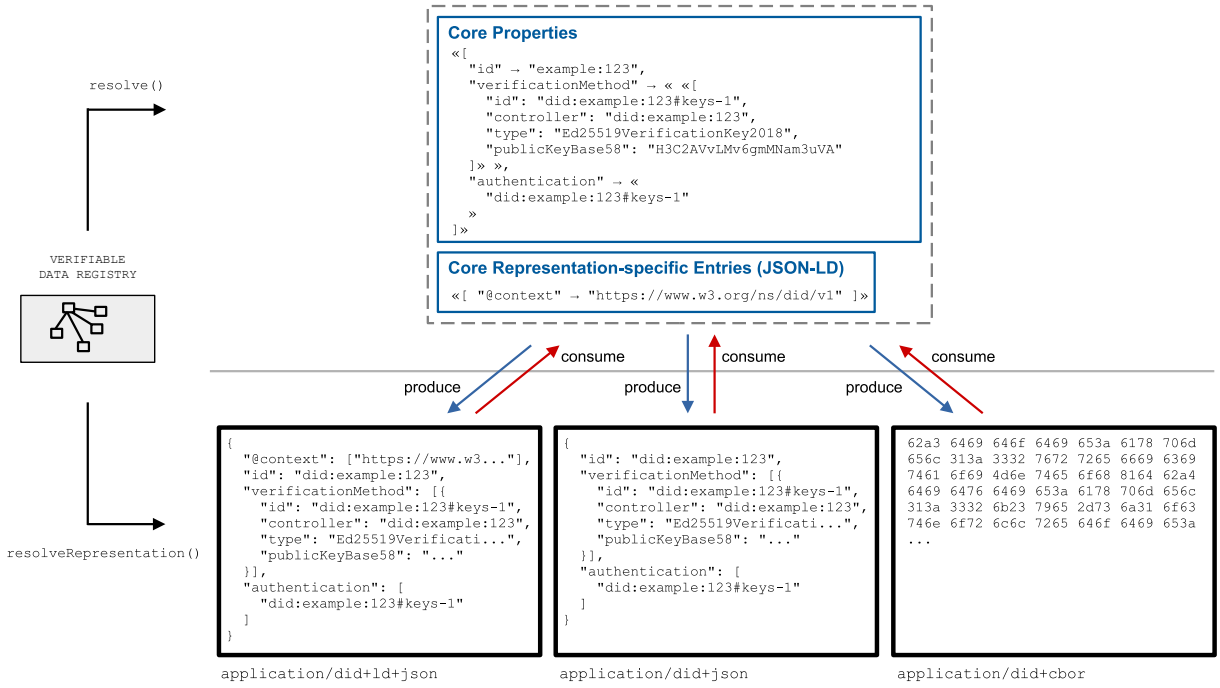

Figure A3: 5 DID resolution

The resolution of a DID is performed by the resolver, which is a software and/or hardware component. The resolver accepts the DID as input and produces a conforming DID document as output. An example is the universal resolver.

A.12 Representation

A concrete serialization of a DID document in this specification is called a representation. A representation is created by serializing the data model through a process called production. A representation is transformed into the data model through a process called consumption. The production and consumption processes enable the conversion of information from one representation to another. This specification defines representations for JSON and JSON-LD, and developers can use any other representation, such as XML or YAML, that can express the data

model. The following sections define the general rules for production and consumption, as well as the JSON and JSON-LD representations.

A.13 Requirements on Identifier

The DID Use Cases Document by Kim Hamilton-Duffy, Ryan Grant, and Adrian Gropper defines 4 characteristics an identifier has to meet:

1. **decentralised**: there should be no central issuing agency;
2. **persistent**: the identifier should be inherently persistent, not requiring the continued operation of an underling organization;
3. **cryptographically verifiable**: it should be possible to prove control of the identifier cryptographically.
4. **resolvable**: it should be possible to discover metadata about the identifier.

A.14 Material-ID resolve DID Subject

Catena-X is using an UUID as identifier for the DPP, in comparison the unique identifier of the DPP for Chem-X is the DID of the entity, which will be generated from a combination of the company identifier, the subject (identifier of the entity, e.g. GTIN, Material-ID) and a salt. This combination will be hashed and can be used for a cryptographic key generation.

A custom resolver accepts the material identifier (material number in combination with a company identifier), GTIN, or another serial number and derives the DID from it. The resolver would allow authenticated resolving of the DID document, already verifying the granted access level of the requester.

The yellow-pages function of the resolver needs to be part of the platform provider.

A.15 Accessibility

The accessibility of the DID Document is defined by the DID method, based on Chapter 8 of the DID Standard DID Definition Document. Next to the definition of the requirement on a DID method syntax, although the specification of the requirements of the DID method operations are part of this chapter.

A DID method must specify how the authentication happens and how CRUD operations are protected. The resolution of a DID Document is a read access and can be already restricted based on the definition of the method.

The specification of DID:web is published as an unofficial draft version at W3C and leaves the implementation of authorization and authentication mechanism and procedures to the implementer.

This would allow an authenticated and authorized resolution of a DID Document in addition to authenticated and authorized access to services like a DPP.

The DID standard allows public and private resolution as well as access to sections of a public DID document.

A.16 Verifiable Credentials

VC is a W3C standard, available in Version 2 . The Chem-X Verification Workstream explains Verifiable Credentials in its Report.