Chem-X Consortium

The Verification Guideline

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

Document information

Project Title	Establishment of a data room for the chemical industry as well as interfaces of the associated value chains using the example of the digital product passport
Project Acronym	CHEM-X
Project Coordinator	Dr. Andreas Wollny
Related Work Package	TP2.WP3
Related Task(s)	E1: Results of the review of existing digital verification components such as Catena-X, TfS, Energy Data-X in the direction of interoperable digital verification mechanisms beyond automotive including the conformity and governance model
Lead Organisation	Spherity
Contributing Partner(s)	BASF, Cofinity-X, Coverstro, Henkel, Merck, SAP, Wacker
Authors	Doruk Sahinel, Martin Westerkamp, Ricky Thiermann, Ingo Wolf, Vikas Mishrikoti, Steffen König, Henning Schwabe, Oliver Mössner

History

Date	Version	Submitted by	Reviewed by	Comments
10.11.2025	0.9	Dr. Doruk Sahinel		

Participating partners

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

Table of Contents

List of Figures

List of Tables

Summary

This document provides a review of existing dataspace projects regarding their verification components and serves as a foundation for developing a verification concept in Chem-X project. It highlights the importance of credential-based verification, public key infrastructure, and registry services within a decentralized framework, referencing standards such as eIDAS, W3C Verifiable Credentials, and active and ongoing dataspace projects like Catena-X.

The chapters of the deliverable are organized as follows: Chapter 1 introduces the objectives and scope of the Chem-X verification framework. Chapter 2 defines foundational concepts such as Self-Sovereign Identity (SSI), conformity assessment procedures, and semantic verification, which form the basis of the trust mechanisms discussed throughout the document. Chapter 3 presents an overview of technical verification components, including clearing house functionalities and reusable or extensible components from Catena-X, other dataspace initiatives, and relevant projects. Chapter 4 focuses on verifiable credentials, distinguishing between business and material identity credentials that are to be used in Chem-X verification framework and Chapter 5 outlines the key verification processes required for Chem-X dataspace. The document concludes with recommendations in Chapter 6 and final reflections in Chapter 7.

Keywords

Catena-X, Certificate Validation, Clearing House, Conformity Assessment, Digital Product Passport, Self-Sovereign Identity, Together for Sustainability, Trust Frameworks, Verifiable Credentials

Abbreviations and Acronyms

AAS	Asset Administration Shell
BPN	Business Partner Number
CAB	Conformity Assessment Body
CBAM	Carbon Border Adjustment Mechanism
DID	Decentralized Identifier
DOI	Digital Object Identifier
DPP	Digital Product Passport
DSSC	Data Space Support Centre
eIDAS	Electronic Identification, Authentication and Trust Services
ESPR	Ecodesign for Sustainable Products Regulation
GS1	Global Standards One
GTIN	Global Trade Item Number
GXDCH	Gaia-X Digital Clearing House
IDSA	International Data Spaces Association
IRDI	International Registration Data Identifier
IRI	Internationalized Resource Identifier
ISO	International Standards Organization
PACT	Partnership for Carbon Transparency
PCF	Product Carbon Footprint
qTSP	Qualified Trust Service Provider
SAMM	Semantic Aspect Meta Model
SSI	Self-Sovereign Identity
TfS	Together for Sustainability
UNTP	UN Traceability Protocol
VAT	Value Added Tax
VC	Verifiable Credentials
VDR	Verifiable Data Registry
W3C	World Wide Web Consortium

1. Introduction

Customers, investors, and regulators rely on product and sustainability information to make informed decisions about sustainability and climate action. For example, ESPR [1] mandates that requirements towards and components of the future Digital Product Passport (such as unique identifiers and data carriers, i.e., QR codes, etc.) shall be verifiable (albeit subject to further standards and delegated acts). Non-compliance can lead to severe consequences, including penalties and reputational damage, if supplier sustainability claims or disclosures are found to be untrue or misleading.

To mitigate these risks, buyers desire tools and methods to verify the sustainability disclosures made by their suppliers. Without trust in the reported sustainability data, stakeholders may be skeptical of the claims made by companies and may question the effectiveness of their sustainability efforts. Therefore, verifiability of product and sustainability information will support businesses in improving the efficiency and trustworthiness of reporting and due diligence processes. For downstream customer industries, this may lead to more frequent and better-informed decisions, thanks to higher comparability and transparency of products and economic actors.

Verifiability is essential for providing auditable evidence of trustworthy assessments that substantiate claims and disclosures regarding product and sustainability information. It also enables the verification of relevant identities, such as product types, place of origin, specific facilities, and business entities. Furthermore, cryptographic verification of digital proofs such as identities and certificates is a prerequisite for enabling the automation of trustworthy data transfer. Data sharing along supply chains is facilitated through interoperable ecosystems such as data spaces, enabled by common data models and data exchange formats. Hence, it can be stated that verification is a foundational concept to realize a trust framework in dataspaces.

In the context of dataspaces, the foundational concepts of Self-Sovereign Identity (SSI), conformity assessment, and semantic verification have been identified as critical building blocks for enabling verification processes. SSI provides a decentralized identity management paradigm in which credentials are issued, held, and presented by economic actors without reliance on centralized intermediaries. Conformity assessment frameworks contribute structured assurance by establishing procedures for evaluating compliance, while semantic verification ensures that the meaning of shared data remains consistent across systems. Together, these concepts lay the groundwork for verification in Chem-X.

With the aim of generating a verification concept for Chem-X, a range of technical verification components has been reviewed from existing literature and dataspace architectures. These include credential schemas, issuer and verifier registries, trust anchors, status and revocation services, and presentation protocols, among others. In addition, verifiable credentials (VCs) are a central mechanism for verification in dataspaces, as they enable the secure transmission of attestations across dataspace actors. To ensure that such components operate effectively, verification processes within dataspaces are defined briefly. These brief definitions will be extended inside the Chem-X verification concept with concrete examples from the chemical industry. Finally, a set of practical recommendations has been derived for Chem-X to address

current gaps in existing dataspace projects and the requirements of the chemical industry, based on this review of core concepts and verification components.

2. Foundational Concepts

From the perspective of technological optimism, a future seems inevitable where autonomous software agents exchange product data between companies automatically. In such a scenario of highly advanced supply chain automation, the verification on the level of single data points becomes an essential feature[1]. However, the journey towards this future will have to start from more humble beginnings. What can serve as a solid starting point for this work package is the fact that regulatory compliance as well as sustainability performance are increasingly determined by the whole supply chain (as opposed to single actors).

Today, manual / analog certification[2] schemes are firmly established in the supply chains of the chemical industry, among others for due diligence during onboarding of new suppliers and customers, reporting of characteristics of biomass as raw material, and certification of chain of custody calculation schemes of manufacturing companies. The essential work processes supported by these types of certifications can be summarized on a high level as:

1. **Compliance:** regarding legal and regulatory requirements
2. **Collection and reporting of evidence** in support of product **claims** subject to quantitative and qualitative conformity assessment criteria[3].
3. **Risk Monitoring**: Pro-active, forward-looking monitoring of supply chain risks in support of planning processes on the customer side.

Since these work processes are labor intensive there is a substantial economic incentive along the supply chain to seek improved solutions that enable a step-by-step approach to automation of these processes. Requirements and risks referenced above can fall into at least two categories:

- **Company**-level data
- **Product**-level data

In addition, various requirements may also demand site-level or even plant-level certifications. It is important to highlight the fact that all factors referenced so far are highly context-specific, as they depend, for example, on the regulatory framework applicable to the product category and market, as well as on customer expectations in the market, which may potentially exceed the regulatory requirements.

The ambitious goal of Chem-X verification concept development is to assess and define design concepts that can be utilized by companies in the chemical industry independent of context. As such, these design concepts should allow cost-efficient scale-up of software tools and effective contributions to standardization. Therefore, we establish the following working hypotheses for potential verification concepts:

---

[1] In fact, such a scenario is comparable to human- or machine verified data deployed in today's training pipelines for very large scale generative artificial intelligence.
[2] "Certification" indicates verification or conformity assessment by a third-party service provider. Manual certification is often facilitated by database providers. See also Section 2.2.
[3] This process is also called "conformity assessment" or "verification" for short.

1. **Flexibility:** Due to the vast diversity of chemical use cases the verification concepts allow for different trade-offs between company effort and required level of evidence, level of risk, etc.

2. For tasks or processes **related to Product Declaration:**
   - Verification processes are subject to and defined by regulatory compliance[4].

3. For tasks or processes **beyond Product Declaration:**
   - Verification of data should address (at least) four dimensions:
     - Legal: "Is the legal status of this data acceptable?"
     - Organizational: “Is this data sender a legitimate counterpart for me?”
     - Semantic: "What does this data mean exactly in view of applicable standards and rule sets, etc.?”
     - Technical: "Can I access this data in a secure and economical way?"

2.1. Self-Sovereign Identity (SSI)

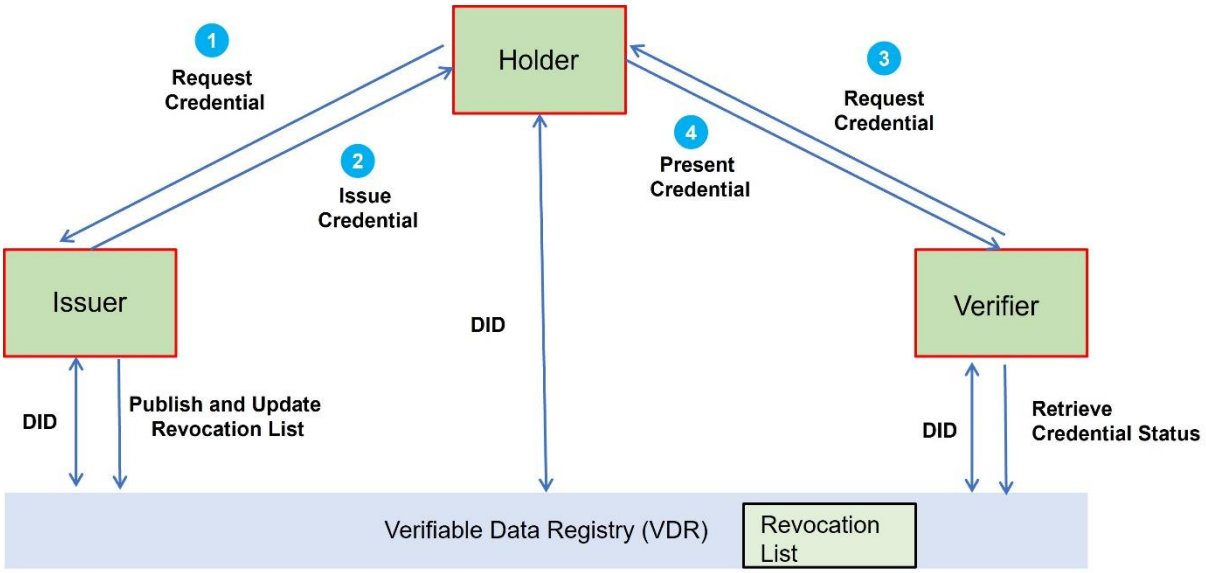

Figure 1 - Interaction of Actors in the SSI Model

Self-Sovereign Identity (SSI) is an innovative identity management model that empowers users with full control over their personal data and identity credentials. Unlike traditional identity management systems, where organizations or third-party providers control users' identities, SSI enables direct connectivity between users and organizations.

