MANUFACTURING-X
GUIDANCE BOARD

IDENTIFICATION GUIDELINE OF PARTICIPANTS WITHIN AND CROSS DATA SPACES

Insights from differerent Manufacturing-X projects

Manufacturing-X
Guidance Board

IMPRINT

Publisher

Manufacturing-X Guidance Board

Project Office Manufacturing-X

Open Industry 4.0 Alliance Implementation GmbH

Willy-Brandt-Platz 6

81829 Munich, Germany

Version History

[Month Xth, 202X – Version 1.0 (First Release)]

Authors

Ingolf Gehrhardt (HTW Dresden, Semiconductor-X)
Henning Berg (Fraunhofer IPK, Aerospace-X)
Thomas Obermeyer (Catena-X)
Nikolaos Saklampanakis (Fujitsu)
Nico Braunisch (TU Dresden, Fluid 4.0)
Alfred Barnard (ifak, Robot-X)
Niklas Schulte (Fraunhofer ISST, Catena-X)
Marcel Ruland (Cofinity-X)
Steffen Turnbull (dlr, RoX)
Christian Lahmer (SAP SE, Factory-X)

Index

Scope of the Document

This document is a guideline for participant identification within and across Data Spaces, primarily based on Catena-X/Manufacturing-X practices. In this document we distinguish between three fundamental concepts:

Term	Definition	Example
Identity	The inherent properties and characteristics that make an entity unique	A natural person or a legal person with its name, registration, legal form, operational history,
Identification	The **act or process** of establishing or assigning an identity	Verifying company registration, credential issuance, authentication processes
Identifier	A **symbol/code/pattern** that references an entity/identity	Tax ID, DUNS number, DID, email address, passport number, local sport membership number

It cover the two identity dimensions:

User Identity (natural person): Portal authentication using OpenID Connect with federated Identity Provider (IdP)support, enabling Single SignOn (SSO) and role-based authorization.

Organization Identity (legal person): Built on Self-Sovereign Identity (SSI) using W3C standards (Decentralized Identifier (DID) and Verifiable Credentials). Organizations receive membership credentials linked to business identifiers for secure data exchange via Decentralized Claims Protocol (DCP) and Eclipse Data Space Connector (EDC).

Key topics include onboarding processes (currently manual, transitioning to digital EU organization identities (EU Org ID), revocation mechanisms via trust lists, cross-Data Space credential reuse ("join once, use everywhere"), and use cases like digital company certificates and product passports *e.g.* Digital Product Passports (DPP) and Product Carbon Footprints (PCF). The document also outlines trust governance, multi-issuer scenarios, and references Catena-X standards, though several sections remain incomplete (Japan, China, US, power of attorney).

Introduction: Identity has Different Flavors

In the context of data spaces, identification (claiming an identity), authentication (proving that identity), and authorization (determining access rights) form a sequential access control chain that exists across multiple dimensions. These three distinct but interdependent processes are not only present within a single data space, covering entities such as organizations, users, machines, products, and countries or regions, but also become more complex when multiple data spaces are combined. When data spaces are interconnected, their respective identification, authentication, and authorization mechanisms must be integrated and made interoperable, adding further layers of complexity to managing digital identities and access rules.

User Identity

In certain data spaces, there is need for centralized portals where participants need to authenticate efficiently and securely. Such portals are typically hosted by a central operator responsible for managing access to services.

To facilitate seamless and secure user authentication, the operator can provide an IdP as part of the portal infrastructure. This IdP serves as a central authentication authority, allowing data space participants to create and manage user accounts directly within the operator's system. Alternatively, to enhance flexibility and interoperability, the operator can enable an IdP federation model. In this approach, data space participants integrate their existing IdPs with the central portal using standard protocols such as OpenID Connect, or Open Authorization Version 2.0 (OAuth 2.0). This way, authentication requests are delegated to each participant's trusted IdP, maintaining local control over user credentials and authentication policies.

