CATENA-X

STANDARD

CX-0018 Eclipse Data Connector (EDC) v2.0.1

Contact: standardisierung@catena-x.net

Table of Contents

ABOUT THIS DOCUMENT & MOTIVATION

Catena-X is the first open and collaborative data ecosystem. The goal is to provide an environment for the creation, operation, and joint use of end-to-end data chains along the entire automotive value chain. All partners are on an equal ground, have sovereign control over their data and no lock-in effects occur. This situation provides a sustainable solution for the digitalization of supply chains, especially for medium-sized and small companies, and supports the cooperation and collaboration of market participants and competitors.

The ever-growing Catena-X ecosystem will enable enormous amounts of data to be integrated and collaboratively harnessed. To ensure that these complex data volumes can be sent, received, and processed smoothly across all stages of the value chain, one language for all players: common standards. The standards of the Catena-X data ecosystem define how the exchange of data and information in our network works. They are the basis for ensuring that the technologies, components, and processes used are developed and operated according to uniform rules.

Common standards create added value for all partners: Within our network, data flows more smoothly through interfaces. In addition, we avoid cumbersome individual IT solutions for sharing data with other partners. In the field of international standardization, Catena-X follows the proven international standardization institutions: ISO/IEC/ITU and CEN-CENELC/ETSI.

For users and data providers, implementation of standards will reduce the costs that would arise from adapting different systems. In addition, no important data is lost. On the contrary, it even becomes easier to collect data across companies. For operators and developers, standards will create a framework that provides reliable orientation and planning security.

The following document describes one of the standards used in the Catena-X ecosystem and the requirements needed to implement it. Here, it serves as main resource to illustrate the following data model. It contains information starting from the format of the model, up to the conceptual and physical model. The standardisation of the data model will enable faster information sharing and homogeneity throughout the entire Catena-X ecosystem.

DISCLAIMER & LIABILITY

The present document and its contents are provided "AS-IS" with no warranties whatsoever.

The information contained in this document is believed to be accurate and complete as of the date of publication, but may contain errors, mistakes or omissions.

The Catena-X Automotive Network e.V. ("Catena-X") makes no express or implied warranty with respect to the present document and its contents, including any warranty of title, ownership, merchantability, or fitness for a particular purpose or use. In particular, Catena-X does not make any representation or warranty, and does not assume any liability, that the contents of the document or their use (i) are technically accurate or sufficient, (ii) conform to any law, regulation and/or regulatory requirement, or (iii) do not infringe third-party intellectual property or other rights.

No investigation regarding the essentiality of any patents or other intellectual property rights has been carried out by Catena-X or its members, and Catena-X does not make any representation or warranty, and does not assume any liability, as to the non-infringement of any intellectual property rights which are, or may be, or may become, essential to the use of the present document or its contents.

Catena-X and its members are subject to the IP Regulations of the Association Catena-X Automotive Network e.V. which govern the handling of intellectual property rights in relation to the creation, exploitation and publication of technical documentation, specifications, and standards by Catena-X.

Neither Catena-X nor any of its members will be liable for any errors or omissions in this document, or for any damages resulting from use of the document or its contents, or reliance on its accuracy or completeness. In no event shall Catena-X or any of its members be held liable for any indirect, incidental or consequential damages, including loss of profits. Any liability of Catena-X or any of its members, including liability for any intellectual property rights or for non-compliance with laws or regulations, relating to the use of the document or its contents, is expressly disclaimed.

REVISIONS & UPDATE

The present document may be subject to revision or change of status. Catena-X reserves the right to adopt any changes or updates to the present document as it deems necessary or appropriate.

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be copied or modified without the prior written authorization of Catena-X. In case of any existing or perceived difference in contents between any versions and/or in print, the prevailing version of the present document is the one made publicly available by Catena-X in PDF format.

If you find any errors in the present document, please send your comments to: standardisierung@catena-x.net

COPYRIGHT & TRADEMARKS

ABSTRACT

The Sovereign Data Exchange within C-X dataspace is governed by the set of rules to which every data exchange process within the dataspace must adhere. The Catena-X platform component that orchestrates the data exchanges in consideration of these rules is called a Connector. This standard describes the functionality that every Connector deployed in the dataspace must have implement in order to follow the rules of Soveregin Data Exchange (SDX). --

1 Introduction

The concept of Sovereign Data Exchange covers a multitude of facets and interconnected components that maintain and ensure data sovereignty requirements in regards to how and when the data is exchanged in the Catena-X (C-X) dataspace. These facets include:

Legal framework of the dataspace including Association membership contracts, specific use case frame contracts and e-contracts maintained by the connectors which are assigned to specific data assets and augment the use case frame contracts.
Business Applications functionality that allows the data owners to create data assets stored in the Connectors and associate access and usage policies with their data assets.
Managed Identity Wallets (MIW) which store Verifiable Credentials (VC) that describe dataspace participants roles and attributes which are used by the Business application to define and by the Connectors to verify data asset access and usage policies.
Central components of the Catena-X platform such as Portal and Marketplace which are used to register participating companies and to issue VCs containing their roles and attributes (for example role: Recycler, location: Germany, etc.).
Company roles and attributes issued and confirmed by the Operating Companies running central components of the Catena-X dataspace. These roles and attributes are defined and standardized by each Use Case defined for the Catena-X.
Finally, the Connectors which are platform components deployed by each company participating in the C-X (or deployed for them by the C-X service providers). The Connectors are responsible for confirming eligibility of the parties to participate in the data exchange and for orchestrating the data exchange based on the defined access and usage policies attached to the data assets stored in the Connectors. The reference implementation of the connector that is provided by the C-X Consortium is called Eclipse Data Connector (EDC) and, therefore, the terms "Connector" and EDC are used interchangeably in this document. The Connectors are also the primary engine of ensuring data sovereignty through the implementation of the International Data Spaces Association (IDSA) Dataspace Protocol (DSP)

(documented here: https://github.com/International-Data-Spaces-Association/ids-specification) as well as Catena-X-specific protocol extensions documented in this standardization document.