The SSI model assigns three key roles: the Issuer, the Holder, and the Verifier. The Issuer is responsible for creating and issuing credentials to the Holder. The Holder then receives these credentials and shares them with the Verifier, who verifies the credentials presented by the Holder. This framework not only enhances privacy but also supports transparency and trust in digital interactions [2]. SSI places the identity holder at the center of its architecture [3]. The identity holder, who can be an individual, organization, or machine, has full control over their data.

[4] The scope of product declaration is further defined in TP3. Example: CLP / GHS.

This model enables selective disclosure, meaning the holder can decide which parts of their identity to share and under what conditions. The fundamental principle of SSI is to empower individuals by providing them with control over their identity data, thus promoting privacy and minimizing data exposure.

The SSI model leverages decentralized identifiers (DIDs) for identity verification. A DID is a globally unique identifier that does not rely on central authorities for its creation or management. Instead, it uses cryptographic methods to verify the identity of the holder. In SSI, the identity holder proves ownership of their identity through challenges or presentations that are authenticated using cryptographic keys. In the architecture presented in Figure 1, entities are identified by their DIDs. This includes issuers, holders and verifiers to ensure transparency and accountability, as requests and presentations can be traced back to the individuals who initiated the process. DIDs can be anchored in a Verifiable Data Registry (VDR), which is a decentralized, secure system that stores and provides access to cryptographically verifiable data, thus ensuring its authenticity and integrity. Consequently, DIDs can be resolved by querying the corresponding VDR. Furthermore, a VDR permits the publication of revocation status for credentials in a privacy-preserving manner.

Based on the SSI concept, Chem-X aims to develop a verification concept that achieves interoperability. Interoperability refers to the ability to exchange data and information between different systems, applications, or components. In the context of SSI, interoperability encompasses four levels: technical, syntactic, semantic, and organizational. Since SSI is decentralized, interoperability between different systems depends on components that build trust and enable secure communication between entities without central authority. Yildiz et al. [4] provide a shared definition of SSI interoperability and present a reference model to understand the differences between technology stacks. They define the four levels of SSI interoperability as follows:

- **Technical Interoperability**: Refers to the ability of machines to communicate with each other through hardware, software, and technologies. The focus is on the underlying protocols and systems that enable communication. In SSI, systems must adhere to common standards to allow secure communication and data exchange between software agents.
- **Syntactic Interoperability**: Deals with how data is formatted and structured for communication. Most SSI systems use data formats like JSON or JSON-LD, which reduce compatibility issues between systems.
- **Semantic Interoperability**: Ensures that both the sender and the receiver understand the meaning of the exchanged data. In SSI, technologies like Linked Data are frequently used to achieve this.
- **Organizational Interoperability**: Enables organizations, regardless of whether they use distributed ledgers or other systems, to exchange and interpret data effectively. SSI can also be integrated with existing identity and access management systems to improve compatibility.

2.2. Conformity Assessment

Conformity assessment is the process of determining whether a product, service, process, management program, or system meets the specified requirements or standards. In the context

of verification, it refers to the activities involved in confirming that an entity's identity, credentials, or data comply with predefined standards and regulations. This process ensures that the systems, identities, and data exchanged across various entities, especially in decentralized and digital ecosystems, are trustworthy, accurate, and compliant with relevant regulations or laws.

In the context of data spaces, conformity assessment ensures that entities, services, and data meet the standards to promote trust and interoperability. This process involves checking claims about performance against objective evidence and may include activities such as testing, inspection, evaluation, and certification. The Data Spaces Support Centre (DSSC) outlines a comprehensive framework for establishing conformity assessment schemes within data spaces [5]. This framework is based on the principles set forth in the ISO/IEC 17000:2020 standard [6], which defines conformity assessment as a process comprising a set of rules and procedures that specify the objects of assessment, define the requirements, and outline the methodologies for conducting the assessment. According to DSSC, conformity assessment schemes in data spaces are categorized into two types: mandatory and optional.

- **Mandatory Conformity Assessment Schemes**: These schemes enforce a basic set of requirements that an entity or service must meet to be considered compliant within the data space. These mandatory requirements are essential for establishing trust and transparency among participants, ensuring that a minimum standard is upheld across the ecosystem.
- **Optional Conformity Assessment Schemes**: These schemes aim to provide additional levels of assurance and offer higher confidence in the compliance of participants. They are intended to enhance trust among participants, particularly in scenarios where more rigorous assessment is needed to support decision-making or where sensitive data is exchanged.

The result of a conformity assessment is an attestation, a statement that confirms whether specified requirements have been met. There are three primary types of attestations based on the party conducting the assessment:

- **First-party Conformity Assessment (Self-declaration)**: This occurs when an individual or organization declares their own compliance with a set of requirements or standards. It is typically used in low-risk or transitional scenarios where the party asserting compliance has the responsibility for the object being assessed.
- **Second-party Conformity Assessment**: This assessment is conducted by an entity that has a vested interest in the subject. For example, a trainer evaluating a trainee's skills or a partner assessing a supplier's capabilities. It provides a level of assurance from a party with an existing relationship to the object being assessed.
- **Third-party Conformity Assessment (Certification)**: This type of assessment involves an independent, impartial assessment body (e.g., auditing company or TÜV) for conducting a conformity assessment. This assessment body then issues a written assurance confirming compliance, called a certificate. Third-party certifications are generally used to ensure a high level of trust and assurance in the data space.#

When defining conformity assessment schemes, the Data Space Governance Authority is responsible for determining the appropriate level of assessment for each requirement—whether it should be a first, second, or third-party assessment. This decision balances the need for trust and assurance with the resources required to conduct the assessment. By aligning the

assessment level with the criticality of the requirement, the governance authority ensures that the right level of scrutiny is applied to different aspects of data space operations.

Aligned with the DSSC definition, the Catena-X conformity assessment concept [7] ensures that all participants and services within the Catena-X ecosystem adhere to standardized protocols. It adopts a modular and role-based certification approach, clearly defining the object of conformity according to participant roles and specific use cases. Catena-X also aligns with the emphasis on trust and assurance by relying primarily on third-party conformity assessments. Independent Conformity Assessment Bodies (CABs) carry out certifications. In scenarios where third-party certification may not yet be practical—such as during ecosystem transitions—Catena-X allows for time-limited self-assessment.

Each certification corresponds to a defined set of standards and is guided by a certification framework that specifies the necessary criteria. This framework is continuously updated alongside new releases of the Catena-X ecosystem, such as the current "Jupiter" release, to ensure that all certifications remain relevant and valid. Successful certifications are then recorded in the Catena-X Data Space Clearance List, which acts as a public registry of all certified entities. To ensure ongoing compliance, certified participants must regularly renew their certification in line with new ecosystem releases or confirm ongoing compliance through approved self-assessments.

Finally, DSSC emphasizes the need for schemes to promote interoperability across data spaces. This is achieved through the development of shared semantic models and common vocabularies, enabling consistency in how conformity objects are defined and assessed across different ecosystems. Conformity assessment schemes should adopt machine-readable and standardized evidence and digital attestation formats to facilitate automation and cross-space validation.

2.3. Semantic Verification

In data spaces, semantic verification is crucial for ensuring that data is interpreted accurately and consistently across various participants and systems. Data models play a vital role in this process by providing structured representations of data elements and their relationships, ensuring that exchanged data retains its intended meaning. These models incorporate metadata to define the semantics of data, enabling semantic interoperability between diverse organizations and systems. This process allows data to be exchanged seamlessly, ensuring that all participants speak the same language.

The need for semantic verification arises from the diverse ways organizations perceive and structure data. Without a shared understanding, data exchanged between parties could be misinterpreted, leading to errors and inefficiencies. To overcome this challenge, data spaces should adopt shared data models or semantic standards. These models act as dictionaries, helping data providers and consumers align their understanding during data exchanges. In data space initiatives, a multi-stakeholder governance structure can be established to ensure consensus on the data models used, promoting uniformity while respecting diverse needs.

A data model consists of metadata that provides the necessary context for understanding shared data. By using shared models, participants in a data space can ensure that data exchanged between them is interpreted consistently. A common repository, such as a Vocabulary Service, helps manage these models, allowing participants to reference and agree upon the data model

during exchanges. This process ensures that both senders and receivers interpret data in a consistent manner.

A list of key components for semantic verification can be listed as follows:

- **Data Model Development and Abstraction:** Data models should facilitate both semantic and technical interoperability. While semantic interoperability ensures that the meaning of concepts is shared across different systems, technical interoperability focuses on the syntax and structure of the data exchanged. Data model abstraction ensures that data is represented in a way that both humans and machines can understand, and it transitions from semantic to technical interoperability.
- **Data Model Governance:** Effective data model governance is crucial for managing the lifecycle of data models. This includes setting guidelines for creating, updating, and maintaining models, ensuring that models evolve with the changing needs of the data space. Governance processes are supported by tools like Vocabulary Services to facilitate the publication, editing, and discovery of data models across the data space.
- **Ontology Matching and Semantic Interoperability:** Ontologies are commonly used to describe the semantic meaning of data. They enable systems to represent and interpret data based on its structure and the relationships between data elements. Ontology matching ensures that different ontologies or data models can be aligned and used across diverse systems, addressing interoperability issues.
- **Machine-Readable Attestations:** Machine-readable evidence and digital attestation formats are used to support the automation of conformity assessments, making it easier to validate compliance across systems. This ensures that conformity assessments can be efficiently carried out and trusted in a decentralized ecosystem.
- **Vocabulary Services and Data Model Reuse:** Vocabulary services store and manage data models, enabling them to be referenced and reused across data spaces. This ensures that data models are consistently applied and interpreted in exchanges between participants. Furthermore, the reuse of existing models, where possible, helps ensure that data spaces can leverage established standards and avoid reinventing the wheel.