By supporting both direct user management and federated authentication, the portal operator addresses the diverse needs of data space participants. This enables efficient, secure access for users from different organizations, while ensuring compliance with each participant's security requirements and identity management strategies.

OpenID Connect (OIDC)

OpenID Connect (OIDC) is an identity layer built on top of the OAuth 2.0 protocol. It enables applications, known as Relying Parties (RPs), to authenticate users through a trusted IdP. OIDC simplifies the authentication process by allowing users to log in with an existing account from a third-party provider

Federated Identity Provider

In a federated IdP setup, authentication responsibilities are distributed across multiple domains or organizations. This setup enables seamless SSO across different services and applications, improving user experience and reducing the need for multiple credentials. The federated IdP acts as a bridge between the RP and the user's IdP, facilitating the exchange of authentication tokens and user identity data.

Authorization Checks

Authorization checks based on OpenID Connect (OIDC) leverage the identity and access tokens issued during the authentication process to control user access to resources. After a user is authenticated through OIDC, the IdP issues a token containing claims that describe the user's identity and roles.

When the user attempts to access a resource, the application or service performs an authorization check by validating the token and examining its claims. These claims, such as roles or permissions, are then compared against the required access policies to determine if the user is authorized to perform the requested action. This approach ensures that only users with appropriate privileges can access or modify specific resources, enhancing security and enforcing access control in a standardized manner.

Organization Identity

Organization identity in Manufacturing-X are built on the concept of SSI, leveraging W3C standards such as DID and Verifiable Credentials (VC). This approach empowers organizations to proof their identity within and across data spaces.

Membership is evidenced through a VC issued by a trusted authority, which functions as the current trust source. Unlike traditional models that rely on a centralized IdP, SSI and DIDs allow organizations to authenticate and interact within the data space ecosystem without surrendering control of their identifying information. As a result, this decentralized model enhances privacy, flexibility, and interoperability among data space participants.

Decentralized Identifier (DID)

DIDs are a foundational component of modern digital identity systems, particularly within data spaces and federated ecosystems. They provide a standardized way to create and manage digital identities that are independent of centralized authorities or registries. Unlike traditional identifiers tied to specific platforms or organizations, DIDs are cryptographically verifiable, persistent, and controllable by their owners, enabling secure and interoperable identity management across different systems and trust frameworks.

The DID is a technical identifier that relates to a DID Document, which contains public key material. DIDs allow the exchange of key material without changing the identifiers. Hence, DIDs can change during the lifetime of a membership, for example, also when another trust infrastructure is chosen. Currently, DID:web is used. This DID method using HTTPS-based domain hosting for Documents containing verification keys and service endpoints associated with a DID. It serves as a pragmatic bridge for organizations to adopt decentralized identity by using their established web infrastructure and reputation. However, with upcoming EU regulations expected to define organization identities in the near future, further changes are anticipated.

Persistent identifiers

DIDs are typically long-lived, but not persistent, and may in some cases get reassigned (similar to a phone number). Every member of a Data Space therefore receives an additional persistent identifier. An example thereof is the Business Partner Number (BPN) used in Catena-X. Other options include the LEI (Legal Entity Identifier) or various country-specific identifiers, provided they are truly persistent and may not be reassigned (even after a legal entity ceases operation or otherwise deregisters).

A verifiable credential binds the logical organization number to the DID. The DID also provides access to the cryptographic material that every data space member needs in order to prove, for example, possession of the membership.

Membership Credentials

Leveraging Organization Identity to Exchange Data

By leveraging the verifiable credential exchange described in the Decentralized Claims Protocol (DCP)[1], Company 1 can securely access the allowed data from Company 2, ensuring that both parties comply with agreed-upon data-sharing agreements and governance standards (described in the Data Space Protocol[2] implemented by the EDC). This mechanism facilitates controlled and secure data collaboration across different organizations within a trusted data space.