1.1 Terminology

> *This section is non-normative*

Term	Description	Reference
Eclipse Dataspace Components (EDC)	Framework for sovereign, inter-organisational data sharing governed by the Eclipse Foundation	https://github.com/eclipse-edc
International Data Spaces Association (IDSA)	Organisation that provides standards and architecture solutions for secure, sovereign data sharing within so-called dataspaces	https://internationaldataspaces.org
Dataspace Protocol (DSP)	Set of specifications designed to facilitate interoperable data sharing within a dataspace, currently governed by the IDSA	https://github.com/International-Data-Spaces-Association/ids-specification
Connector	(Catena-X) Technical component that allows business applications to interact with each other within a dataspace	https://github.com/eclipse-tractusx/tractusx-edc
Data Asset	Is defined as intangible information or representations of tangible objects, or a defined collection of them (e.g., file, database, stream, access to an API)	https://eclipse-tractusx.github.io/docs-kits/category/connector-kit
(Catena-X) Business Applications	(Catena-X) Applications that enable functionality of different use cases, hosted by a data provider or consumer itself or by a business application provider	https://eclipse-tractusx.github.io/developer
Catena-X Marketplace	The Marketplace inside a portal, allowing participants of the Catena-X network to search and select Catena-X Business Applicactions	https://catena-x.net/en/offers/portal-marketplace
Business Partner Number (BPN)	Every participant in the Catena-X network has a unique, unchangeable identifier, called business partner number (BPN). The legal entity of an organization is represented by the Business Partner Number Legal Entity (BPNL)	CX - 0010 Business Partner Number
Data Catalog Vocabulary (DCAT)	RDF vocabulary designed to facilitate interoperability between data catalogs published on the Web	https://www.w3.org/TR/vocab-dcat-3
Open Data Rights Language (ODRL)	Policy expression language that provides a flexible and interoperable information model, vocabulary, and encoding mechanisms for representing	https://www.w3.org/TR/odrl-model, https://www.w3.org/TR/odrl-vocab, https://w3c.github.io/odrl/bp

	statements about the usage of content and services	
Managed Identity Wallet (MIW)	In order to implement the Self-Sovereign Identity (SSI) functionalities, Managed Identity Wallet (MIW) is used. MIW is a centrally managed solution to provide a repository of Verifiable Credentials (VCs) representing C-X participant attributes, roles and identities.	https://github.com/eclipse-tractusx/managed-identity-wallet

1.2 Audience

> *This section is non-normative*

[Mandatory] The following stakeholders are to be distinguished.

1.2.1 Core Service Provider

For a *Core Service Provider* this standard is relevant for the operation and provisioning of managed Connectors and business applications for data sharing in the C-X dataspace.

1.2.2 Data Provider / Consumer

For a *Data Provider / Consumer* this standard is relevant for the data exchange that have to always be initialized and orchestrated by the Connectors ((or equivalent functionality built into the business applications) deployed on both Data Provider and Data Consumer sides. Therefore, the provider and consumer applications must be using the Connectors (or equivalent functionality built into the business applications) to initiate and orchestrate the data exchange.

1.2.3 Business Application Provider

For a *Business Application Provider* this standard is relevant as the provided business application must use either embedded or standalone Connector(s) for data sharing in the C-X dataspace.

1.2.4 Enablement Service Provider

For an *Enablement Service Provider* this standard is relevant if the operation and providing of a Connector-as-a-Service for data sharing is part of the enablement service.

1.2.5 Platform Application Provider

For a *Platform Application Provider* this standard is relevant if the Platform Application Provider develops another version (than the listed reference implementations) of the Connector to be used in the C-X dataspace (either in tandem with the business applications from the same vendor or a standalone version to be used with Catena-X applications available in the C-X marketplace).

1.3 Scope

> *This section is non-normative*

"Data sovereignty refers to the self-determination of individuals and organizations with regard to the use of their data." (Jarke et al., 2019)

The implementation of data sovereignty includes technical and non-technical aspects. In addition to some aspects of it, which have already been mentioned in the Introduction section, data sovereignty encompasses legal, organizational and technical components briefly described below.

As a prerequisite, it is important to have data governance applied within an organisation:

Data assets must be identified and properly managed (i.a., documented). This is complemented by the assessment of the data value and related risks of sharing.
Roles and rights must be defined. This includes the assignment of roles and rights to data assets.
The data must be made accessible and prepared for sharing (i.a., data cleansing).

Moreover, legal and trust aspects have to be clarified within the dataspace:

The existence and structure of trusted authority
Verifiable Presentation to prove organizational identity and membership in the dataspace?
Defined legal framework enabling terms and conditions predefinition and per contract definition.