Catena-X provides a practical example of semantic verification through the implementation of semantic data models. For instance, in CX-0135 Business Partner Company Certificate Management [8], semantic verification ensures that data, such as company certificates, is both machine-readable and semantically interoperable across the Catena-X ecosystem. The semantic model for certificate management is based on SAMM (Semantic Aspect Meta Model), version 2.1.0, which is aligned with the Catena-X standard CX-0003 [9]. This model allows data providers to define the semantics of the information being exchanged using a formal structure. By including a semantic model identifier, data providers ensure that consumers interpret the data consistently and accurately.

The semantic model includes rich metadata attributes like certificate type, issuing authority, trust level, and enclosed sites. These attributes are standardized semantically and contextually enriched, facilitating validation and trust-building across the network. The machine-readable format of the semantic model (RDF Turtle) ensures that semantic definitions are both human-comprehensible and machine-processable, supporting the automation of verification processes and reducing ambiguity during data exchanges. Catena-X manages these semantic models

centrally through a public GitHub repository (Eclipse Tractus-X), which reinforces transparency and encourages reusability across different domains and use cases.

3. Technical Verification Components

Trust models comprise a set of guidelines, standards, processes, and compliance criteria for verifiable statements or certificates of authenticity that must be applied and implemented by the participants in an ecosystem to establish trust among the stakeholders. Such models require a set of technical components to ensure that these criteria are met. This chapter provides an overview of key technical components that enable verification within data ecosystems.

Catena-X initiative is taken as a main reference model for the Chem-X dataspace, for this reason the technical verification components are analyzed in detail, together with the required modifications, extensions and the future work planned internally for the Catena-X project. Furthermore, Catena-X and Together for Sustainability (TfS) verification framework is reviewed to examine its relevance, structure, and applicability as a reference model for verification processes in Chem-X. Finally, reference projects that work on trust frameworks and technical verification components are analyzed under “Beyond Catena-X” section.

3.1. Catena-X Verification Components

Catena-X is an initiative aimed at creating a collaborative and secure data ecosystem for the automotive industry [10]. This project focuses on enhancing the efficiency and transparency of the automotive supply chain by facilitating seamless data exchange among manufacturers, suppliers, and service providers. Catena-X has created the Catena-X Association, which has taken on the tasks of the supervisory body, the standardization committee, and the accreditation body. Some of the tasks of the supervisory body are linked to the Catena-X steering committee as the decision-making body. The role of conformity assessment body is currently performed by Deloitte Germany within the Catena-X ecosystem.

The Catena-X Operating Model White Paper [11] describes the basic features of the trust model and the associated processes within the Catena-X ecosystem. It focuses on standardization, certification, and conformity assessment to create trust and security within the network. This subsection defines the main technical verification components of Catena-X and provides a review regarding the required extensions.

3.1.1. Clearing House

The Catena-X Association has officially designated a centralized Clearing House, which is currently operational in a production environment. This Clearing House serves as a trusted intermediary for validating data transactions within the Catena-X ecosystem. It ensures secure, standardized, and compliant data exchange by enforcing identity management, transaction validation, and regulatory compliance based on industry standards such as GAIA-X and International Data Spaces (IDS).

The Clearing House in Catena-X plays a critical role in ensuring trust, transparency, and compliance in the automotive data ecosystem. The Catena-X Clearing House, operated by T-Systems (a Deutsche Telekom company), fulfills a role comparable to that of a Qualified Trust

Service Provider (qTSP) under the eIDAS Regulation. Its primary responsibilities include executing the onboarding process, verifying the identity and credentials of participant organizations, and issuing Catena-X member and identity credentials. This ensures that only authorized and validated entities can participate in the data space. The T-Systems clearing house is comparable to the role of a trust service provider in eIDAS. In addition, Cofinity-X provides central services such as the operation of trust lists and a register for authorized Catena-X participants as well as for qualified services that have undergone conformity testing.

Complementing these services is the Gaia-X Digital Clearing House (GXDCH) [12], which functions as an external trust infrastructure aligned with the Gaia-X Trust Framework for onboarding new ecosystem actors and technical features designed to ensure interoperability between ecosystems. GXDCH is responsible for validating legal entities, checking Gaia-X compliance, verifying self-descriptions, and issuing eIDAS-compliant digital signatures and Gaia-X credentials. For Catena-X, a single GXDCH provider is appointed and managed by the Association to ensure uniform compliance. All Onboarding Service Providers that support participant integration into Catena-X are required to connect to the GXDCH and adhere to its verification processes. In addition to onboarding and credential issuance, the Clearing House also contributes to maintaining transaction traceability by supporting the logging of data exchanges. By facilitating interoperable and secure data handling, it reinforces transparency and accountability within the network.

The implementation of a new Clearing House requires careful consideration of multiple factors, including development time, cost, resource allocation, and regulatory approvals. The process involves technical implementation efforts, integration with the existing Catena-X infrastructure, and ensuring compliance with data governance frameworks such as GAIA-X. Additionally, securing approval from the Catena-X Association and relevant stakeholders is a critical step, which can be time-intensive due to the need for consensus, regulatory validation, and alignment with industry standards.

3.1.2. Verification Components with No Required Modifications

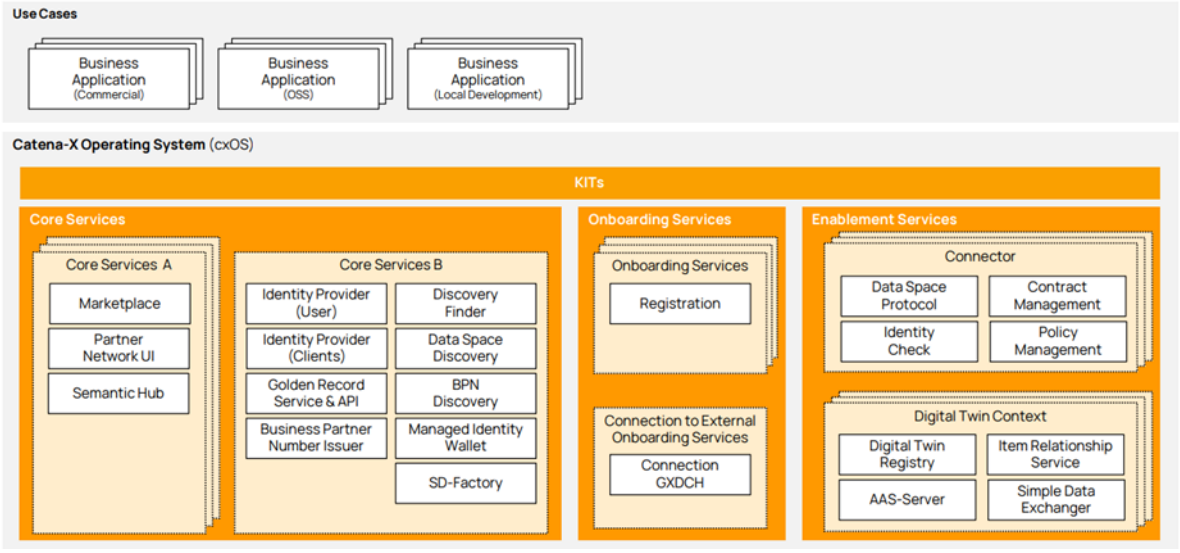

Figure 2– Catena-X Service Map [11]

This sub-chapter describes the existing components of the Catena-X ecosystem that already fulfill the functional verification requirements and hence do not need to be adapted or extended. The components discussed in this and the subsequent section can be identified in the service map of Catena-X, given in Figure 2.

A. BPN DID Resolution Service

Reference: github.com/eclipse-tractusx/bpn-did-resolution-service

Definition: This service maps Business Partner Numbers (BPNs) to Decentralized Identifiers (DIDs), facilitating the resolution of a BPN to its corresponding DID document.

Use in Verification: It enables the retrieval of public keys and service endpoints associated with a BPN, which are essential for verifying digital signatures and establishing trust in decentralized identity frameworks.

Interaction with Other Components: The service interacts with the Identity Wallet and Issuer Service to resolve identities and verify credentials during data exchanges.

B. Business Partner Number Issuer

Reference: catenax-ev.github.io/docs/next/standards/CX-0010-BusinessPartnerNumber

Definition: This component is responsible for issuing globally unique, semantically enriched identifiers (BPNs) to organizations within the Catena-X network.

Use in Verification: BPNs serve as the primary identifiers for companies, enabling consistent and reliable verification of business partner identities across the network.

Interaction with Other Components: The BPN Issuer works in conjunction with the Identity Provider and Semantic Hub to ensure that issued BPNs are integrated into identity management and semantic data models.

C. Identity Provider

Reference: catena-x.net/ecosystem/onboarding

Definition: This service manages user identities, handling authentication and authorization processes for individuals accessing the Catena-X ecosystem.

Use in Verification: It authenticates users and issues tokens that are used to verify user identities during interactions with other services and components.

Interaction with Other Components: The Identity Provider interfaces with the Identity Wallet and Issuer Service to manage user credentials and facilitate secure access to resources.

D. Issuer Service

Reference: catenax-ev.github.io/docs/next/standards/CX-0013-IdentityOfMemberCompanies

Definition: This service issues verifiable credentials to entities within the Catena-X network, attesting to various attributes such as company identity and certifications.

Use in Verification: Verifiable credentials issued by this service are used to authenticate and authorize entities during data exchanges and interactions within the network.

Interaction with Other Components: The Issuer Service collaborates with the Identity Wallet and BPN DID Resolution Service to ensure that credentials are properly linked to decentralized identities and can be verified by other participants.

E. Semantic Hub

Reference: github.com/eclipse-tractusx/sldt-semantic-models

Definition: The Semantic Hub is a centralized repository within the Catena-X ecosystem that stores and manages semantic models, known as Aspect Models. These models are based on the Semantic Aspect Meta Model (SAMM) standard and define the structure and semantics of data exchanged in the network.

Use in Verification: By providing standardized semantic definitions, the Semantic Hub ensures that data exchanged between participants is semantically interoperable. This standardization facilitates the validation and verification of data structures, enabling consistent interpretation and processing across different systems.

Interaction with Other Components:

- **Digital Twin Registry**: The Semantic Hub works in conjunction with the Digital Twin Registry to associate semantic models with digital representations of physical assets, ensuring that data about these assets is semantically enriched and standardized.
- **Data Providers and Consumers**: Participants in the Catena-X network use the Semantic Hub to access and utilize semantic models for data exchange, ensuring that the data they provide or consume adheres to agreed-upon standards.
- **Aspect Model Catalog**: The Semantic Hub integrates with the Aspect Model Catalog, allowing for the publication and discovery of semantic models that define various aspects of assets and processes within the ecosystem.

3.1.3. Verification Components with Required Modifications and Extensions

This sub-chapter focuses on Catena-X verification components that require either changes to existing Catena-X functionality or the addition of new modules. To enable robust verification and secure verifiable credential exchange across the Catena-X and Tractus-X ecosystems, several key components must be either introduced or extended.

