CATENA-X
STANDARD

CX - 0018 ECLIPSE DATASPACE CONNECTOR (EDC)

PLATFORM CAPABILITY: SOVEREIGN DATA EXCHANGE

Contact: standardisierung@catena-x.net

Note: Please specify the platform capability in the subject line

DISCLAIMER AND 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. (current version available at https://catena-x.net/fileadmin/user_upload/Vereinsdokumente/Catena-X_IP_Regelwerk_IP_Regulations.pdf) 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 AND UPDATES

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 current version of the present document is publicly available at https://catena-x.net/de/standardisierung/catena-x-einfuehren-umsetzen/standardisierung/standard-library

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 at https://catena-x.net/de/standardisierung/catena-x-einfuehren-umsetzen/standardisierung/standard-library

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

COPYRIGHT AND TRADEMARKS

Any and all rights to the present document or parts of it, including but not limited under copyright law, are owned by Catena-X and its licensors.

The contents of this document shall not be copied, modified, distributed, displayed, made publicly available or otherwise be publicly communicated, in whole or in part, for any purposes, without the prior authorization by Catena-X, and nothing herein confers any right or license to do so.

The present document may include trademarks or trade names which are registered by their owners. Catena-X claims no ownership of these except for any which are indicated as being the property of Catena-X, and conveys no right to use or reproduce any such trademark or trade name contained herein. Mention of any third-party trademarks in the present document does not constitute an endorsement by Catena-X of products, services or organizations associated with those trademarks.

"CATENA-X" is a trademark owned by Catena-X registered for its benefit and the benefit of its members. Using or reproducing this trademark or the trade name of Catena-X is expressly prohibited.

No express or implied license to any intellectual property rights in the present document or parts thereof, or relating to the use of its contents, or mentioned in the present document is granted herein.

The copyright and the foregoing restrictions extend to reproduction in all media.

© Catena-X Automotive Network e.V. All rights reserved.

RELEASE HISTORY

Version	Release Date	Description
1.0.0	30. November 2022	Initial version by Catena – X Association
1.0.1	6. March 2023	Addendum for Conformity Assessment added

Contents

Introduction and Overview 4
1. Data Sovereignity 5
1.1. Data Sovereignity components within Catena-X 6
1.2. Definition of Access Policy in the EDC connector 7
2. Data Sovereignity Guardrails 8
2.1. Access Policies 8
2.2. Usage Policies 8
2.3. Duration restricted Data Usage 8
2.4. Role-restricted Data Usage 9
2.5. Purpose-restricted Data Usage 10
3. Enforcing Policies 11
4. Eclipse Data Connector (EDC) User Guide 13
5. Data provisioning applications – Data Sovereignity considerations 15
5.1. Large corporations perspective - business domains and use cases 15
6.2. SME perspective 16
7. Next Steps and Evolution of EDC 16

Figure 1: EDC Architecture 14

INTRODUCTION AND OVERVIEW

Data sovereignty is a principle that spans multiple layers of the dataspace ecosystem. These layers range from identity and attributes of the C-X network participants and services that are trusted and verifiable, through middleware provisions for DS such as ability to define access and usage policies, sign contracts and verify the validity of the conditions before the data exchange takes place, through the end-user applications on both data consumer and data provider sides being able to integrate with the C-X services to read and enforce usage policies. In a more general level, data sovereignty aims to allow users to keep control over their data.

The Eclipse Data Connector (EDC) enables data exchange across Catena-X dataspace while maintaining conditions of data sovereignty and interoperability. A set of reference tools and standardized specifications (APIs, protocols etc.) that allow data flow conditions verification and orchestrate the data exchange preparation and data flow. For this documentation, we are assuming that the identity and attributes of the network participants and services are in place, and we focus on the components and processes listed in the sections below.

Who should use the EDC connector

As stated above, any data exchange within Catena-X dataspace can only take place if there is an existing contract between the participants of the exchange. Eclipse Data Connector is the tool where the presence of the contract is maintained and verified and also performs a role of the data exchange orchestrator. Therefore, any company participating in the dataspace as either data provider or data consumer has to use a connector compliant with the EDC interoperability specification. At present the only connector compliant with the requirements of data exchange in C-X is the Eclipse Data Connector provided as a reference implementation.

Since the source code of the connector is freely available, developing EDC alternatives is possible and allowed, however not encouraged until the interoperability protocols are fully defined, standardized and published (as stated in the final chapter, our expectation is that the next version of the IDSA specification will include EDC extensions and therefore the IDSA specification v2 will become the official standard). Furthermore, we encourage any company requiring additional connector functionality to actively participate in the EDC project instead of creating their own solution.