Finally, technical implementation is ensured by policy enforcement and security mechanisms. These cover all layers, from application layer down to the hardware layer - within the dataspace as well as within the oganisation's infrastructure.

With respect to the above, this document focuses on the role of the Connector as a gateway for business applications to the dataspace, and its functionality as the technical foundation for the successful implementation of data sovereignty. It also provides guideline for software vendors to develop their own versions of the Connectors that would be interoperable with other Connectors deployed in the C-X dataspace.

1.4 Context

> *This section is non-normative*

The technical implementation of the Connectors for Catena-X dataspace (also called Sovereign Data Exchange) is driven by:

1. Data Sovereignty requirements specified for the current release of Catena-X dataspace. At the time of this version of the standard the current release is Catena-X 3.2.
2. Implementation of the Dataspace Protocol.
3. Implementation of the Catena-X extensions of the Dataspace Protocol.
4. Reference implementation of a Connector API.

The following paragraphs specify the current data sovereignty requirements in detail.

1.4.1 Requirement: Identification of data exchange partners

An application can act as Data Provider as well as Data Consumer. A *Business Application Provider* must either ensure that a Connector can be conncted to the application or the application must provide a Connector for each company using the application (in this case the Connector is either defined as a Connector functionality embedded in the application or is bundled with the business application).

This must be enabled via the registration of a specific Connector instance/tenant (or instances/tenants) for each company using the application (see Standard CX - 0017 Company Role by the Connector) as published on the Catena-X standards library).
An application must be enabled to use a Connector for Catena-X specific data transfer or provide a Connector functionality itself.
In both cases, the Connector used for a particpant (i.e., legal entity) must go through the onboarding process and must have a valid SSI verifiable credential.
An application must enable a Data Provider to add the correct Use Case contract ID `RahmenbedingungsID` through the contract definition of a Data Asset (see example below).
In case of data consumption, the application must have the capability to validate whether the data consumer has a verifiable credentail confirming that they signed the same Use Case contract `Rahmenbedingungs` that the data provider attached to their contract offer. That means that before data access is granted, it must be checked that the Data Consumer has agreed to the "Rahmenbedingungen" that are requested by the Data Provider for the given data offer (applicable to the Release 3.2)

In the case of data contract offers created for data consumption, an application must be able to check if a valid `RahmenbedingungsID` is attached to the contract offer:

Example:

```
{
  "odrl:permission": {
    "odrl:action": {
      "odrl:type": "USE"
    },
    "odrl:constraint": {
      "odrl:or": {
        "odrl:leftOperand": "idsc:PURPOSE",
        "odrl:operator": "EQ",
        "odrl:rightOperand": "ID 3.2 Trace"
      }
    }
  }
}
```

1.4.2 Requirement: Terms & Condition Signing

At least one Use Case frame contract which covers the business process of the app must be available and is submitted to the Catena-X association for approval (or already approved). (Covered by Use Case)
An application provider must (Release 3.2) be able to check if a company in Catena X signed the overall "Rahmenbedingungen" and the relevant "Rahmenbedingungen" for the use cases.
An application provider CAN show the "Rahmenbedingungen" mapped to a data asset.
In addition to the reference to the "Rahmenbedingungen" in usage policies, an application must also support access policies as specified in the EDC reference implementation documented here: Connector Kit

1.4.3 Requirement: Data Asset Creation

The application must enable a Data Provider to add the right `RahmenbedingungsID` to the contract offer. A minimal example of a policy with a reference to a "use case Rahmenbedingung" is shown below:

Example:

```
{
  "odrl:permission": {
    "odrl:action": {
      "odrl:type": "USE"
    },
    "odrl:constraint": {
      "odrl:or": {
        "odrl:leftOperand": "idsc:PURPOSE",
        "odrl:operator": "EQ",
        "odrl:rightOperand": "ID 3.2 Trace"
      }
    }
  }
}
```

1.4.4 Requirement: Data Asset Deletion

In the role of a Data Consumer, the application must have the capability to delete consumed data based on the "Rahmenbedingungen" of the use case.

1.4.5 Requirement: Data consumption & data providing

The application must ensure that contract negotiations and data exchange history are logged and that these logs are persisted. It must be ensured that these logs can be made available in case of necessary legal clarifications.

1.5 Architecture Overview

> *This section is non-normative*

![src](Architecture_v2.png)

The architecture diagram illustrates the sovereign data exchange landscape's essential components, stakeholders, and relations. Companies sharing data in the network are illustrated as *Data Provider* and *Data Consumer* with their own IT landscape (grey boxes). Every participant needs to use a Connector as a component for cross-company data sharing that only transfers data after having a *(Policy) Agreement*. This Connector uses the Dataspace Protocol as standardized by the IDSA. This *Connector* can either be self-deployed on the Data Consumer's or Provider's IT infrastructure, or as a managed service. To ensure data sovereignty, the Connector is able to enforce access policies, like the BPN validation. Since value is only generated when data is used in the specific application, it can be transferred from the Connector to either specific Catena-X *Business Applications* from a dedicated *Business Application Provider* or to custom *Data Products* that aren't directly associated with Catena-X. Since control over data is important, other access policies as well as usage policies MUST be checked and enforced in the respective applications.