Identity Wallet

Definition: Digital identity wallets allow businesses to store and present official credentials, enabling trusted and automated interactions with partners.

In the European Union, the eIDAS regulation provides the legal framework for this system. It allows governments to issue credentials like Legal Person Identification Data (LPID) to businesses. These, along with non-governmental certificates (e.g., ISO certifications), can be managed in an EU Digital Identity Wallet.

For global transactions, the Legal Entity Identifier (LEI) offers a worldwide alternative for authenticating companies. Both EU and global credentials serve to digitally verify a company's identity, subject to jurisdictional rules.

Use in Verification: Identity wallets enable dataspace participants to request and store verifiable credentials from various sources and presenting them to other data space participants. This includes the presentations of identity credentials (e.g. LPID) issued by the government during onboarding, dataspace membership credentials issued by clearinghouses, and business certifications (e.g., ISO certifications). As a result, the gap between dataspace internal and external trust ecosystems is bridged, creating enhanced interoperability.

Interaction with other components:

- **Clearing house:** Onboarding to dataspaces currently involves a manual authentication process that can be automated by using identity wallets. The result of the process is a membership credential issued to the identity wallet.
- **Semantic hub:** In order to achieve interoperability with certifications issued by entities external to the dataspace, the semantic definition of the certification is required. It is expected that definitions are present outside the dataspace but need to be mirrored to the semantic hub to achieve accessibility for all participants.
- **Wallets:** A common communication protocol is required for exchanging verifiable credentials to ensure interoperability.
- **Trusted issuers:** A registry of trusted issuers is required defining who is authorized to issue certain credential types.

Schema Registry

A Schema Registry is essential to validate the syntactical structure and semantics of verifiable credentials. While initial foundations exist through eclipse-tractusx/sldt-semantic-models, this needs to be extended to cover governed, versioned credential schemas aligned with regulatory data models (e.g., ESPR, Battery Regulation).

Trusted Authority Registry

This component must hold a list of recognized credential issuers—such as regulators, recyclers, or notified bodies—to enable verifiers to check whether a credential was issued by a trusted entity.

Dependency and Integration

Verification requires both components to work in tandem: the Trusted Authority Registry defines who is authorized to issue, while the Schema Registry defines what can be issued and how it should be validated. Without both, reliable credential verification in the Catena-X ecosystem is not possible.

Company Certificate Verification

Reference: catenax-ev.github.io/docs/next/standards/CX-0135-CompanyCertificateManagement

Definition: A process and associated tools for validating company-issued certificates, ensuring their authenticity and compliance with Catena-X standards.

Use in Verification: Enables participants to verify the legitimacy of company certificates, which is crucial for establishing trust and ensuring secure interactions within the ecosystem.

Interaction with Other Components: Works in conjunction with the Identity Wallet and Credential Verifier to authenticate certificates and associate them with the correct digital identities.

Credential Verifier

Definition: An entity - such as a service, application, or platform - that receives a digital credential from a user (the holder) and checks its validity.

Use in Verification: during the verification process the following tasks are executed by a credential verifier implementation:

- *Checking the credential's integrity:* Ensuring the credential has not been tampered with by verifying its cryptographic signature.
- *Validating the issuer:* Confirming the credential was issued by a trusted and recognized authority.
- *Verifying status:* Making sure the credential is still valid (not expired or revoked)

Interaction with Other Components:

The Credential Verifier gathers information from the Trusted Authority Registry to validate the issuer. When the credential includes revocation information, the credential verifier accesses that information to verify the revocation status of the credential.

Data Space Governance

Reference: https://catenax-ev.github.io/docs/operating-model/how-data-space-governance

Definition: Data Space Governance in Catena-X defines the organizational and technical rules for secure, interoperable, and fair participation in the data ecosystem. It covers identity management, credentialing, data sharing policies, compliance enforcement, and dispute resolution mechanisms. It ensures that all participants behave according to shared rules and that these rules are technically enforceable.

Use in Verification: Data space governance provides the legal and procedural foundation for trust frameworks used in verifying identity, credentials, and access rights. It also establishes certification and compliance criteria for participants and services (e.g., wallets, verifiers), and ensures verification is consistent with policies agreed upon by data space members.

Interaction with Other Components:

- Issuer Service & Credential Verifier: Must align with governance policies when issuing and verifying credentials.
- Trusted Issuer List: Maintained and controlled according to governance decisions.
- Identity Wallets: Must be compliant with rules for identity presentation and data minimization.
- Data Space Participants: Required to onboard through a governance-compliant process.

Product Identifier Verification

Definition: A system for validating product identifiers, ensuring that products are accurately and uniquely identified within the Catena-X network.

Use in Verification: Ensures the authenticity and traceability of products by verifying their identifiers, which is essential for supply chain transparency and integrity.

Interaction with Other Components: Works alongside the Semantic Hub to understand product data structures and with the Credential Verifier to authenticate product-related credential

3.1.4. Catena-X Future Vision on Verification

This section outlines the anticipated developments in the Catena-X ecosystem related to verification processes and supporting infrastructure. The listed roadmap items reflect planned enhancements aimed at increasing compliance, trust, automation, and interoperability across different verification domains.

A. Gaia-X Compliance into Catena-X Release 25.09 for Enhanced Compliance and Interoperability

Description: To align with the evolving Gaia-X Trust Framework, the Gaia-X Loire Release is to be integrated into Catena-X Release 25.09. This integration is crucial for maintaining interoperability, data sovereignty, and trust within the Catena-X ecosystem, aligning with European data protection and transparency principles.

Expected Outcome: Expected Outcome: Successful integration of Gaia-X Loire Release components into Catena-X Release 25.06, including updated compliance mechanisms, digital clearinghouse functionalities, and adherence to the Gaia-X Compliance Document 24.06.

Project Benefits: Enhances the Catena-X platform's compliance with European data standards, ensuring interoperability and trustworthiness. This integration also streamlines automated compliance processes, reducing manual oversight and potential errors.

B. Roadmap Item: Definition of Carbon Border Adjustment Mechanism (CBAM) Use Case

Description: A roadmap item targets the implementation of a Carbon Border Adjustment Mechanism (CBAM) use case within the Catena-X infrastructure. The goal is to enable privacy-preserving certificate and data workflows between suppliers, importers, and the EU registry.

Expected Outcome: Standardization of CBAM-compliant data exchanges along the value chain in accordance with EU customs and sustainability requirements.

Project Benefits: Improved readiness for regulatory compliance, support for suppliers and importers, and enhanced traceability of carbon-related data.

C. Validation Mechanism Certificates

Description: The project aims to develop an automated validation system for certificates, which are often issued as PDFs. This system will scan the certificate and validate its key attributes using AI technology.

Expected Outcome: An AI-powered tool that automatically scans and validates PDF certificates.

Project Benefits:

- Efficiency: Reduces the time and effort required for manual certificate validation.
- Accuracy: Ensures precise validation of key attributes, minimizing human error.
- Security: Enhances the credibility and trustworthiness of certificates.
  Scalability: Can be applied to various types of certificates across different industries.

D. Improve data integrity and security after EDC exchange packing data in Verifiable Credentials and Presentations

Reference: https://github.com/eclipse-tractusx/digital-product-pass/tree/main/dpp-verification

Description: Based on the Data Certification and Verification Framework (DCVF), propose a solution for all Catena-X standardized data to keep the data sovereignty after leaving the Dataspace taking into consideration the B2C concept.

Expected Outcome: Using verifiable credentials for "certify" the data issuance will increase the security and integrity for all the Catena-X data. Once the data is issued it can be also presented to external partners and be traced back to the Catena-X dataspace partner (keeping the data sovereignty).

Project Benefits: Have more interoperability with other data spaces that use verifiable credentials to "certify" and "secure" their data. Using W3C Standards. And enables the verification of any Catena-X data that was transferred with the EDC. Also enables a better data origin trust and traceability.

Market Benefits: Enables companies to have more data quality and trust the origin of the data provided via Catena-X

E. Integration of the Verifier role

Description: In order to increase the trust and transparency of data within the Catena-X ecosystem, the role of verifier is to be introduced. This role is responsible for checking and verifying the data sets provided by companies. The integration of the verifier role is essential in order to increase the credibility and acceptance of data within the ecosystem and thus enable well-founded decisions in the value chain. In addition, the extent to which the concept of the verifier role can be transferred to various use cases within Catena-X will be investigated to increase the trustworthiness and transparency of data there as well.

Expected Outcome: A clearly defined verifier role with associated responsibilities, relationships and prerequisites

Benefits: Increased trust in the quality and reliability of data

3.2. Catena-X & Together for Sustainability (TfS) Verification Framework

As of November 2025, the joint framework[5] by Catena-X e.V. and TfS AISBL is specifically designed for the verification of product carbon footprint (PCF) data that is transferred from supplier to customer for the purpose of PCF calculation. The guideline supports flexible implementation in terms of levels of evidence, roles and work processes that are supported.

In terms of level of evidence or so-called "levels of trust" the guideline specifies:

- **Level 1** (entry level): "...use of (automated) solutions to perform PCF dataset completeness checks, including conformity with the PCF data models, transferred through data exchange platforms and connected solutions. This level of trust does not constitute any type of verification or certification." (p. 9)
- **Level 2**: "...certification of PCF programs operated by companies against requirements [...]. The certificate of an independent third party demonstrates that a company operating a PCF program is able to organize and to run PCF calculations in line with the requirements of the respective rulebook." (p. 9)
- **Level 3**: "...verification of specific PCF datasets by an independent party." (p. 9)

The guideline prescribes a number of roles that are tied to the different "levels of trust":

- **Independent third-party** verification (i.e., conformity assessment body / service provider) to certify Level 2 or Level 3. Catena-X and TfS have stated plans to ensure the competence of third-party service providers via a separate "appointment" process (chapter 6.3.10).
- **First-party** verification (in-house role in the supplier company) - provided the company is certified on Level 2 – to verify specific data sets on Level 3.
- **Second-party** verification (in-house role in the supplier company) - provided the company is certified on Level 2 - to verify specific data sets on Level 3 (in technical conformity assessment this role is sometimes called "Eigenüberwachung" in German).

Moreover, the guideline envisions two distinct work processes:

- **"Verification of reporting"**, i.e., verification of evidence in retrospect. For example, reports about past GHG emissions related to specific products delivered to the customer.
- **"Validation of forecasting"**, i.e., verification of forecasts of future GHG emissions. This is a prospective task supporting planning and risk monitoring on the customer side (see also Section 2 of this paper). The evidence in this case is, for example, the production plan provided by the supplier.