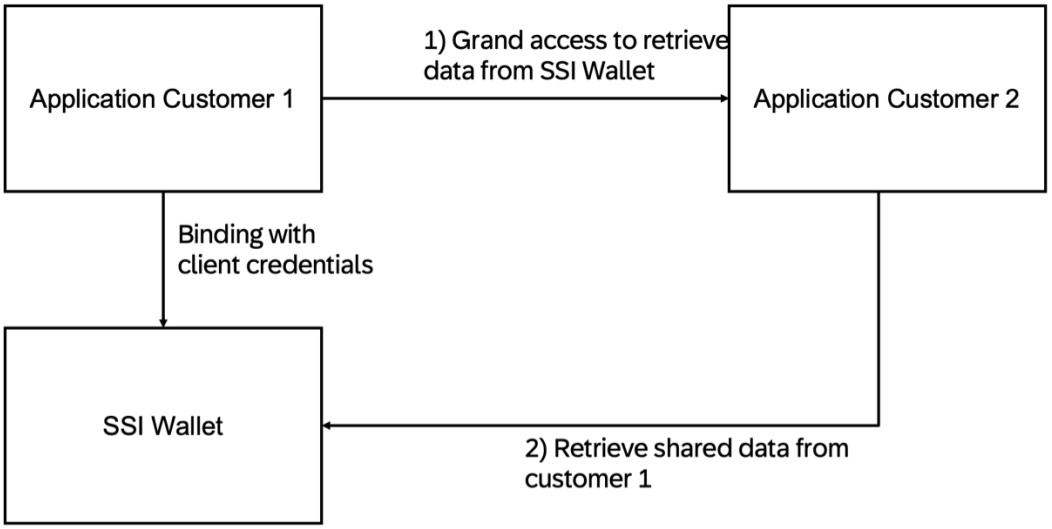


Figure 1: Data Exchange with SSI

The following figure describes how Verifiable Credentials (VC) are presented based on DCP to proof the identity of the Data Space participants. The (DCP) is designed to address the problem of resolving Verifiable Presentations (VPs) when they cannot be passed as part of a client request.

[1] https://eclipse-dataspace-dcp.github.io/decentralized-claims-protocol
[2] https://eclipse-dataspace-protocol-base.github.io/DataspaceProtocol/

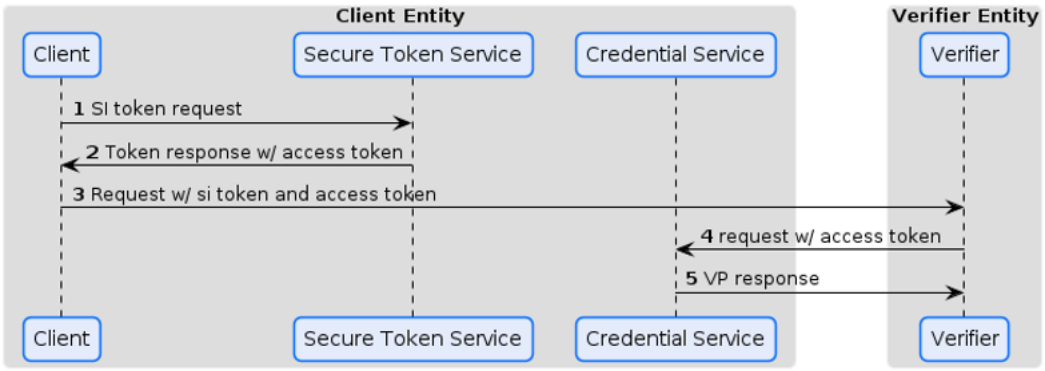


Figure 2: Presentation flow of the Decentralized Claims Protocol

Receiving Verifiable Credentials

Data space participants receive verifiable credentials (VCs) as part of their onboarding and ongoing participation in the data space. Operators are responsible for issuing these credentials, such as membership credentials, which serve as proof of the participant's verified status and rights within the ecosystem. The transfer of these VCs from the operator to the participant's organization wallet is carried out in accordance with the Decentralized Claims Protocol (DCP). There are two primary methods for this exchange: either the operator proactively pushes the credential directly to the participant's wallet, or the participant initiates the process by pulling the credential from the operator's system.