Different *Core Services* in the Catena-X network use a *Managed Connector* that works the same way as the Connector from the Data Provider and Consumer. Nevertheless, *Platform Application Providers* and *Enablement Service Providers* are able to build their own *Connector Implementation* or *Connector-as-a-Service* versions.

Furthermore, all applications in the Catena-X dataspace (orange box) have to prove *Catena-X Compliance* to ensure that the standards and principles are fulfilled and correctly applied.

2 Conformance

2.1 Preconditions & Dependencies

2.1.1 External Dependencies

> *This section is non-normative*

As a dataspace project, Catena-X must follow the developments in relevant initiatives and projects and assess their integration into own implementations and specifications.

IDSA

The IDSA proposes a solution architecture for dataspaces by specifying central components and their architectures, i.a., the identity service, catalog service, and the Connector. This is done by defining essential parts of the business, functional, process, information, and system layers. As part of this, the Dataspace Protocol aims to standardise the essential communication processes within a dataspace. The architecture and designs of the Catena-X dataspace partly build on those specifications and recommendations and therefore are strongly affected by ongoing delevopments, e.g., the trend from central components to a more decentralized architecture. This comprises, i.a.:

Architecture of the Dynamic Attribute Provisioning Service (DAPS) and used identity claims
Interaction of Connectors and data apps
Used ontologies, e.g., Data Catalog Vocabulary (DCAT) and Open Data Rights Language (ODRL)

In return, Catena-X gives feedback to the IDS community in order to confirm or improve the developed ideas and concepts.

EDC

The Eclipse Dataspace Components (EDC) provide an open-source software framework for sovereign, cross-organizational dataspaces. The framework includes implementations for cataloging, identity management, data exchange, policy enforcement, and monitoring. In doing so, it integrates with existing and established technologies and dataspace standards. One of the reference implementations of a Catena-X conform dataspace connector is build on the EDC. Therefore, devlopments within the open source project are highly relevant for architecture decisions and interface identification. Common feature requests are contributed to the EDC project in order to establish the provided and further developed dataspace technologies, also for associated dataspace initiatives and projects.

2.1.2 Internal Dependencies

> *This section is non-normative*

Catena-X and the development of Connectors that aim for a solid foundation of data sovereignty do not only have external dependencies, but also internal ones. These are described in the following.

2.1.2.1 Managed Identity Wallet

Managed Identity Wallet (MIW) is a centrally managed solution to provide a repository of Verifiable Credentials (VCs) representing C-X participant attributes, roles and identities. The standards governing this solution are listed in the Section 2.1.2.3 and the Connector connections to the MIW are described in the section 2.3.2 of this standard.

2.1.2.2 Portal and Marketplace: VC issuing process and validation

The dependancy of the C-X Connectors on the Portal and Marketplace central service is indirect (i.e. there is no direct impact on this standard if the Portal and Marketplace changes the APIs or/and endpoints). However, it is important to note that Verifiable Credentials stored in the MIW (see section 2.1.2.1) are issued via the Portal service.

2.1.2.3 Catena-X Identity and Access Management Standards

```
Catena-X connectors need to be aware of the identities and attributes/roles of the participating
companies. The standards defining these identities and attributes are listed below:
```

- CX-0013 Identity of Member Companies
- CX-0016 Company Attribute Verification
- CX-0017 Company Role by the connector
- CX-0049 DID Document Schema
- CX-0050 Framework Agreement Credential
- CX-0051 Summary Credential

2.1.2.3.1 CX-0013 Identity of Member Companies

This standard is the definition of the DID method used and the use of the "Managed Identity Wallet" for Release 3.2

2.1.2.3.2 CX-0016 Company Attribute Verification

This standard defines the schema of Verifiable Credentials for the Company Attributes of the participants. For the issuance of Verifiable Credentials, which represent the Company Attributes, that defines the necessary data fields. In order to be able to develop further attribute schemes in the future, a template is defined in addition to the schemes for the Business Partner Number and the Membership Credential, on which use case-specific credentials are based, for example.

Example: In addition to the BPN and the membership, the Product Carbon Footprint use case also requires proof that the partner is a "Dismantler". The Verifiable Credential defined in the use case must follow the template defined here.

2.1.2.3.3 CX-0017 Company Role by the connector

This standard defines the identity-giving component for the connectors of the network participants. In the Catena-X context of decentralised decentralised identities -described in CX-0013- the identity of the connector is confirmed by a Verifiable Credential issued by the participant to the connector using its Self Sovereign Identity. The use of a Verifiable Credential ensures that the connector belongs to the participant that confirms it. This also ensures that the connector is acting on behalf of the participant.

2.1.2.3.4 CX-0049 DID Document Schema

The purpose of this standardization request is the definition of the DID Document Schema

2.1.2.3.5 CX-0050 Framework Agreement Credential

This standard is the definition of Verifiable Credentials for the constent / signing confirmation of framework agreements / framework contracts. In the Catena network, use case specific framework agreements / framework contracts for the exchange of data are agreed and provided to the partners. the OpEnv receives the signed framework agreements from the partners involved in these use cases and issues a corresponding Verifiable Credential to the signing partner. This Verifiable Credential can then be made available via the EDC to manage the exchange of data between the partners based on their agreement to the corresponding Framework Agreement. An example of this would be participation in the "Product Carbon Footprint" use case and thus consent to the corresponding framework agreement for data exchange.