3.3. Beyond Catena-X: Verification Reviews of Different Projects

To broaden the Chem-X verification review beyond Catena-X, this section reviews five major projects Battery Pass, CIRPASS, PACT, UNTP, and Energy Data-X. The first four projects are reviewed through a common structure, comparing their verification mechanisms for business identity, product identity, and value-related claims using structured tables[6]. These comparisons focus on credential types (self-signed vs. third-party), trust anchors, roles of issuers and verifiers,

[5] https://catenax-ev.github.io/docs/non-functional/overview
[6] The tables reflect the status of the projects as of November 2025.

and identity management practices. Finally, Energy Data-X represents a domain-specific implementation of a Gaia-X-compliant trust framework in the regulated energy sector. Specific attention is given to the definition of market roles in this dataspace project, as the project introduces an alternative approach via use of a sector-specific database to extend credentials so that they are not limited to proving identity but prove role-specific regulatory authorization.

3.3.1 Battery Pass

The Battery Pass Consortium is dedicated to developing the technical standards and content guidance necessary for the implementation of the EU Battery Passport, which is mandated by the EU Battery Regulation [13]. The consortium comprises leading organizations from industry, technology, and academia, and it focuses on enhancing sustainability and circularity in the battery value chain. In this section, Battery Pass Consortium's verification processes for business identity, product identity, and product identity and value are summarized, as presented in Battery Passport Technical Guidance [14].

Table 1: Battery Pass Business Identity Process Overview

	Self-Signed	**Third-Party Signed**
Claim Type	Legal entity name, address	Economic Operator Identifier
Evidence Type	Text assertion	Credential signed with DID/BPN
Process Description/Pilot	No verification	Catena-X onboarding
Rule set (Method, Standards)	None	eIDAS, GAIA-X, Catena-X onboarding
Role: Credential Issuer	Company IT	GAIA-X compliant IdP / Notified Body
Role: Credential Holder	Company	Company
Role: Credential Verifier	Internal system	Platform or partner
Role: Identity Provider	None	Notified Body / Company IdP
Identity Registry/ Trust Anchor	None	GAIA-X Trust Framework
Identity Wallet	None	Federated or Enterprise wallet
Credential Wallet	None	IDunion, Lissi, etc.

Table 2: Battery Pass Product Identity Process Overview

	Self-Signed	**Third-Party Signed**
Claim Type	Internal Serial Number	Unique Product Identifier (e.g. battery ID)
Evidence Type	Manual entry	Manufacturer-issued VC
Process Description/Pilot	Manufacturer entered	Traceable item registration
Rule set (Method, Standards)	Internal rule	Battery Pass ID method
Role: Credential Issuer	Company	Manufacturer or trusted entity

Role: Credential Holder	Manufacturer	Manufacturer
Role: Credential Verifier	Application UI	Battery Platform
Role: Identity Provider	None	Manufacturer or registry
Identity Registry/ Trust Anchor	None	Battery Registry / Platform
Identity Wallet	None	Manufacturer's system
Credential Wallet	None	Platform-secured

Table 3: Battery Pass Product Identity and Value Process Overview

	Self-Signed	**Third-Party Signed**
Claim Type	Internal attributes	Certified environmental data (e.g., CO_2 footprint)
Evidence Type	Informal attribute entry	3rd-party test/lab signed data
Process Description/Pilot	Data provided by manufacturer	Validation via notified body
Rule set (Method, Standards)	Informal rules by company	EU Regulation (e.g., 2023/1542)
Role: Credential Issuer	Manufacturer	Accredited Certification Lab
Role: Credential Holder	Manufacturer	Economic Operator
Role: Credential Verifier	Platform system	Platform or regulator
Role: Identity Provider	None	Certifying Body or Trust Framework
Identity Registry/ Trust Anchor	None	EU Notified Bodies
Identity Wallet	None	SSI-enabled data vault or cloud wallet
Credential Wallet	None	IDunion, company-assigned SSI wallet

3.3.2 CIRPASS

The CIRPASS project [15] is focused on the development and implementation of DPPs. One of the project's key objectives is to define a cross-sectoral product data model for DPPs that aligns with circular economy principles. The project emphasizes the need for a robust data exchange protocol tailored to the needs of circular economy stakeholders.

In this section, CIRPASS's verification processes for business identity, product identity, and product identity and value are summarized. Regarding the verification processes of third-party signed business identities, CIRPASS argues for DID based identities where the identities are issued by a trusted authority against evidence by a provider such as GS1 or a certified EU issuer. Alternatively, the GS1 based identity system is considered for investigation. On the other hand, self-signed identities are not supported in favor of third-party issued identities in the DID approach.

Table 4: CIRPASS Business Identity Process Overview

	Self-Signed	Third-Party Signed
Claim Type	REO (Responsible Economic Operator) Identifier	REO Identifier
Evidence Type	GLNs (Global Location Number) from GS1, REO linked to the Commercial Registers, Actor DID	GLNs (Global Location Number) from GS1, REO linked to the Commercial Registers, Actor DID
Process Description/Pilot	OpenID & OAuth2.0 standard implementation + SSI Infrastructure (Wallets,Verifiable Credential (VC))	OpenID & OAuth2.0 standard implementation + SSI Infrastructure (Wallets,VCs)
Rule set (Method, Standards)	OpenID & OAuth2.0 standard + DCP (Decentralized Claims Protocol)	OpenID & OAuth2.0 standard + DCP Protocol
Role: Credential Issuer	Responsible Economic Operator (REO) or trusted authority	Responsible Economic Operator (REO) or trusted authority
Role: Credential Holder	DPP Data user or Circular Economy Operator(CEOP) or any other Actor	DPP Data user or Circular Economy Operator(CEOP) or any other Actor
Role: Credential Verifier	Responsible Economic Operator (REO)	Responsible Economic Operator (REO)
Role: Identity Provider	n/a	n/a
Identity Registry/ Trust Anchor	Root Certificate Authority (CA), Identity Registry	Root Certificate Authority (CA), Identity Registry
Identity Wallet	DPP minting App, DID & VC Issuer Wallet (REO-App) 4.1.1.1 Minting a Product UID	DPP minting App, DID & VC Issuer Wallet (REO-App)
Credential Wallet	DPP minting App, DID & VC Issuer Wallet (REO-App)	DPP minting App, DID & VC Issuer Wallet (REO-App)

Table 5: CIRPASS Product Identity Process Overview

	Self-Signed	Third-Party Signed
Claim Type	Unique product identifier	Unique product identifier
Evidence Type	URL (RFC3986, IEC6I406-x, GS1 Digital Link) or Product DID (did:method:UID)	URL (RFC3986, IEC6I406-x, GS1 Digital Link) or Product DID (did:method:UID)
Process Description/Pilot	OpenID & OAuth2.0 standard implementation + SSI Infrastructure (Wallets,VCs)	OpenID & OAuth2.0 standard implementation + SSI Infrastructure (Wallets,VCs)
Rule set (Method, Standards)	OpenID & OAuth2.0 standard + DCP Protocol	OpenID & OAuth2.0 standard + DCP Protocol

Role: Credential Issuer	Responsible Economic Operator (REO)	Responsible Economic Operator (REO)
Role: Credential Holder	Responsible Economic Operator (REO)	Responsible Economic Operator (REO)
Role: Credential Verifier	DPP Data user or Circular Economy Operator (CEOP) or any other Actor	DPP Data user or Circular Economy Operator (CEOP) or any other Actor
Role: Identity Provider	Identity Provider of Responsible Economic Operator (REO)	Identity Provider of Responsible Economic Operator (REO)
Identity Registry/ Trust Anchor	Root Certificate Authority (CA), Identity Registry	Root Certificate Authority (CA), Identity Registry
Identity Wallet	DPP App, DID & VC Issuer Wallet	DPP App, DID & VC Issuer Wallet
Credential Wallet	DPP App, DID & VC Issuer Wallet	DPP App, DID & VC Issuer Wallet

Table 6: CIRPASS Product Identity and Value Process Overview

	Self-Signed	**Third-Party Signed**
Claim Type	named knowledge graph	named knowledge graph
Evidence Type	signed graph elements	signed graph elements
Process Description/Pilot	n/a	n/a
Rule set (Method, Standards)	n/a	n/a
Role: Credential Issuer	Responsible Economic Operator (REO)	Responsible Economic Operator (REO)
Role: Credential Holder	Responsible Economic Operator (REO)	Responsible Economic Operator (REO)
Role: Credential Verifier	n/a	n/a
Role: Identity Provider	Identity Provider of Responsible Economic Operator (REO)	Identity Provider of Responsible Economic Operator (REO)
Identity Registry/ Trust Anchor	n/a	n/a
Identity Wallet	n/a	n/a
Credential Wallet	n/a	n/a

3.3.3 PACT

The Partnership for Carbon Transparency (PACT) is an initiative convened by the World Business Council for Sustainable Development to promote standardized, transparent, and interoperable reporting of PCFs across global value chains [16]. In the PACT ecosystem, business identity can be managed either through self-signed mechanisms or third-party-signed authentication [17]. Since PACT does not prescribe a trust-anchor-based business identity system, self-signed identities remain a possibility. In such cases, the responsibility for conducting due diligence during user onboarding is delegated to the software vendor. This introduces a potential

vulnerability, as PACT-interoperable software could, in principle, be created and operated under a false flag.

In scenarios involving third-party-signed identity management, business identity authentication and authorization are implemented via APIs using widely adopted standards such as OpenID and OAuth2.0. Regarding product identity, self-defined (but not self-signed) product identifiers are recommended in certain formats (e.g., UUID acc. to RFC9562) alongside standardized & verified name spaces (e.g., CAS Number). The tables below indicate PACT's verification processes for business identity, product identity, and product identity and value.