Leveraging Organization Identity for Onboarding

Currently, the initial onboarding of an organization to a data space requires manual paperwork and cannot yet leverage digital organization identities, as the necessary EU regulations and the implementation of digital identity wallets are still in progress. For example, onboarding to a data space like Catena-X is presently a manual and paper-based process. At the end of this process, an organization can obtain an SSI wallet. We expect that in the future most of the organizations have already a wallet. If this is not the case a wallet may be provided.

Upon successful onboarding, the new participant receives their credentials delivered to their wallet. For subsequent onboarding to additional data spaces, this identity credential can be reused to simplify the process, since all "*Know Your Customer*" procedures have already been completed. Looking ahead, this process is expected to become much more streamlined. It is anticipated that by 2027, all EU organizations will be equipped with a government-provided digital identity. This identity credential can then be used for onboarding without any further paperwork, and at the conclusion of the process, a membership credential will be issued to the organization.

Revoking a Participant and Data Space Operators

In a data space the trust and control over operators are maintained through a trust list. All operators must be included in this trust list, which is distributed and managed by an association like Catena-X. Should it become necessary to exclude an operator from the data space, the association will remove the operator's DID from the trust list. This action

immediately invalidates all verifiable credentials issued by that operator, rendering them unusable for identification or access.

For data space participants, disabling access is managed at the operator level: the operator can revoke a participant's membership credential, blocking the participant from further participation in the data space. In rare cases where an operator must revoke their private key (for example, due to compromise), all verifiable credentials previously issued with that key are rendered invalid and must be re-issued to preserve the integrity and security of the data space. This layered approach enables precise and rapid exclusion of either entire operators or individual participants, ensuring robust access control and fostering trust in the data ecosystem.

Usage of Verifiable Credentials (VCs) Issued from One Data Space to Onboard to Another Data Space

Participants in multiple manufacturing value chains (e.g., automotive, aerospace) face significant overhead in onboarding and managing identities for each Data Space they join. This friction hinders the networking effect of Manufacturing-X. The solution outlines the use of W3C Verifiable Credentials (VCs) and a specialized "multi-Data Space identity wallet." This will enable a "join once, use everywhere" paradigm.

Credential Governance

Trust Frameworks such as GaiaX play a pivotal role in enabling interoperable trust between different Data Spaces by defining a harmonized set of rules, assurance levels, credential formats, and compliance requirements. The GaiaX Trust Framework specifies how participants, services, and identities must be verified, which credential issuers are accepted, and which governance processes ensure ongoing compliance. GaiaX Digital Clearing Houses (GXDCH) operationalize this framework by acting as neutral trust intermediaries: they validate organizational attributes, check the authenticity of Verifiable Credentials, and confirm compliance with GaiaX policies. Through their verification services and trust lists, GXDCHs provide machinereadable and globally consistent trust signals that can be consumed by any compliant Data Space.

Discuss the role of trust frameworks like Gaia-X and the function of Gaia-X Digital Clearing Houses (GXDCH) in anchoring trust between different Data Spaces.

Policies

Policies define the ways in which actors are allowed to use digital assets. In the context of data spaces and beyond, policies are often formulated in the W3C Open Digitial Rights Language (ODRL)[3]. ODRL standardizies policies into a machine-readable format that is used with permissions, prohibitions and obligations. In the context of decentrazied identities, policies typically address who is allowed to issue which type of credentials in the Data Space and thus enables the credential verification for the Data Space participants.

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

As mentioned in the previous section, certain credential types are general-purpose Data Space credentials, such as Membership Credentials.

Trust Anchor / Trust Lists

Trust anchors are the backbones of the decentralized identity infrastructure. When building decentralized trust infrastructures under SSI principles, ideally there should be no trust root, but rather identification should happen on peer-to-peer level. Figure 3 shows the synchronization of trust list across Credential Service Provider (CSP).