The following document highlights the importance of data sovereignty and its rules in the context of Catena-X. It commences by defining the data sovereignty components within Catena-X, followed by the definition of the Access Policy in the EDC connector. Then it emphasizes on the requirements necessary to implement the access and usage policies, which are managed and enforced with the help of EDC. The EDC is explained from a technical viewpoint. The interaction with other provisioning applications is stressed out from two company perspectives, the large corporation's perspective and the SME perspective.

For more information regarding the EDC relationship to the IDSA standard and future development of EDC please refer to the last chapter of this document.

1. DATA SOVEREIGNTY

Data sovereignty (DS) is a principle that spans multiple layers of the dataspace ecosystem. These layers range from identity and attributes of the Catena-X dataspace participants and services that are trusted and verifiable, through middleware provisions for DS such as ability to define access and usage policies, sign contracts and verify the validity of the conditions before the data exchange takes place, through the end-user applications on both data consumer and data provider sides being able to integrate with the C-X services to read and enforce usage policies. On a more general level, data sovereignty aims to allow users to keep control over their data.

In the context of C-X Market Entry Release, our view of data sovereignty assumes that identity of users, companies and services is established and trusted across the dataspace. Therefore, the scope of DS for the current release is based on the following requirements and technical components:

No.	Rule	Technical component implementing the rule
1.	Data exchange within C-X dataspace can only take place if there is a electronic signed	Eclipse Data Connector (EDC) - as a reference implementation - or equivalent

	contract between the parties of the data exchange	component(s) created by C-X software vendors (standalone or embedded in their business applications) that are able to connect and exchange data with EDC. Both EDC and other connectors can henceforth be referred to as connectors.
2	Data provider applications are able to define data assets, usage and access policies and contract offers compliant with the EDC reference implementation standard	Business application set used by the data provider (company) and connectors
3	Data consumer applications enable review and electronic signing of the contract offers available to them from data provider companies in the C-X dataspace	Business application set used by the data consumer (company) and connectors
4	Data consumer application are able to establish data exchange through their connectors and data provider connectors	Business application set used by the data consumer (company) and connectors
5	Visibility of their contract offers can be limited by the data providers to only selected companies in the dataspace	Business application set used by the data consumer (company) and connectors
6	Contract offers and signed electronic contracts can be reviewed by their respective data providers and data consumers in Human Readable Text (HRT)	Business application set used by the data consumer and data provider (companies) and connectors
7	All C-X association member companies are legally bound to observe the access and usage polices listed in their signed electronic contracts for data exchange	No technical component. Instead, the association contract must include provisions that will make the electronic contracts for data exchange legally binding.

Future Data Sovereignty Provisions

The current scope of data sovereignty as briefly documented in the table above will be sequentially updated and expanded in conjunction with the Catena-X future releases. Possible future extensions will include technical enforcement of the usage policies by the consumer business applications, rules, and technical enablement of data encryption with decryption keys lifetime and availability controlled by the data providers (data owners) etc.

1.1. DATA SOVEREIGNTY COMPONENTS WITHIN CATENA-X

Association contract

Every company joining the association will sign the membership contract that will state that the participant will be legally bound to observe the data policies associated with each data offer that the company will use. Each data offer can have a separate set of access and usage policies assigned to it.

Contract Offer

There will be no data exchange within the C-X unless both parties electronically sign data offer contract. The creation of this contract is triggered by the data consumer user accepting the data offer created previously by the data provider. Once the approval is made, an electronic contract is created by the EDC connector control plane which will include statements on all policies that the provider defined for this particular data offer. By accepting this offer, the data consumer company accepts the contract conditions and policies and agrees to be legally bound by them. After the contract is electronically signed, it is stored in the both data consumer and provider connectors.

Access Policies

Data provider will be able to create a set of standardized access policies in the process of creating a data offer. These access policies will limit who can see and access the data offers. There will be several criteria used in the access policies based on attributes that each participant of C-X will have. So, it will be possible to limit access to the data offer based, for instance, on the role of the data consumer and/or on the location of the company. An example of such a policy would be to limit access to the offer to a specific recycler based in Germany (location attribute). Since the access policies are based on attributes that can be read by the connector, they will be technically enforceable in the future (as opposed to most of the usage policies).

In preparation for the PI5, only a rudimentary set of access policies will be available but will be expanded during the PI5.