Table 7: PACT Business Identity Process Overview

	Self-Signed	Third-Party Signed
Claim Type	n/a	User Identity
Evidence Type	n/a	Login credentials
Process Description/Pilot	n/a	OpenID & OAuth2.0 standard implementation
Rule set (Method, Standards)	n/a	OpenID & OAuth2.0 standard
Role: Credential Issuer	n/a	Identity provider of software application vendor
Role: Credential Holder	n/a	Identity provider of software application vendor
Role: Credential Verifier	n/a	software application
Role: Identity Provider	n/a	Identity provider of software application vendor
Identity Registry/ Trust Anchor	n/a	Root Certificate Authority (CA)
Identity Wallet	n/a	Identity provider of software application vendor
Credential Wallet	n/a	n/a

Table 8: PACT Product Identity Process Overview

	Self-Signed	Third-Party Signed
Claim Type	Product Identity	Product Identity
Evidence Type	n/a	Third-party assigned identifier from third-party managed name space
Process Description/Pilot	n/a	n/a
Rule set (Method, Standards)	n/a	n/a
Role: Credential Issuer	n/a	n/a
Role: Credential Holder	n/a	n/a
Role: Credential Verifier	n/a	n/a
Role: Identity Provider	n/a	n/a

Identity Registry/ Trust Anchor	n/a	n/a
Identity Wallet	n/a	n/a
Credential Wallet	n/a	n/a

Table 9: PACT Product Identity and Value Process Overview

	Self-Signed	**Third-Party Signed**
Claim Type	PCF value and associated meta data attributes	n/a
Evidence Type	TBD: digital signature	n/a
Process Description/Pilot	n/a	n/a
Rule set (Method, Standards)	n/a	n/a
Role: Credential Issuer	n/a	n/a
Role: Credential Holder	n/a	n/a
Role: Credential Verifier	n/a	n/a
Role: Identity Provider	n/a	n/a
Identity Registry/ Trust Anchor	n/a	n/a
Identity Wallet	n/a	n/a
Credential Wallet	n/a	n/a

3.3.4 UNTP

The UN Traceability Protocol (UNTP) establishes a standardized framework for digital traceability across various industries [18]. It defines the structure and types of traceability events—transaction, aggregation, association, and transformation—ensuring consistent and reliable data tracking throughout supply chains. The protocol facilitates transparency and accountability by providing a common language for traceability events.

UNTP is the GS1 standards specific implementation of Rec 49 by UNCEFACT because UNTP relies fully on the implementation of the EPCIS protocol by GS1. Decentralized authentication protocol options and N-tier supplier visibility are unsolved problems pointing back at the centralized GS1 system. Overall, UNTP stands out for its holistic approach linking (1) DPP, (2) Digital Traceability Event, (3) Digital Conformity Credential, and (4) Digital Facility Record. The tables below summarize UNTP's verification processes for business identity, product identity, and product identity and value.

Table 10: UNTP Business Identity Process Overview

	Self-Signed	**Third-Party Signed**
Claim Type	Business Identifer/ Locations	Business Identifer /Locations

Evidence Type	DIA (DID linked public identity such as VAT)	DIA (DID linked public identity such as VAT)
Process Description/Pilot	Identity Resolver (IDR) specification	Identity Resolver (IDR) specification
Rule set (Method, Standards)	IETF link-set, UNTP DPP, DCC	IETF link-set, UNTP DPP, DCC
Role: Credential Issuer	n/a	Trusted authority (eg a government agency)
Role: Credential Holder	n/a	Provider of product information, facility, Supplier
Role: Credential Verifier	n/a	Product buyer/customer
Role: Identity Provider	n/a	Provider of product information or facility
Identity Registry/ Trust Anchor	Digital Identity Anchor (DIA) Trusted Authority	Digital Identity Anchor (DIA) Trusted Authority
Identity Wallet	required, but not specified	required, but not specified
Credential Wallet	required, but not specified	required, but not specified

Table 11: UNTP Product Identity Process Overview

	Self-Signed	**Third-Party Signed**
Claim Type	Identity Resolver (IDR)	Identity Resolver (IDR)
Evidence Type	ISO/IEC 18975, Format RFC9264	ISO/IEC 18975, Format RFC9264
Process Description/Pilot	Identity Resolver (IDR) specification	Identity Resolver (IDR) specification
Rule set (Method, Standards)	IETF link-set, UNTP DPP,DCC	IETF link-set, UNTP DPP,DCC
Role: Credential Issuer	n/a	n/a
Role: Credential Holder	Supplier, Producer or Certifier	Supplier, Producer or Certifier
Role: Credential Verifier	Product buyer/customer	n/a
Role: Identity Provider	n/a	n/a
Identity Registry/ Trust Anchor	Digital Identity Anchor (DIA)	Digital Identity Anchor (DIA)
Identity Wallet	n/a	n/a
Credential Wallet	n/a	n/a

Table 12: UNTP Product Identity and Value Process Overview

	Self-Signed	**Third-Party Signed**
Claim Type	n/a	Attribute/Claim Verification
Evidence Type	n/a	(DCC) Digital conformity credential with additional Accreditation Credential

Process Description/Pilot	Identity Resolver (IDR) specification	Identity Resolver (IDR) specification
Rule set (Method, Standards)	IETF link-set, UNTP DPP,DCC	IETF link-set, UNTP DPP,DCC
Role: Credential Issuer	n/a	iTrusted Assessment
Role: Credential Holder	Supplier, Producer or Certifier	Supplier, Producer or Certifier
Role: Credential Verifier	n/a	n/a
Role: Identity Provider	n/a	n/a
Identity Registry/ Trust Anchor	Digital Identity Anchor (DIA)	Digital Identity Anchor (DIA)
Identity Wallet	n/a	n/a
Credential Wallet	n/a	n/a

3.3.5 Energy Data-X and use of Market Roles in Trust Framework

The Energy Data-X project is a Gaia-X-compliant data space initiative that enables secure and interoperable data exchange in the energy sector through standardized digital identities and trust services [19]. Highlighting eIDAS as a best practice, the project details role structures, trust levels for electronic signatures and seals, and formal requirements that can be used as part of a dataspace trust framework.

In Energy Data-X, the concept of market roles plays a central role in the design of digital trust infrastructures for the energy sector. These roles, such as grid operator and supplier, represent legally distinct entities within regulated energy market processes. The trust model relies on Verifiable Credentials to encode the attributes and responsibilities associated with a given market role. These credentials are issued to wallets and contain cryptographically signed claims such as the associated MP-ID (Market Partner-ID), the name of the legal entity, and the specific role being performed. A core principle of the system is the strict separation of market roles to ensure compliance with legal unbundling requirements. For example, if a company operates as both a supplier and a metering point operator, it must manage separate wallets for each role with separate MP-IDs. This separation supports clear accountability and simplifies authorization logic in the trust infrastructure.

In the context of Energy Data-X, the Business Partner Number (BPN), as introduced in Catena-X, serves as a company-wide identifier, but must be linked to specific MP-IDs for the execution of regulated functions. In the emerging SSI-based architecture, Decentralized Identifiers (DIDs) are technically bound to wallets and used in credential exchanges for authentication and authorization. Authorization decisions are made by a Policy Engine, which evaluates presented credentials to determine whether a party is entitled to perform a specific action within the energy data space. In this context, credentials are not limited to proving identity but also serve as proof of role-specific regulatory authorization. Example use cases include proof of market communication authorization (MaKo), access to Redispatch processes, and the issuance of Origin Proof-Credentials for proving energy origin. A list of market roles in energy data sector is given in Table 13.

Table 13: Energy Market Roles in Energy Data-X Dataspace Project [20]

Market Role	Description
Alignment Agent	Aligns forecasts with nominations to prevent imbalances.
Balance Responsible Party	Handles financial responsibility for energy imbalances.
Balancing Service Provider	Offers balancing capacity and reserves for grid stability.
Billing Agent	Manages invoicing between involved parties.
Capacity Trader	Buys/sells capacity in energy markets (e.g., in the capacity market).
Consumer	End consumer of energy.
Consumer Representative	Acts on behalf of a consumer in energy-related transactions.
Data Provider	Supplies data into the system (e.g., metering, energy usage).
Data Manager	Ensures the accuracy, completeness, and handling of relevant data.
Demand Side Aggregator	Aggregates flexible loads to offer services to the grid or market.
Distribution System Operator	Manages the electricity distribution network.
Energy Supplier	Sells energy to consumers or other businesses.
Flexibility Operator	Offers or manages flexible assets (e.g., batteries, demand shifting).
Market Operator	Administers energy market platforms and ensures fair trade mechanisms.
Metered Data Aggregator	Aggregates metered data for market and settlement purposes.
Metering Point Administrator	Registers and manages metering points in the system.
Metering Point Operator	Installs and operates metering equipment at consumer sites.
Producer	Generates electrical energy for market participation.
Producer Group	Aggregates multiple producers under one commercial interface.
Program Responsible Party	Plans energy schedules and forecasts.
Transmission System Operator	Manages the transmission grid and secures system balance.
Virtual Power Plant Operator	Coordinates decentralized energy resources as a single controllable unit.

4. Verifiable Credentials

W3C Verifiable Credentials [21] are tamper-evident credentials whose authorship can be cryptographically verified, allowing them to serve as reliable digital representations of physical

credentials. They can encapsulate the same information found in traditional credentials, enhanced by technologies like digital signatures, which increase their trustworthiness and resistance to tampering. A verifiable credential comprises one or more claims made by a single entity, accompanied by identifiers and metadata detailing aspects such as the issuer, validity periods, representative images, and status information. Examples of verifiable credentials include digital employee IDs, driver's licenses, and educational certificates, all designed to support the creation of verifiable presentations that can also be cryptographically validated.

Verifiable credentials express properties related to one or more subjects and the credentials themselves. The specification defines several key properties, including @context, which provides the context of the credential; id, which serves as a unique identifier; type, indicating the category of the credential; and name and description for human-readable details. Additionally, properties like issuer, which denotes who issued the credential, and credentialSubject, specifying the subject of the claims, are included. Other relevant properties cover validity periods (validFrom and validUntil), status, which indicates the current state of the credential, and credentialSchema, detailing the structure of the credential. The specification also allows for the inclusion of a refreshService for updates, termsOfUse, and evidence to support the claims made. Moreover, verifiable credentials can be customized with additional properties through an extensibility mechanism.

As explained in Section 2.1 for the SSI model, the trust model of the verifiable credentials' ecosystem assigns three key roles: the Issuer, the Holder, and the Verifier. The Issuer is responsible for creating and issuing credentials to the Holder. The holder of a verifiable credential operates in a triangle of trust, in which the issuer trusts the holder, the holder trusts the verifier, and the verifier trusts the issuer.

The credentials are presented in a standardized format, and the holder can share them with verifiers to confirm their identity or claims. The Verifiable Credentials Data Model v1.1 [21] outlines a standardized method for expressing secure, privacy-respecting, and machine-verifiable credentials on the web. It details essential components such as issuer information, subjects, claims, and cryptographic proofs to ensure data integrity, making it adaptable for various credential types. The subsequent version, Verifiable Credentials Data Model v2.0 [22], builds on this foundation by refining the specifications and enhancing privacy considerations. This iteration facilitates improved interoperability and expands the mechanisms for credential verification, thereby enabling secure digital interactions across multiple platforms.

4.1. Business Identity Credentials

The identity of any entity or partner in the context of a Chem-X dataspace—such as a company, user, or technical client/connector—is defined as the collection of describing attributes, including company name, address, and tax number. Participating partners must be identifiable in an independent and interoperable manner across different networks. This requirement can be addressed at the company level using SSI and verifiable credentials. In Catena-X, the digital identity of a partner serves as the basis for all interactions with other participants. To preserve independence and data sovereignty, the identity remains under the control of the respective partner company. Within the Catena-X ecosystem, various types of identity credentials are applied to support this approach.