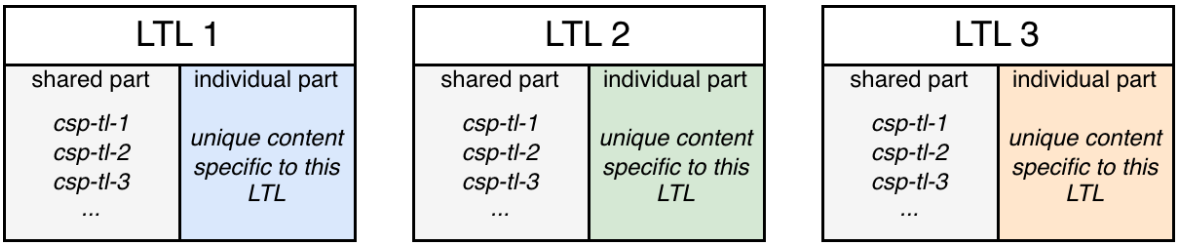


Figure 3: Examplary Lists of Trusted Lists

To ensure the trust lists are updated across the individual CSPs, …

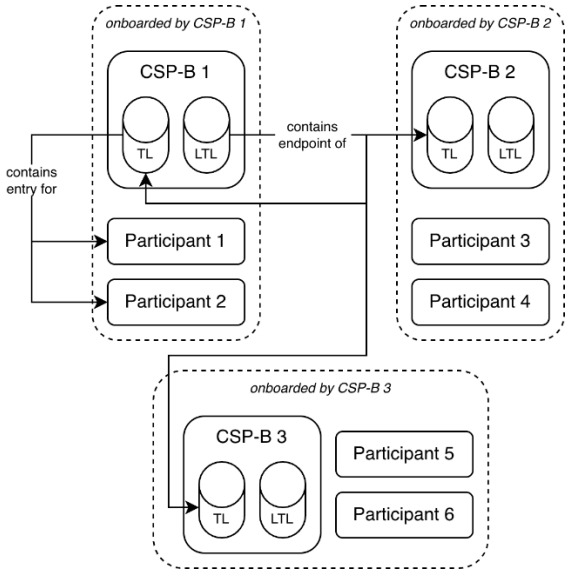
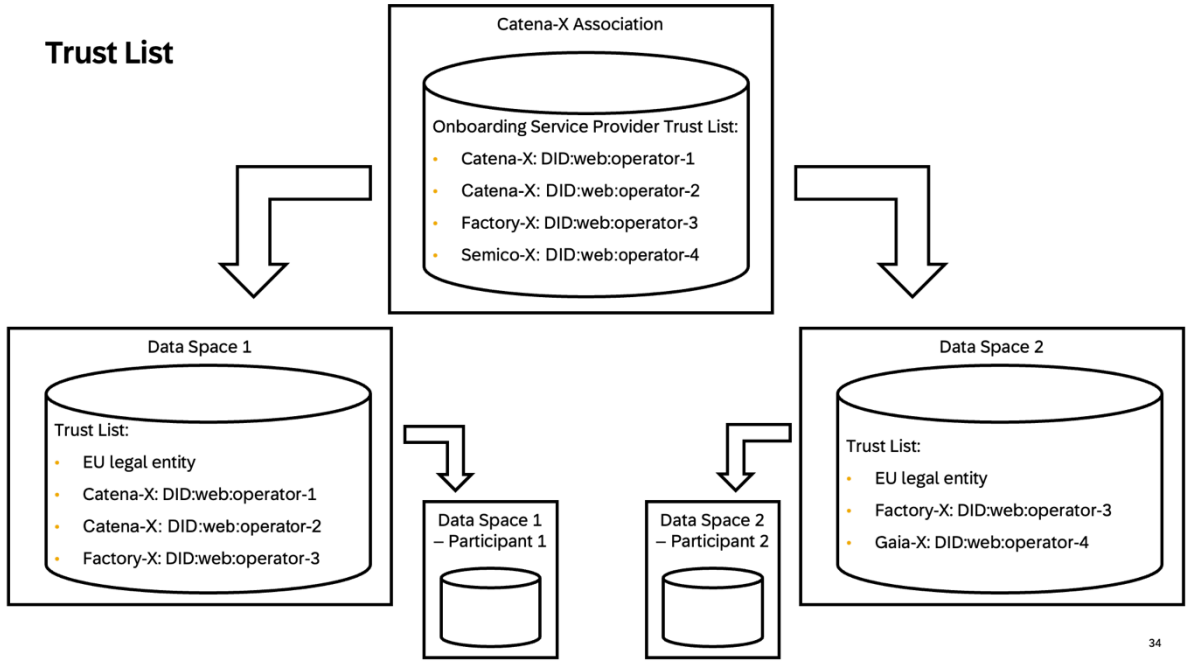