1.2. DEFINITION OF ACCESS POLICY IN THE EDC CONNECTOR

What is an Access Policy in the EDC

Access policy in the connector does not mean that the connector will enforce back-end system data access rules (ACLs). Instead, the EDC Data Offer Access Policy limits who (which companies - or rather which connectors registered in DAPS) can access the data offers and data contracts. The scenario below illustrates that concept with the BPN-restricted access policy.

1. A data provider created a data offer and a BPN-restricted access policy associated with this data offer. The access policy stated that only connectors registered with Mercedes-Benz and BMW BPNs can see the data offer.
2. Since data provider connector control plane will only allow MB and BMW to see the data offer, only connectors of those companies can accept the data offer and sign a data contract.
3. From that point on, only the connectors with valid data contract for that data offer, can establish the connection to the provider's data. However, both BMW and MB connectors

will be treated by the EDC as valid data exchange partners for this offer and both will be directed to the same endpoint.

4. From that point on - it is the back-end data provider app's responsibility to respond to the data request with appropriate payload (that is with the MB-relevant data for MB and with BMW-relevant data for BMW) - this is important!

Usage Policies

Similar to access policies, a data provider will be able to create a set of standardized usage policies in the process of data offer creation. They will be able to select pre-defined usage polices and modify their attributes or parameters and, if the pre-defined policies are not enough for the data to be shared, we will implement a free-form policy that will allow the data providers to add any number of text policies to the data offer.

It is important to note that, since these policies govern HOW the transmitted data can be used, these policies are not technically enforceable at present. However, since they are included in the data contract signed by both data exchange parties, the data consumer is legally bound to observe the policies and to execute them according to their conditions. An example of such a non-technically enforceable policy would be a policy stating that the transmitted data can only be used for a given number of days after which the data has to be deleted.

To provision for the technical enforcement of the usage policies in the future, we are planning to define a certification process for the vendor applications that would verify that the applications can access, read the usage policies and, most importantly, enforce them within their business logic implementation. This certification process would, most likely, be optional but it could be a supporting factor in market penetration of the commercial application that is certified to comply with C-X usage policies.

2. DATA SOVEREIGNTY GUARDRAILS

2.1. ACCESS POLICIES

BPN-based access policy: This policy will allow limiting access to a data offer based to a list of specific BPNs. This translates to the following functionality:

1. The data offer creator will be able to create a policy listing all the BPNs that can access the data offer
2. This means that only the connectors registered in DAPS with the BPNs listed in the policy can see the data offer and accept it (for the creation of data contracts and subsequent data exchange)

2.2. USAGE POLICIES

Migration Information: Due to fast development in the EDC, policy payloads and endpoints may change over time. Please always consider existing migration guides here. The current version is 0.1.2.

2.3. DURATION RESTRICTED DATA USAGE

Description: The data asset can only be used for a specific time. The duration of the usage time is defined in the policy itself. It starts counting after the contract agreement is made on the control plane, even before the data transfer itself is made on the data plane. Remember that this policy restricts only the usage time itself. It doesn't specify a concrete end date.

Attributes:

- **duration**: Time how long the data asset can be used.
  - The duration value is expressed based on the xsd:duration data type having the structure PnYnMnDTnHnMnS:
    - P: prefix indicating the start of the expression
    - nY: number of years followed by a literal Y
    - nM: number of months followed by a literal M
    - nD: number of days followed by a literal D
    - T: literal value that separates the date and time
    - nH: number of hours followed by a literal H
    - nM: number of minutes followed by a literal M
    - nS: number of seconds followed by a literal S

Sample payload:

```
{
  "id": "<PolicyId>",
  "policy": {
    "prohibitions": [],
    "obligations": [],
    "permissions": [
      {
        "edctype": "dataspaceconnector:permission",
        "action": {
          "type": "USE"
        },
        "constraints": [
          {
            "edctype": "AtomicConstraint",
            "leftExpression": {
              "edctype": "dataspaceconnector:literalexpression",
              "value": "idsc:ELAPSED_TIME"
            },
            "rightExpression": {
              "edctype": "dataspaceconnector:literalexpression",
              "value": "P2Y6M5DT12H35M30S"
            },
            "operator": "LEQ"
          }
        ]
      }
    ]
  }
}
```

2.4. ROLE-RESTRICTED DATA USAGE

Description: The data asset can only be used by specific persons or roles (e.g. a quality engineer is allowed to see the data asset while the risk department isn't allowed).