4.1.1. Membership Credential

A membership credential confirms that the participant is onboarded to Catena-X and agreed to the Catena-X terms and conditions. The credential is issued to the participant by the core service provider or a core service provider assigned issuer. A verifiable membership credential is issued and stored in the membership holder wallet after the membership verification process as described in Section 5.1.

4.1.2. Business Partner Number (BPN)

The BPN credential contains the Business Partner Number of the part and is issued by the core service provider as described in CX-0010 [23]. BPN is an identifier for business partners known in data spaces that represent an organization or one of its organizational parts from foundation to closure. It also serves as the unique identifier for the data space participants and is issued by the operating company. The BPN functions as a blueprint for similar data spaces that follow the Catena-X concepts, thereby promoting interoperability between these data spaces. It is used in the data model of the Business Partner Data Management (BPDM) system as a primary key for business partners (Golden Records) and to build references between the individual business partner types.

BPN is a structured 16-character identifier used to uniquely identify business partners. It always begins with the uppercase prefix "BPN", marking it explicitly as a Business Partner Number. The fourth character in the sequence denotes the type of business partner and is represented by one of three uppercase letters: 'L' for legal entity, 'S' for site, and 'A' for address. Following this, ten alphanumerical uppercase characters make up the entity section, ensuring global scalability and allowing for the identification of approximately 3.6 quadrillion distinct business partners per type. The final two characters serve as check characters, implementing error detection using a verification algorithm based on ISO/IEC 7064:2003 MOD 1271-36. The full BPN format can be described by the regular expression: BPN[LSA][A-Z0-9]{10}[A-Z0-9]{2}.

BPN qualities can be listed as follows:

1. BPN is a globally unique identifier, with which an organization or one of its organization parts have exactly one identifier world-wide, so that no two organizations or organization parts have the same identifier, and no two identifiers stand for the same organization or organization part
2. BPN is a world-wide scalable identifier, that can identify all organizations and their organization parts on a global scale
3. BPN is a semantically enriched identifier, that includes the type of the business partner it identifies
4. BPN is an interoperable identifier, which is used cross-application and cross-organization in all conceivable business contexts
5. BPN is a time-dependent identifier, that has a validity for which it identifies an organization or one of its organization parts in the (legally) defined limits of their existence
6. BPN is a stable identifier, which never changes structurally, never ceases to exist and never is reassigned, even if the organization or one of its organization parts ceases to exist

7. BPN is a human-readable identifier, that is comparable to a telephone number or a postal code
8. BPN is an identifier, which inherently supports error detection

Additionally, BPNL is a legally secure identifier, that enables the unambiguous identification of contracting parties, ensuring a reliable foundation for legally binding data exchange contracts.

4.2. Material Identity Credentials

To decide for material identification, firstly an overview of existing material identification approaches across various data spaces, standards, and solutions are generated. Identifiers vary by industry, region, and application, with examples such as UUIDs in Catena-X, GS1 codes (GTIN), and DID-based identifiers in Battery Pass and IDSA projects. Frameworks like Manufacturing-X and the Asset Administration Shell (AAS) support multiple identifier schemes, including IRI, IRDI, DOI, and decentralized methods.

The Chem-X framework introduces a hierarchical structure for material information across three levels of granularity: Model, Batch, and Item. The Model Level captures general product data, such as formulation and certifications, with low update frequency and is suitable for compliance and sales. The Batch Level addresses specific production lots, including raw material sources and lab results, and supports quality assurance and traceability. The Item Level refers to individual units, with detailed tracking data for logistics and recycling, used mainly for high-value or critical products. JTC'24 Digital Product Passport – Unique Identifiers standard (prEN18219, Clause 5.2) mentions that the material identification links must take this hierarchy into account. The details of the Material IDs and DPP IDs used in existing projects, along with a draft DPP ID proposal for Chem-X, are available on the Chem-X Wiki.

5. Verification Processes

This section introduces the verification processes foreseen in Chem-X. Membership verification is based on Catena-X membership verification process for the companies to register and submit identifier data. DPP verification summarizes a generic process, which uses decentralized identifiers and verifiable credentials to ensure traceable product data. Finally, the section details how certificates within DPPs are verified based on issuer authenticity, signature integrity, validity periods, and compliance with cryptographic and semantic standards.

5.1. Membership Verification Process

To initiate participation in the Catena-X ecosystem, companies must complete a membership verification process. This begins with the submission of company data through the Catena-X portal, operated by Cofinity-X. During this registration, the company submits information such as the legal entity name, VAT or tax identification number, globally recognized identifiers such as DUNS or LEI, address and country of operation, as well as the contact person's email address.

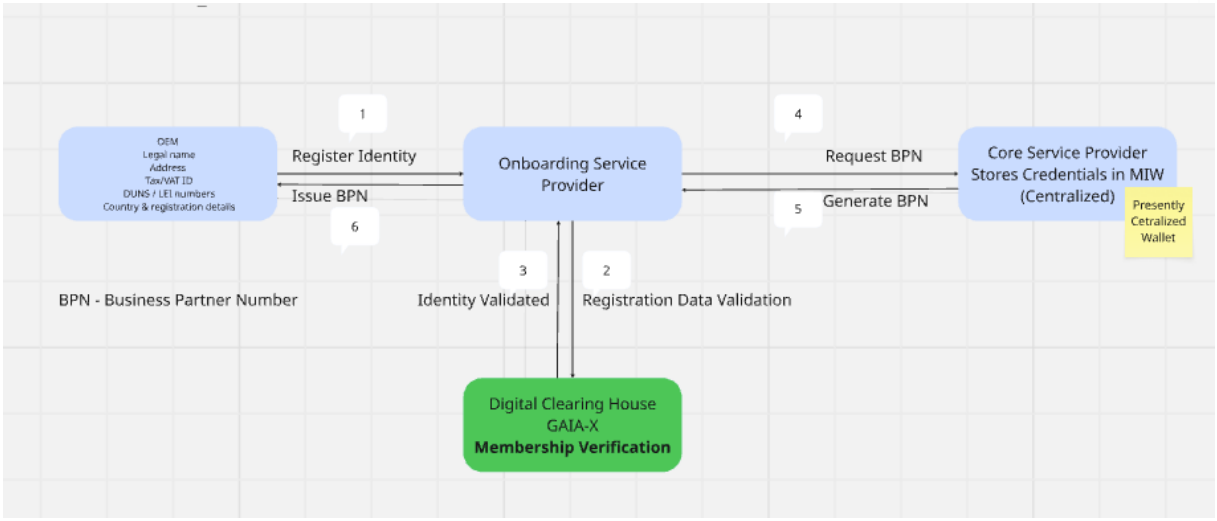

Figure 3 - Catena-X Membership Verification Process

The validation of this submitted information is conducted by Onboarding Service Providers (OSPs) within the Catena-X framework. These OSPs make use of established GAIA-X trusted frameworks to confirm the legitimacy of the registering company. Trusted data sources such as the Global Legal Entity Identifier Foundation (GLEIF) for LEIs, Dun & Bradstreet databases, and the European VAT Information Exchange System (VIES) are used to cross-check and verify submitted identifiers and registration data. This ensures that only legitimate, identifiable legal entities are onboarded into the network.

The role of GAIA-X in the verification process within ecosystems like Catena-X is to provide the framework and principles for trusted, sovereign, and interoperable data exchange. While GAIA-X is not a platform or service provider itself, it defines the rules, architecture, and trust mechanisms that participants must follow to be considered verifiable and compliant.

5.2. DPP Verification Process

The Digital Product Passport (DPP) is a regulatory instrument and data structure designed to enhance product transparency and compliance. As defined in the ESPR and related frameworks such as the Battery Regulation, the DPP must support lifecycle traceability, secure access and interoperability across supply chains.

Among other identifier options, DPPs may use a decentralized architecture based on W3C Decentralized Identifiers (DIDs). Each product is assigned a globally unique DID, which is generated and anchored in a secure digital wallet using standardized methods such as DID:web. This DID resolves to a DID Document containing the public keys and service endpoints necessary for verifying associated credentials and enabling interaction with the data holder. Based on this identity, manufacturers, suppliers, or authorized third parties issue credentials, each representing a distinct claim about or property of the product—such as carbon footprint, recycled content, or safety data. A DPP can be discovered by scanning a data carrier, such as a QR code or RFID tag, which encodes a reference to a DPP with a specific product identifier DID. Retrieval follows a decentralized process, ensuring that DPPs can be retrieved securely from the economic operator's DPP system and without contacting a central registry.

DPP verification concept for Chem-X is first and foremost required to build trust in the data content. Each verifiable credential retrieved from the DPP is independently verified by validating the digital signature against the public key in the issuer's DID Document and verifying issuer legitimacy via a trusted Issuer list. Regarding semantics, schema conformity must be ensured using a shared vocabulary. Finally, checking revocation and validity status from credential registries is required.

Despite the technical maturity of decentralized identifiers and verifiable credentials, several critical gaps remain in the governance and operational model of DPP verification, especially within the context of Catena-X. First, there is currently no unified trusted list of auditors or credential issuers, making it difficult for verifiers to assess the legitimacy of data sources. This absence undermines the trust chain that DPP verification depends on, particularly for third-party attested credentials. Second, there is no formalized set of criteria defining who qualifies as a “trusted auditor” or issuer. Without clear qualification thresholds, conformance requirements, or onboarding procedures, the concept of "trust" becomes vague and unverifiable. Third, verifiers lack access to a standardized framework or policy for validating data content, beyond cryptographic signature checks. In other words, even if the signature is valid, it is unclear what data quality, completeness, or semantic alignment standards must be met to treat a credential as trustworthy—this constitutes a major unresolved issue on the "data trust" layer. Finally, the ownership of these trust lists and qualification frameworks within Catena-X remains undefined. Ideally, such responsibilities would reside with the Catena-X Association or a designated trust governance body, to ensure neutrality, updateability, and long-term stewardship.

5.3. Certificate Verification Process

Certificates as part of a DPP are data elements (single valued or multivalued) or collections thereof with a defined value data type and regarded as documents. Structured JSON data such as W3C Verifiable Credentials and XML schema defined value data types shall be supported [24]. These credentials are digitally signed using the issuer’s private key, adhere to the W3C VC Data Model in either JSON-LD or VC-JSON serialization formats and include essential product identifiers as well as metadata for versioning and regulatory compliance.