2.1.2.3.6 CX-0051 Summary Credential

This standard defines a Verifiable Credential, that contains a summary of several Verifiable Credential as a summery. For the data exchange and the associated identification and authorisation, the corresponding Verifiable Credentials, which describe the corresponding attributes of the partners, are exchanged. In order to be able to exchange all necessary attributes of the partner companies, all verifiable credentials must be provided in a corresponding verifiable presentation via the EDC. The exchange between the EDCs should take place via the HTTP header. However, the data size of the HTTP header is limited to 4 kilobytes. This limit is exceeded by the size of a Verifiable Presentation which contains all attributes. To solve this problem, a single Verifiable Credential is issued to the partner by OpEnv, which contains all credentials issued for this partner.

The summary credential can contain the following credentials

MembershipCredential
BpnCredential
DismantlerCredential
PcfCredential
SustainabilityCredential
QualityCredential
TraceabilityCredential
BehaviorTwinCredential

2.2 Communication

> *This section is non-normative*

2.2.1 Dataspace Protocol

The Dataspace Protocol is a set of specifications designed to facilitate interoperable data sharing between entities respecting data sovereignty. These specifications define the schemas and protocols required to publish data, negotiate data usage agreements, and access data as part of a federation of technical systems termed a dataspace.

The *Catalog Protocol* defines how data offers are published as DCAT catalogs and datasets, referencing ODRL data usage policies.
The *Negotiation Protocol* defines how contract negotiations are conducted between Data Providers and Data Consumers in order to agree on a legally binding data access/usage contract.

The *Transfer Protocol* defines how transfer processes using a given data transfer protocol are governed.

The Catena-X dataspace SHOULD adopt the by *Dataspace Model* and Dataspace *Terminology* documented key terms.
Catena-X Connectors MUST implement the described protocols, regardless of used technologies and architectures (e.g., programming language, monolith vs. micro services).

2.2.2 Data Assets

A Data Asset represents data (databases, files, cache information, etc.) which are to be exchanged between organisations participating in the dataspace. Usage Policies represent permitted and prohibited actions over a certain Data Asset.

A Connector MUST use DCAT to describe its Data Assets, resp. structure their metadata. Following the Dataspace Protocol, the root class is `dcat:Dataset`.
Each Data Asset MUST link to a resolvable *Data Address*. A data address is a pointer into the physical storage location where a Data Asset will be stored.
As specified by the Dataspace Protocol, one Data Asset MUST refer to at least one Usage Policy, expressed in ODRL.
Connectors COULD implement a technical enforcement of the negotiated Usage Policies.
Connectors MUST persist the resulting Agreement.

> *A Data Offer is a dynamic representation of the Data Asset and Usage Policies for a specific consumer and CAN serve as the protocol's data transfer object (DTO) for a particular contract negotiation. Data Offers are not persisted and will be regenerated on every request. The Connector acting as Data Provider will generate Data Offers only dedicated to the organisation or dataspace participant operating the requesting Connector acting as Data Consumer.*

2.2.3 API Specification

With the definition of the protocol sequences, the Dataspace Protocol also provides binding documents.

Per each protocol (catalog, negotiation, transfer), HTTP(S) endpoints for Data Provider and Data Consumer Connectors are defined.
The bindings do not include any instructions about authentication and authorization mechanisms.

Connectors MUST support the specified HTTP binding. They CAN implement other binding as well.
Connectors CAN only implement the part of the binding that is dedicated for their role in the dataspace. For instance, Connectors only acting as Data Consumer do not need to implement interfaces of the Data Provider.
Connectors MUST ensure that the required transfer protocols to provide or consume Data Assets are supported.

2.2.4 Authorization

To restrict the access to certain APIs and Data Assets, a Connector CAN implement its own mechanisms.

The Connector MUST provide a possibility to restrict the access of a Data Asset to specific business partners by attribute(s), e.g., represented as a VC. Example in ODRL (not mandatory):

```
{
 "odrl:permission": {
   "odrl:action": {
     "odrl:type": "USE"
   },
   "odrl:constraint": {
     "odrl:or": {
       "odrl:leftOperand": "[Membership | Dismantler | FrameworkAgreement.pcf |
FrameworkAgreement.sustainability | FrameworkAgreement.quality | FrameworkAgreement.traceability
| FrameworkAgreement.behavioraltwin | BPN]",
       "odrl:operator": "[ EQ | GT | GEQ ]",
       "odrl:rightOperand": "active"
```

```
      }
    }
  }
}
```

The Connector MUST provide a possibility to restrict the access of a Data Asset to specific business partners. Example in ODRL (not mandatory):

```
{
  "@context": {
    "odrl": "http://www.w3.org/ns/odrl/2/"
  },
  "@id": "176c1a58-a712-4231-b5f0-84e7f5c72b75",
  "@type": "odrl:Set",
  "odrl:permission": {
    "odrl:action": {
      "odrl:type": "USE"
    },
    "odrl:constraint": {
      "odrl:or": {
        "odrl:leftOperand": "BusinessPartnerNumber",
        "odrl:operator": "EQ",
        "odrl:rightOperand": "BPNPOLICY"
      }
    }
  }
}
```

The Connector MUST restrict the data usage to partners and purposes for a specific use case. Example in ODRL (not mandatory):

```
{
  "odrl:permission": {
    "odrl:action": {
      "odrl:type": "USE"
    },
    "odrl:constraint": {
      "odrl:or": {
        "odrl:leftOperand": "idsc:PURPOSE",
        "odrl:operator": "EQ",
        "odrl:rightOperand": "ID 3.2 Trace"
      }
    }
  }
}
```

The Connector MUST validate given access restrictions, e.g., with the content of a VC.