Attributes:

role: Array of the roles as string values that are allowed to use the data asset (e.g. "quality engineer")

For release #2, the role can be freely defined, without a list of possible names, an enum, vocabulary etc. Every use case can and should define their roles individually.

Sample payload:

```
{
  "id": "<PolicyId>",
  "policy": {
    "prohibitions": [],
    "obligations": [],
    "permissions": [
      {
        "edctype": "dataspaceconnector:permission",
        "action": {
          "type": "USE"
        },
        "constraints": [
          {
            "edctype": "AtomicConstraint",
            "leftExpression": {
              "edctype": "dataspaceconnector:literalexpression",
              "value": "idsc:ROLE"
            },
            "rightExpression": {
              "edctype": "dataspaceconnector:literalexpression",
              "value": [ "<Custom CX Role 1>", "<Custom CX Role 2>" ]
            },
            "operator": "IN"
          }
        ]
      }
    ]
  }
}
```

2.5. PURPOSE-RESTRICTED DATA USAGE

Description: The data asset can only be used for a specific purpose (e.g. only the quality investigation scenario is allowed to access the data asset). This policy is similar to the role restricted data usage policy.

Attributes:

purpose: Array of the purposes as string values (e.g. "quality investigation")

For release #2, the purpose can be freely defined, without a list of possible names, an enum, vocabulary etc. Every use case can and should define their purposes individually.

Sample payload:

```
{
  "id": "<PolicyId>",
  "policy": {
    "prohibitions": [],
    "obligations": [],
    "permissions": [
      {
        "edctype": "dataspaceconnector:permission",
        "action": {
          "type": "USE"
        },
        "constraints": [
          {
            "edctype": "AtomicConstraint",
            "leftExpression": {
              "edctype": "dataspaceconnector:literalexpression",
              "value": "idsc:PURPOSE"
            },
            "rightExpression": {
              "edctype": "dataspaceconnector:literalexpression",
              "value": [ "<Custom CX Purpose 1>", "<Custom CX Purpose 2>" ]
            },
            "operator": "IN"
          }
        ]
      }
    ]
  }
}
```

3. ENFORCING POLICIES

The table below illustrates which types of policies can be technically enforced and by which component as well as whether the implementation of the technical enforcement is planned for the PI5.

Category	Policy	Techinca l enforce ment planned for PI5	Technical enforceme nt possible by the connector ?	Comments

Access Policy	Limit access to the data offer to a list of specified BPNs (to the connectors with the BPN attribute listed in the policy)	Yes	Yes	This and any other policy which are based on attributes stored in DAPS can be enforced by the connector. So, if a connector is registered in DAPS with attributes such as BPN, Recycler, Germany, an access policy base on any combination of these attributes can be defined and technically enforced by the EDC
Usage Policy	Duration-restricted data policy	Yes	Yes	This policy specifies for how long the data contract is valid. After the expiry of the data contract, no data exchange under the conditions of this contract can take place. Since the connector is aware of when the contract was electronically signed, it can monitor the validity period and can invalidate the contract.
Usage Policy	Role-restricted data policy	No	No	These are the policies that require each use case to define their own set of "roles" such as quality engineer etc. These policies can only be enforced by the consumer applications. Note: keep in mind that this policy is different from any future access policy(ies) that would rely on a role of a company (such as Recycler). These roles, just like the BPN-based access policy, can be enforced by the connector
Usage Policy	Purpose-restricted data policy	No	No	These are the policies that require each use case to define their own set of "purposes" such as "CO2 emissions" etc. These policies can only be enforced by the consumer applications.

Application Access	Back-end application ACLs, RBAC, ABAC etc.	No	No	To clarify: the access control and datasets filtering in the back-end applications is the responsibility of the respective apps. The connector cannot enforce the rules such as "This subset of the data is only accessible to BMW and this subset to Bosch". If these data subsets are represented by a single data offer, the connector will only check if there is a valid contract before allowing the connection. If your back-end application (the one providing the data to the connector data plane) cannot enforce the access, then you will need to create separate data offers for BMW, Bosch etc and provide different endpoints in the offers for each as well as set up access policy limiting who can see the individual data offers based on the BPN numbers.

4. ECLIPSE DATA CONNECTOR (EDC) USER GUIDE

The Eclipse Dataspace Connector provides a framework for sovereign, inter-organizational data exchange. It will implement the International Data Spaces standard (IDS) as well as relevant protocols associated with GAIA-X. The connector is designed in an extensible way in order to support alternative protocols and integrate in various ecosystems. The EDC is built in a simple and efficient way with as little external dependencies as possible, to avoid third party dependencies as much as possible. The connector is a plain Java application built with Gradle, but it can be embedded into any form of application deployment.