Verification of certificates must provide means to a verifier to check the following criteria associated with the certificate:

- The authenticity of the *certificate issuer* can be verified against a list of trusted issuer identifiers
- The authenticity and integrity of the *certificate* can be verified against a signature or data integrity proof over that certificate
- Temporal constraints on the validity period time for that certificate are satisfied (if available within the certificate)
- The enclosing data element contains a valid DictionaryReference to the unique idéntifiér of the data point specification defined in the repository/data dictionary
- Signature schemes and cryptographic algorithms used to secure the certificate comply with the ecosystem-wide policy
- Information about the revocation status of the certificate can be verified if available and results at least in a boolean status revoked/not-revoked

6. Recommendations

To enhance the Chem-X verification framework and to address existing limitations across identity management, credential issuance, and validation, several recommendations have been derived from the technical review and stakeholder consultations inside Chem-X TP2 working group. These recommendations aim to strengthen the alignment of Chem-X with the upcoming European digital identity regulations, the requirements of the chemical industry for a scalable dataspace solution, and interoperability principles. The following recommendations have been derived from the verification components review:

Dataspace Onboarding Processes: The onboarding process will be extended with *bring-your-own-wallet* (BYOW) scenarios. This is not a replacement for the existing Catena-X onboarding and wallet management, but an addition. Aligning onboarding flows with EUBW requirements is also another essential topic and Chem-X aims to propose an onboarding concept that encompasses EU company certificates and Legal Person Identifiers aligned with the upcoming regulations.

Presentation Flows: The existing presentation flows in reviewed projects, such as Catena-X, currently does not support OpenID-based protocols. The absence of OpenID compatibility has the potential to limit the integration with the EUBW and for business-to-government (B2G) use cases. To address this gap, OpenID support for the credential presentation mechanisms will be discussed for Chem-X, thereby enabling credential exchange with public authorities and other trust frameworks aligned with eIDAS 2.0.

Protocols in Dataspace: As a full scope discussion of the existing protocols was not completed during this review, it is recommended that the protocol distinctions for credential flows (inbound vs. outbound) within the dataspace will be defined separately to ensure compatibility with internal data exchange processes and external regulatory systems.

Trusted Issuers: As mentioned in the onboarding process, the role of Legal Person Identifiers (LPID) and EU Company Certificates (EUCC) has been acknowledged as critical for future use of Chem-X dataspace. Under eIDAS 2.0, the issuance of such credentials is to be governed by designated supervisory authorities listed in national trust lists of Qualified Trust Service Providers (QTSPs). In accordance with this framework, Chem-X should establish a trusted issuer registry aligned with LPID and EUCC standards to enable verifiable trust across both B2B and B2G use cases.

Multi-Issuer Challenges: To address the growing demand for decentralized and flexible credential ecosystems, it is recommended that Chem-X adopts a multi-issuer verification model. In line with emerging developments within Catena-X, this includes supporting multiple Core Service Providers, enabling participants themselves to act as credential issuers, and validating verifiable credentials issued by external parties. The integration of multiple clearing houses and external issuers is particularly relevant for supply chains involving regulatory attestations and cross-domain trust scenarios.

Wallet Certification Schemes: The need for a wallet certification scheme has been identified as a relevant area for future work together as the "bring-your-own-wallet concept" will allow multiple wallet providers to become part of the dataspace. It is recommended that wallet certification criteria for dataspace participants are provided inside Chem-X, based on emerging Catena-X compliance checklists and security assurance expectations.

Interoperable Trust Frameworks: In line with broader interoperability objectives, Chem-X should aim to align its trust framework both with existing architectures such as Gaia-X, EUBW, and Catena-X; and the upcoming European regulations such as eIDAS2.0. Ensuring such convergence will promote scalability and regulatory harmonization.

7. Conclusions

The Chem-X project aims to define a verification architecture for digital product data sharing in the chemical sector, drawing on insights and lessons learned from Catena-X and other related initiatives. Central to this effort is the verification of data sources, claims, and credentials, which serves as a key enabler for building trust, ensuring regulatory compliance, and achieving interoperability among supply chain actors.

To create a guideline for Chem-X verification concept, this document reviews the Catena-X verification model, which defines a decentralized credential issuance and verification framework governed by a central policy authority. It enables fine-grained trust decisions through the use of verifiable credentials for business identity, product data, and compliance claims. In the context of Chem-X, a flexible and interoperable verification architecture is required to support a diverse range of actors and use cases, with a particular emphasis on product identity and regulatory compliance, especially for tracking hazardous materials and safety-related information. The document also examines verification approaches from projects such as Battery Pass, CIRPASS, PACT, UNTP, and Energy Data-X, highlighting transferable mechanisms including credential issuance practices, trust anchor models, and defined identity roles. Notably, Energy Data-X provides a legally grounded, role-based credentialing system suitable for regulated environments, emphasizing strict compliance and wallet separation.

This review is used as a foundational work to develop the Chem-X verification concept, including both company identifier and certificate verification and product-level verification. Using the Cofinity-X Playground and standardized technologies such as W3C verifiable credentials, practical tests will be conducted to evaluate existing capabilities and identify technical gaps. Key outcomes are expected to include user journey definitions, test protocols, and a joint set of recommendations to guide the integration of business identity, certifications, and product attributes into a comprehensive verification framework. In this context, the Chem-X Demonstrator requirements for use cases involving credential exchange are to be taken into account. The final step involves the formulation of decision points and proposals, potentially feeding into ongoing discussions in expert groups such as those related to SSI, eIDAS, and Digital Product Passports.

To enhance the verification concept for Chem-X based on the identified recommendations, a structured methodology will be applied following the steps outlined in the process diagram. First, the current implementation status of each recommendation area will be assessed to establish a clear baseline. Subsequently, alternative options from the state of the art will be identified and evaluated, including a justification of their relevance. This will be followed by a gap analysis that considers emerging regulatory and technical requirements such as JTC 24, eIDAS 2.0, the EUBW framework, and sector-specific chemical regulations. Based on these insights, relevant use cases will be defined to ensure the enhanced concept addresses real-world verification needs.

In the final decision-making step, legal considerations must be explicitly incorporated to ensure that the developed concept aligns with relevant regulatory frameworks and liability structures. Moreover, coordination with external stakeholder groups is essential for broad acceptance and

reuse. This includes ensuring alignment with Catena-X working and expert groups, as well as planning how the concept will be presented for validation and potential adoption. Additionally, it is aimed that our recommendations are included in future Catena-X and Tractus-X release planning, and relevant initiatives such as Manufacturing-X, particularly its topic group on business partner identification, should be targeted to promote the developed concept and gather cross-industry feedback.

8. References

[1] European Union. Regulation (EU) 2024/1781 of the European Parliament and of the Council of 13 June 2024 on establishing a framework for a European Digital Identity. Official Journal of the European Union, L 178, 13.6.2024, pp. 1–58. Relevant articles: Art. 5(12), Art. 12(5)(c).

[2] Allen, C. (2016). Self-sovereign identity principles. [Online]. Available: https://github.com/ChristopherA/self-sovereign-identity/blob/master/self-sovereign-identity-principles.md

[3] Soltani, R., Nguyen, U. T., & An, A. (2021). A Survey of Self-Sovereign Identity Ecosystem. *Security and Communication Networks*, 2021, 1-26. https://doi.org/10.1155/2021/8873429.

[4] Yildiz, H., Küpper, A., Thatmann, D., Göndör, S., & Herbke, P. (2022). *A Tutorial on the Interoperability of Self-sovereign Identities*. TU Berlin, Service-centric Networking, and Telekom Innovation Laboratories.

[5] Data Spaces Support Centre (DSSC). (2025). Identity and Attestation Management. Retrieved from https://dssc.eu/space/bv15e/766068449/

[6] International Organization for Standardization (ISO). (2020). ISO/IEC 17000:2020 - Conformity assessment — Vocabulary and general principles. Retrieved from https://www.iso.org/standard/73029.html

[7] Catena-X Association. (2025). Operating Model. Retrieved from How: Data Space Governance | Catena-X - Library

[8] Catena-X Consortium. CX-0135 Business Partner Company Certificate Management. Version 1.0, 2024. Available at: https://catenax-ev.github.io/docs/next/standards/CX-0135-CompanyCertificateManagement

[9] Catena-X Consortium. CX-0003 Semantic Aspect Meta Model (SAMM). Version 2.0, 2024. Available at: https://catenax-ev.github.io/docs/standards/CX-0003-SAMMSemanticAspectMetaModel

[10] Gaia-X Association. Digital Clearing House. 2024. Available at: https://gaia-x.eu/services-deliverables/digital-clearing-house/

[11] Catena-X Association. (2023). Enablement Services Whitepaper. Retrieved from https://catena-x.net/fileadmin/_online_media_/231006_Whitepaper_EnablementServices.pdf

[12] Gaia-X Association. Digital Clearing House. 2024. Available at: https://gaia-x.eu/services-deliverables/digital-clearing-house/

[13] European Commission. (2023). Regulation (EU) 2023/1542 of the European Parliament and of the Council of 30 July 2023 concerning batteries and waste batteries. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1542

[14] Battery Pass Consortium. (2024). Battery Passport Technical Guidance. Retrieved from https://cirpassproject.eu/wp-content/uploads/2024/05/D3.2v1.9.pdf

[15] CIRPASS Consortium. Cirpass: Digital product passport initiative. https://cirpassproject.eu/, 2024.

[16] Partnership for Carbon Transparency (PACT). PACT Methodology and Network, 2024. World Business Council for Sustainable Development. Available at: https://www.carbon-transparency.org/pact-methodology

[17] PACT. (2023). PACT Framework: Building on existing frameworks and standards to provide guidance on accounting and verification.

[18] United Nations Development Programme (UNDP). (n.d.). UNTP Specifications – Federated Blockchain for the Base of the Pyramid (FBB45F). Retrieved from https://spec-untp-fbb45f.opensource.unicc.org/

[19] Energy Data-X. (2023). TAP 1.5 – Einführung in Vertrauensmodelle für Digitale Identitätsökosysteme

[20] ENTSO-E, EFET & ebIX®. (2022). The Harmonised Electricity Market Role Model – Version 2022-01. ENTSO-E AISBL, European Network of Transmission System Operators for Electricity.

[21] W3C. (2021). Verifiable Credentials Data Model v1.1. Retrieved from https://www.w3.org/TR/vc-data-model-1.1/

[22] W3C. (2023). Verifiable Credentials Data Model v2.0. Retrieved from https://www.w3.org/TR/vc-data-model-2.0/

[23] Catena-X Automotive Network e.V. (2024). CX-0010 Business Partner Number.

[24] DIN EN 18223. Digital Product Passport – System interoperability; German and English version prEN 18223:2025. Deutsches Institut für Normung (DIN), 2025.

[25] CEN/CLC/JTC 24. (2025). Digital Product Passport – Unique Identifiers (prEN 18219:2025, Draft for Enquiry). CEN-CENELEC Management Centre, Brussels.

9. Glossary

All definitions used in this deliverable are aligned with the terminology provided in the Chem-X - Glossary.