The SSI policy is enforced by the Managed Identity Wallet (MIW), based on a *SummaryCredential* described in a json-ld context. The *SummaryCredential* is part of the HTTP Authorization token. Example of a *SummaryCredential*:

```
{
  "credentialSubject": [
    {
      "contractTemplate": "https://public.catena-x.org/contracts/",
      "holderIdentifier": "BPN123",
      "id": "did:web:localhost%3A8080:BPN123",
      "items": [
        "BpnCredential",
        "DismantlerCredential",
        "ResiliencyCredential",
        "QualityCredential"
      ],
      "type": "SummaryCredential"
    }
  ],
  "issuanceDate": "2023-07-06T11:32:00Z",
  "id": "did:web:localhost%3A8080:BPNOPERATOR#e6e6984d-29bf-4b96-a882-ec5482b19a57",
  "proof": {
    "created": "2023-07-06T11:32:01Z",
    "jws": "eyJhbGciOiJFZERTQSJ9..NsBK9dEYb6NIy5Ihjuu9HZsRy8Xg-tvFnUl4vbPrYDLeGYkHyiAXB1HTh9u0X-
0Zt23IGA1SuWGXlDLfUygwAQ",
    "proofPurpose": "proofPurpose",
    "type": "JsonWebSignature2020",
    "verificationMethod": "did:web:localhost%3A8080:BPNOPERATOR#"
  },
  "type": [
    "VerifiableCredential",
    "SummaryCredential"
  ],
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://catenax-ng.github.io/product-core-schemas/SummaryVC.json",
    "https://w3id.org/security/suites/jws-2020/v1"
  ],
  "issuer": "did:web:localhost%3A8080:BPNOPERATOR",
  "expirationDate": "2023-09-30T22:00:00Z"
}
```


The Connector then checks the content of `/credentialSubject/items/*`. For each attribute, the Connector would enforce/expect another entry. The Summary Credential MUST be issued by an operator of the Catena-X dataspace.

Attribute	Credential Subject Item
Membership	MembershipCredential
Dismantler	DismantlerCredential
FrameworkAgreement.pcf	PcfCredential
FrameworkAgreement.sustainability	SustainabilityCredential
FrameworkAgreement.quality	QualityCredential

FrameworkAgreement.traceability	TraceabilityCredential
FrameworkAgreement.behavioraltwin	BehaviorTwinCredential
BPN	BpnCredential

2.3 Identities

Each dataspace is managed by one or more dataspace **operators**. The identities, participating in the dataspace, are called **participants**. Each connector *represents* a single participant.

2.3.1 Authentication

According to the HTTP Bindings of the Dataspace Protocol, an identity token is part of each HTTP message. For Catena-X, this identity token will be a Verifiable Presentation (as JWT), containing a single *SummaryCredential*. The *SummaryCredential* contains information about the Verifiable Credentials a dataspace participant owns (see Section 2.3.3).

For this release the *SummaryCredential* can be obtained from the **Managed Identity Wallets** application. The content of the *SummaryCredential* depends on how the participant is registered in the **Portal**.

To obtain the Verifiable Presentation as JWT the following steps are to be taken:

1. The participant queries its Verifiable Credentials for the *SummaryCredential*
2. The participant sends the *SummaryCredential* to the MIW to obtain a Verifiable Presentation as JWT, containing the *SummaryCredential*
3. The participant adds the JWT to the Data Space Protocol HTTP message's *Authoritzation Header*

To validate the Verifiable Presentaion as JWT the following steps are to be taken:

1. The participant gets the Verifiable Presentation as JWT from a Data Space Protocol HTTP message
2. The participant sends the Verifiable Presentation to the **Managed Identity Wallets** for validation 2.1 The **Managed Identity Wallet** validates
    - Verifiable Credential und JWT/Verifiable Presentation signatures
    - json-ld schema
3. The participant validates itself (at minimum)
    - audience of the JWT
    - issuer of the JWT/Verifiable Presentation (must be Verifiable Credential Subject)
    - issuer of the *Summary Credential* (must be a Data Space Operator)

The **Managed Identity Wallets** endpoints can be called by the same authentication token/mechanism, that is also used by the **Portal**.

2.3.2 Managed Identity Wallet

To align the identity, authentication and data exchange of participants with the open and decentralized concepts within GAIA-X, especially self-sovereign identities, every legal entity associated to a BPNL number should have the possibility to also get a W3C compliant DID (Decentralized Identifier). Due to the lack of production-ready SSI infrastructure and slow adoption on the market, this is in a first step achieved by providing a managed wallet (also called "Custodian") with a private/public key pair and related DID for a legal entity along with the onboarding. This wallet can then be used via the Managed Identity Wallet API by other services or applications such as the Self Description or the EDC to issue and retrieve verifiable credentials and create verifiable presentations on behalf of a certain legal entity as part of governance processes and use cases.