Figure 4: Synchronization of Trust Lists

Establishing Cross-Data Space Trust

Establishing cross–data space trust relies on the ability to recognize and accept verifiable credentials (VCs) issued by trusted parties across different data spaces. In this model, credentials may originate from issuers inside a data space or from authoritative external entities such as government bodies or GLEIF. Each data space maintains its own list of trusted issuers, defining who is allowed to assert identities or attributes for onboarding and interaction. To support interoperability, the Catena-X Association will provide a global trust list that includes all data spaces and their onboarding service providers. Individual data spaces can use this global list as a foundation and then extend or restrict it based on their own policies

and governance rules. With this shared trust framework in place, organizations can seamlessly onboard to a data space using any credential that is recognized as trustworthy—significantly simplifying access, reducing manual verification, and enabling scalable, interoperable data ecosystems.



Cross-Data Space Trust ensures that participants from one Data Space can seamlessly interact with participants and services in another while maintaining consistent assurance levels. To enable this, Data Spaces must rely on interoperable trust frameworks that define how identities, credentials, and governance rules are recognized across ecosystem boundaries.

Power of Attorney

Power of Attorney (PoA) is essential in Data Spaces whenever legal, administrative, or technical actions must be performed on behalf of an organization. Typical scenarios include onboarding, wallet and connector administration, contract acceptance, issuing or presenting Verifiable Credentials, and compliance or audit processes. Since these tasks are often carried out by individuals or systems that are not the organization's legal representative, a PoA serves as a verifiable delegation credential, ensuring that only authorized entities may act for the company. PoA establishes the root of trust during onboarding by linking real-world corporate authority to digital identities, enables delegated administration in large or distributed organizations, and ensures cross-Data Space interoperability through standardized, machine-verifiable formats. Without a verifiable digital PoA, a Data Space cannot guarantee non-repudiation.

Multi-OpCo / Multi-Issuer Enablement

A Data Space is operated by one ore multiple “Operating Company” (OpCo). Although currently most data spaces operate under a single OpCo, by design it is possible, and potentially also desirable, to have multiple OpCos governing a data space. When onboarding new participants to the data space, the onboarding process should ensure that a participant can only have one Membership Credential and thus requires a unique identification of the participant. Onboarding at one OpCo will be sufficient and trusted in the complete data space across multiple OpCos.

In a Multi-OpCo setup, each OpCo is authorized to issue Membership Credentials and operate trust services, provided it is listed on a commonly governed Trust List maintained by the Data Space Authority. To avoid duplicated or conflicting identities, onboarding processes must ensure that each participant receives exactly one Membership Credential, independent of the OpCo performing the onboarding. This requires a shared, authoritative registry of participants and a harmonized process for identity proofing.

Furthermore, Multi-OpCo ecosystems require synchronization of Trust Anchors, Trust Lists, and issuer metadata across all operators. This ensures that credentials issued by one OpCo can be verified by any other and by all connectors, wallets, and participants in the Data Space.