2.3.3 Connector Endpoints

Get Credential

For fetching a Credential, the Connector SHOULD use the credentiale endpoint and define the requested Credential Type. The Summary Credential can only exist once in a User Wallet.

```
/api/credentials?type=['SummaryCredential']
```

Create Presentation

```
/api/presentations?withAudience=['Audience1','Audience2']+asJwt=true
```

Validate Presentation

The endpoint is called with the presentation in the body

```
/api/presentations/validation?withDateValidation=true
```

2.3.4 Summary VC

The *Summary VC* is a temporary credential designed to consolidate a set of individual Catena-X Verifiable Credentials (VCs) into a compact form. It serves the purpose of fitting within HTTP header limits, which facilitates the efficient transmission and processing of credentials. This section provides the specifications for the Summary VC schema, outlining its structure and key properties.

Example

Here is an example of a Summary VC in JSON-LD format:

```
{
  "@context": [
    "https://w3id.org/2023/tractusx/credentials/summary/v1"
  ],
  "id": "<credential uid>",
  "type": [
    "VerifiableCredential",
    "SummaryCredential"
  ],
  "issuer": "<did:web:issuer>",
  "issuanceDate": "2023-06-02T12:00:00Z",
  "expirationDate": "2022-06-16T18:56:59Z",
  "credentialSubject": {
    "id": "<did:web:subject>",
    "holderIdentifier": "<BPN>",
    "type": "SummaryCredential",
    "items": [
      "MembershipCredential",
      "DismantlerCredential",
      "PcfCredential",
      "SustainabilityCredential",
      "QualityCredential",
      "TraceabilityCredential",
      "BehaviorTwinCredential",
      "BpnCredential"
    ],
    "contractTemplates": "https://public.catena-x.org/contracts/" Connector MUST restrict the
```

```
data usage to partners and purpo   }
}
```

Specification

The Summary VC schema is based on the JSON-LD format and consists of the following properties:

Property	Type	Description
@context	array of strings	Specifies the context in which the Summary VC is interpreted. In this case, it references the Catena-X Summary VC schema version 1 contex
id	string	Represents the unique identifier for the Summary VC.
type	array of strings	Indicates the type of the credential. It includes "VerifiableCredential" and "SummaryCredential" to identify the Summary VC.
issuer	string	Represents the decentralized identifier (DID) of the entity issuing the Summary VC.
issuanceDate	string	Specifies the date and time when the Summary VC was issued, following the ISO 8601 format (e.g., "2023-06-02T12:00:00Z").
expirationDate	string	Represents the date and time when the Summary VC will expire, following the ISO 8601 format.
credentialSubject	object	Contains information about the subject of the Summary VC.
id	string	Represents the decentralized identifier (DID) of the subject entity associated with the Summary VC.
holderIdentifier	string	Provides an identifier (e.g., BPN) for the holder of the Summary VC.
type	string	Specifies the type of the credential subject, which is "SummaryCredential" in this case.
items	array of strings	Lists the types of individual Catena-X VCs included in the summary. Each item is represented by a string value corresponding to the type of the VC.
contractTemplates	string	Indicates the URL pointing to the contract templates associated with the Summary VC.

Conclusion: The Summary VC schema defines a structure for consolidating multiple Catena-X VCs into a concise format suitable for transmission within HTTP headers. It allows for efficient processing and sharing of credentials while adhering to the limitations imposed by header size restrictions. The example provided demonstrates the key properties and their roles within the schema.

2.4 Data Persistence

Required: The Data Sovereignty and Legal Framework requirements dictate that the Connectors MUST implement record Data Exchange contract negotiation and history. The history of the data exchange MUST provide the date/time and ID of the data asset that was exchanged. Apart from these attributes, this standard does not define implementation or interoperability requirements for transaction history.

3 Proof of Conformity

> *This section is non-normative*

All participants and their solutions MUST prove that they are conformant with the Catena-X standards. To validate that the standards are applied correctly, Catena-X employs Conformity Assessment Bodies (CABs). Please refer to the process of conformity assessment and certification.

> *More details regarding reference implementations observing the CACs defined below can be found in Section 4.2.*

Specifically, the Conformity Assessment Criteria are defined as follow:

3.1 Dataspace Protocol CACs

1. The Catena-X Connectors SHOULD adopt the by *Dataspace Model* and Dataspace *Terminology* documented key terms.
2. Catena-X Connectors MUST implement the described protocols, regardless of used technologies and architectures (e.g., programming language, monolith vs. micro services).

> *Details for this section are available in Section 2.2.1*

3.2 Data Assets CACs

1. A Connector MUST use DCAT to describe its Data Assets, resp. structure their metadata. Following the Dataspace Protocol, the root class is `dcat:Dataset`.
2. Each Data Asset MUST link to a resolvable *Data Address*. A data address is a pointer into the physical storage location where a Data Asset will be stored.
3. As specified by the Dataspace Protocol, one Data Asset MUST refer to at least one Usage Policy, expressed in ODRL.
4. Connectors COULD implement a technical enforcement of the negotiated Usage Policies.
5. Connectors MUST persist the resulting Agreement.

> *Details for this section are available in Section 2.2.2.*

> *A Data Offer is a dynamic representation of the Data Asset and Usage Policies for a specific consumer and CAN serve as the protocol's data transfer object (DTO) for a particular contract negotiation. Data Offers are not persisted and will be regenerated on every request. The Connector acting as Data Provider will generate Data Offers only dedicated to the organisation or dataspace participant operating the requesting Connector acting as Data Consumer.*

3.2 API Specification CACs

1. Connectors MUST support the specified HTTP binding. They CAN implement other binding as well.
2. Connectors CAN only implement the part of the binding that is dedicated for their role in the dataspace. For instance, Connectors only acting as Data Consumer do not need to implement interfaces of the Data Provider.
3. Connectors MUST ensure that the required transfer protocols to provide or consume Data Assets are supported.

> *Details for this section are available in Section 2.3.3*

3.3 Authorization CACs

1. The Connector MUST provide a possibility to restrict the access of a Data Asset to specific business partners by attribute(s), represented as a set of Verifiable Credentials (VCs).
2. The Connector MUST provide a possibility to restrict the access of a Data Asset to specific business partners.
3. The Connector MUST restrict the data usage to partners and purposes for a specific use case.
4. The Connector MUST validate given access restrictions, e.g., with the content of a VC.
5. The Connector then checks the content of `/credentialSubject/items/*`. For each attribute, the Connector would enforce/expect another entry. The Summary Credential MUST be issued by an operator of the Catena-X

dataspace.

> *To restrict the access to certain APIs and Data Assets, a Connector CAN implement its own mechanisms.*

> *Details for this section are available in Section 2.2.4*

3.4 Authentication and Identity CACs

1. The Connector MUST implement Authentication and Identity verification mechanism described here: Section 2.3 and its subsections.

3.5 Data Providers / Consumers

1. These entities MUST ensure that the business applications they deploy for Catena-X data exchange are designed to provision for data exchange through Connectors.

3.6 Application Providers

Application Providers need to ensure that the applications they offer as managed services (AaaS or PaaS) comply with the standards of Catena-X. Therefore these applications MUST always use a C-X Connector for data exchange orchestration and the Connector MUST be interoperable with other Connectors deployed in the dataspace following the specifications described in Section 2.

3.7 Application Vendors

1. ALL connectors developed for use in the Catena-X dataspace MUST use IDSA Dataspace Protocol and MUST implement extensions of the Dataspace Protocol documented in this standard.
2. Business Application developed for use in Catena-X MUST follow the specifications for creating Data Assets, Contract Offers and orchestrating Data Exchange through C-X Connectors (see Sec 2.2.1). They also COULD support the Connector's data management API which provides an interface between the Catena-X-specific business applications and the Connectors. In order to provide business application vendors with flexibility to build end-to-end solution, the Management API is not a mandatory part of the Connector specification. However, we provide several recommendations regarding the use of the Management API in other Connector implementations:
3. Application vendors who want to create standalone Connectors and to ensure that those Connectors can be used by a wide range of C-X applications provided by other vendors SHOULD implement the EDC Management API
4. Application vendors who want to create business applications for Catena-X use cases without the connector functionality embedded into the business applications SHOULD use the EDC Management API in connecting their applications to C-X Connectors.
5. Application vendors who either embed Connector functionality into their applications or want to create their own connectors tightly coupled to their applications CAN use EDC Management API or they CAN implement their own unique versions of the Management API.

4 References

4.1 Normative References

1. Each Connector deployed within the Catena-X dataspace MUST be fully compliant with the Dataspace Protocol, not older than v0.8.
2. Each Connector deployed within the Catena-X dataspace MUST be fully compliant with the Catena-X custom extensions of the Dataspace Protocol.
3. Each Connector deployed within the Catena-X dataspace MUST be able to connect to the Managed Identity Wallet (MIW) service in Catena-X and MUST be able to read Verifiable Credentials (VCs) documented in the following

standards:

CX-0013 Identity of Member Companies (provide link once published)
CX-0016 Company Attribute Verification (provide link once published)
CX-0017 Company Role by the connector (provide link once published)
CX-0049 DID Document Schema (provide link once published)
CX-0050 Framework Agreement Credential (provide link once published)
CX-0051 Summary Credential (provide link once published)

4.2 Non-normative References

> *This section is non-normative*

Catena-X Business Applications communicate with the reference implementation of the Connector (a.k.a Catena-X Eclipse Data Connector - EDC) via Management API to create contract offers (data assets and associated access and usage policies) and to initiate data exchange. This API and all its prior/future versions are documented here.

4.3 Reference Implementations

> *This section is non-normative*

The validation and enforecement of Access Policies as mentioned in Sec 2.2.4 is handled by the cx-policy extension.

The validation of the Business Partner Number (BPN) is implemented by the business-partner-validation extension. Using the Business Partner Validation Extension it's possible to add configurable validation against BPNs

To enable the exchange of information like the BPN, the provisional-additional-headers extension was implemented and extends the http headers. The goal of this extension is to provide additional headers to the request to the backend service done by the provider in order to retrieve the data that will be given to the consumer.

The custom implementation of the EDC identity service for SSI. The implementation is split into a number of submodules, that implement different aspects needed for SSI.

Finally, the reference implementation of the Eclipse Dataspace Connector (EDC) for Catena-X Release 3.2 (EDC Release 0.5.0) is available here: EDC 0.5.0.

5 Annexes

5.1 Figures

> *This section is non-normative*

5.2 Tables

> *This section is non-normative*

5.3 Bibliography

Jarke, M., Otto, B., & Ram, S. (2019). *Data sovereignty and data space ecosystems. Business & Information Systems Engineering, 61*, 549-550.

6 Resources

CX-018 Sovereign Data Exchange - Architecture.drawio