By enabling Multi-OpCo and Multi-Issuer models, Data Spaces achieve true federation: operational redundancy, regional autonomy, scalability across industries, and interoperability with other Data Spaces that follow similar governance frameworks.

Example Use Case Credentials

Company Certificates

An organization identity wallet enables companies to securely receive, store, and manage digital certificates issued to them by trusted third parties, such as auditors or certification bodies. For example, in the future, auditors like ISO may issue certifications, such as ISO 9001 or ISO 27001, as verifiable credentials, which can then be stored directly in the organization’s digital wallet. When engaging with buyers, suppliers can easily present these certifications upon request, providing transparent and tamper-proof evidence of compliance with required standards. This streamlined approach not only eliminates the need for cumbersome manual document exchanges but also enhances trust between business partners. Furthermore, such verifiable certificates could be automatically requested and validated during EDC communications or contract negotiations, allowing for real-time verification and significantly accelerating supply chain interactions and onboarding processes.

Attest Digital Product Passports (DPP) and Product Carbon Footprints (PCF)

An organization identity wallet plays a pivotal role in the secure management and exchange of digital product passports (DPPs) and product carbon footprint (PCF) credentials. A supplier can request an attestation for their DPP or PCF data by submitting it to an independent auditor for verification. The auditor reviews the underlying information such as product composition, lifecycle details, or carbon footprint calculations and, if the data is validated, issues a corresponding Verifiable Credential (VC) to the supplier’s wallet. The supplier can share the

verified DPP or PCF VC with buyers, providing proof of product compliance, sustainability, or other key attributes.

In certain scenarios, organizations may also be permitted to issue self-attested DPPs directly from their wallet, facilitating rapid information exchange when formal auditing is not required. This approach not only streamlines compliance and due diligence processes but also strengthens trust and transparency within value chains, as verified product claims can be readily presented and authenticated at each transaction or handover.

Revocation of Use Case Credentials

In order to fully accommodate the dynamics of the use case for VCs above, it must also be supported to revoke them. Following the W3C Standard for Verifiable Credentials, a status property[4] enables to propagate status changes of credentials, including their invalidation. Thus, it is suggested for verifiers to check the status oft the credential before usage, to ensure its validity.

None MX-Wallets

EU Organization Identities

Looking ahead, the adoption of EU digital organization identities promises to significantly enhance the trust and interoperability within data spaces. Whereas today the Manufacturing data spaces rely on DID:web and BPN-based verifiable credentials to onboard and identify. In the future the integration of standardized, government issued organizational identities will be used. These digital identities will simplify data space collaboration, reduce administrative overhead, and bolster security by providing a harmonized and legally recognized framework for all EU participating entities. As initiatives such as the European Digital Identity Wallet mature, organizations will benefit from more streamlined onboarding processes and improved credential management. This evolution is expected to pave the way for seamless interaction between companies, public authorities, and stakeholders across the continent, ultimately driving greater trust, compliance, and innovation in the digital economy.

The European Business Wallet offers promising opportunities to simplify and accelerate onboarding in Catena-X by providing a secure, verifiable digital identity for legal entities. While the detailed concept is still under development, several integration paths are already imaginable.

For example, after completing the onboarding process, Catena-X could issue the membership credential directly into the company's European Business Wallet or into a second, dedicated wallet used specifically for data-space interactions. Another possibility is leveraging a wallet manager that can operate or bridge multiple identities, enabling organizations to seamlessly manage different credentials across ecosystems.

Outlook

The development of organizational wallets and digital identities varies significantly across regions. In the EU, government-issued organization identities and business wallets are

[4] https://www.w3.org/TR/vc-data-model-2.0/#status-0

emerging as a common foundation for onboarding and trust. In addition, initiatives such as GAIA-X emphasize federated, interoperable identity frameworks that align with European values of data sovereignty and decentralized trust, reinforcing the role of verifiable credentials within data spaces.

In contrast, China follows a highly centralized, state-driven model where organizational credentials are typically issued and governed by public authorities or regulated entities, with limited focus on self-sovereign wallets. Japan takes a hybrid approach, combining governmental frameworks with strong involvement of industry bodies and commercial trust service providers, often relying on centralized or semi-centralized wallet solutions.

In many other countries, government-issued digital organization identities are either not available or not interoperable across borders. To avoid exclusion of participants from these regions, non-governmental identity providers become essential. Organizations such as GS1 and GLEIF offer globally recognized, persistent identifiers (e.g. GS1 identifiers, LEI) that can be used as trust anchors for issuing Verifiable Credentials to organization wallets.

A future-proof data space identity model should therefore support a multi-issuer approach: leveraging government-issued identities where available, while equally accepting credentials issued by trusted non-governmental providers. This ensures global inclusiveness, interoperability, and scalable trust across data spaces, independent of national identity system maturity.

Glossary

Business Partner Number (BPN)	Persistent identifier for uniquely identifying organizations within Catena-X.
CSP (Credential Service Provider)	Entity responsible for issuing, managing, and maintaining credentials or trust artifacts within an identity ecosystem.
Data Space (DS)	Federated environment enabling secure, governed, interoperable data exchange.
Data Space Authority (DSA)	Governance entity defining rules, trust anchors, and policies for a data space.
Data Space Operator (DSO)	Entity operating onboarding, trust services, and infrastructure components of a data space.
Data Space Protocol (DSP)	Protocol defining interaction, negotiation, and data exchange flows.
Decentralized Claims Protocol (DCP)	Protocol for exchanging Verifiable Credentials and Verifiable Presentations.
Decentralized Identifier (DID)	Cryptographically verifiable, decentralized identifier resolving to a DID Document.
Digital Product Passport (DPP)	Standardized digital record of product lifecycle information.

Eclipse Data Space Connector (EDC)	Connector enabling secure and compliant data transactions.
EU Organizational Identity (EU Org ID)	Government-issued digital identity for legal entities in the EU.
Gaia-X Digital Clearing Houses (GXDCH)	the one-stop place to go and get verified against the Gaia-X rules to obtain compliance in an automated way
Identity Provider (IdP)	Service authenticating users and issuing identity tokens.
Legal Entity Identifier (LEI)	Globally unique identifier for legal entities.
Membership Credential	Verifiable Credential proving an organization's membership in a data space.
Open Digital Rights Language (ODRL)	W3C standard for machine-readable usage policies.
OpenID Connect (OIDC)	Authentication layer built on OAuth 2.0 for issuing identity tokens.
Operating Company (OpCo)	Organizational entity providing operational Data Space services.
Product Carbon Footprint (PCF)	Total CO_2 emissions associated with a product's lifecycle.
Self-Sovereign Identity (SSI)	Decentralized identity model using DIDs and Verifiable Credentials.
Single Sign-On (SSO)	Mechanism enabling multi-service access through one authentication.
Verifiable Credential (VC)	Digitally signed credential containing verifiable claims about an entity.
Verifiable Presentation (VP)	Holder-assembled presentation of Verifiable Credentials for verification.

References

- Construct-X & Semiconductor-X & Energy-Data-X & Aerospace-X
- *Marcel Ruland (Cofinity-X). About the future of SSI in Catena-X, this is a link to the slides:* tech-talk.pdf.

Catena-X Standards

The following Catena-X standards provide detailed information:

- https://catenax-ev.github.io/docs/next/standards/CX-0010-BusinessPartnerNumber
- https://catenax-ev.github.io/docs/next/standards/CX-0018-DataspaceConnectivity
- https://catenax-ev.github.io/docs/next/standards/CX-0049-DIDDocumentSchema
- https://catenax-ev.github.io/docs/next/standards/CX-0050-CXSpecificCredentials
- https://catenax-ev.github.io/docs/next/standards/CX-0135-CompanyCertificateManagement
- https://catenax-ev.github.io/docs/next/standards/CX-0149-WalletRequirements