General information about the EDC and its components (see figure 1) can be found on the following GitHub webpage:

https://eclipse-dataspaceconnector.github.io/docs/#/README

More details to the setup can be accessed on this page:

https://github.com/eclipse-dataspaceconnector/DataSpaceConnector

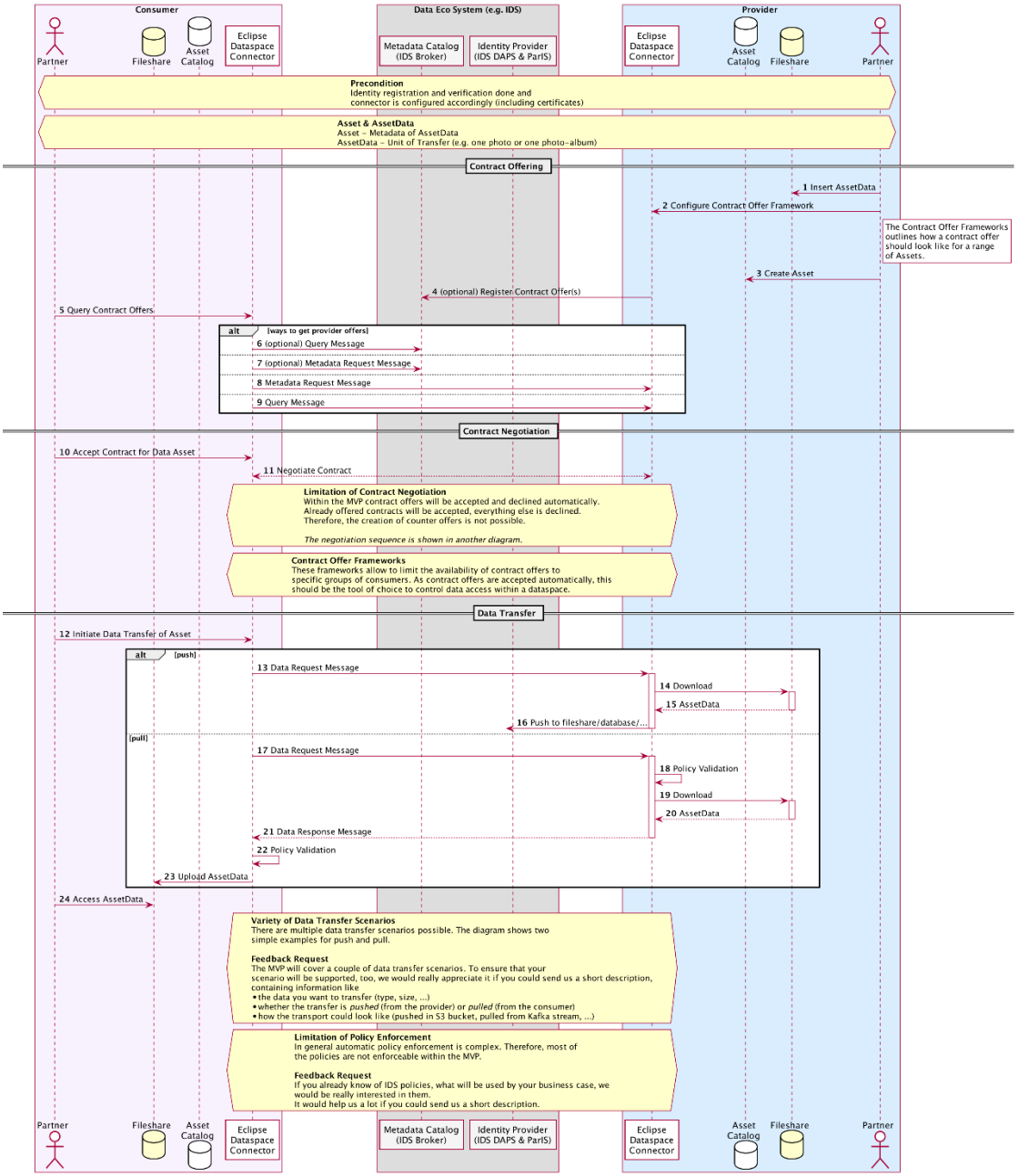


FIGURE 1: EDC ARCHITECTURE

The Catena-X Product EDC Repository creates runnable applications out of EDC extensions from the Eclipse DataSpace Connector repository. When running an EDC connector from the Product EDC repository there are three setups to choose from. They only vary by using different extensions for:

- Resolving of Connector-Identities
- Persistence of the Control-Plane-State
- Persistence of Secrets (Vault)

The instructions to the Connector Setup and to additional Documentation can be found at:

https://github.com/catenax-ng/product-edc/tree/develop/docs

The EDC consists of a Control Plan and a Data Plan Application. The Data Plane handles the actual Data transfer, and the Control Plane is responsible for:

- Resource Management
- Contract Offering and Contract Negotiation
- Data Transfer Coordination / Management

There are several confidential settings that should not be part of the actual EDC configuration file. As it is possible to configure EDC settings via environment variables, one way to do it would be via Kubernetes Secrets. For other deployment scenarios than Kubernetes equivalent measures should be taken.
Information about the EDC REST API and data policy creation can be found here:

https://eclipse-dataspaceconnector.github.io/docs/submodule/Connector/docs/swaggerui/index.html

5. DATA PROVISIONING APPLICATIONS – DATA SOVEREIGNTY CONSIDERATIONS

We need to ensure that all other data provisioning applications interact with EDC for both:

1. Creating data assets and associated policies to form contract offers
2. Awareness of EDC functionality related to the Data Sovereignty (contracts, data offers, usage and access policies etc.)

This section will include instructions for users from both SMBs and large organizations.

5.1. LARGE CORPORATIONS PERSPECTIVE - BUSINESS DOMAINS AND USE CASES

For each use case this is the minimum required set of conditions for the solution to pass the implementation quality gate:

I. For each data product offered by C-X association member acting in the capacity of the data provider, the solution has to be able to connect to the EDC control plane API and create the following:
   1. A corresponding data offer (matching the data product);
   2. An access policy based on the BPN-based policy implemented by the EDC API
   3. A set of usage policies as outlined in the document;
   4. Attach those policies to the data offer;
   5. Provide a view of the existing data offers created on a given instance of the connector (representing a location or department) including the review of the attached policies (either from within the application or via GUI tools provided by C-X consortium for SMB market);
   6. Optional: for increased visibility (for the management review or auditing purposes), Catena-X-facing solutions should also provide an overview of all the data offers (current, expired etc.) created for a company across multiple instances of EDC connectors;

II. Applications created or modified to connect to the EDC to create data offers and electronically sign data contracts should be able to provide a contract-review tooling that would allow C-X participants to review the contract offers that they have signed with other participants. It will be required for the purpose of internal company auditing.

1. Optional: for increased visibility (for the management review or auditing purposes), Catena-X-facing solutions should also provide an overview of all the data contracts (current, expired etc.)

6.2. SME PERSPECTIVE

It is understood that the capabilities of the small and medium companies participating in the Catena-X dataspace are limited compared to the large corporations which relay mostly on the commercial offerings from companies such as SAP etc. Vendors of those already are working on implementing integration features with Catena-X middleware. However, for the SMB market sector, these companies will most likely rely on software provided by the C-X consortium and deployed either in their own IT environment, or purchased as a service from the C-X service provider. In either case, the users of the C-X software will tend to rely on the Graphical User Interface rather than APIs and on relatively simple and convenient tools for data provisioning. These companies would also, most likely, rely on the onboarding process to provide them with the complete set of tools (henceforth referred to as C-X toolset) for all the use case they would need to participate in the C-X data exchange. Therefore, for each use case, the applications developed by C-X consortium must meet the following minimum requirements to pass the implementation quality gate:

I. For each data product offered by C-X association member acting in the capacity of the data provider, the C-X offered solution portfolio has to be able to create the following:

   1. A corresponding data offer (matching the data product) that's created either via a GUI or automatically and transparently to the user (as implemented in the Data Converter Tool, for instance);
   2. A BPN-based access policy implemented by the EDC. There must a be a convenient interface for the SMB users to create this policy and attach it to any given data offer that their C-X toolset generated;
   3. A set of usage policies as outlined in the section Usage Policies. There must a be a convenient interface for the SMB users to create these policies and attach it to any given data offer that their C-X toolset generated;
   4. Provide a view of the existing data offers created by the company including a review of the attached policies;

II. Applications created or modified to connect to the EDC to create data offers and electronically sign data contracts must be able to provide a contract-review tooling that would allow C-X participants to review the contract offers that they have signed with other participants. It will be required for the purpose of internal company auditing.

Optional: for increased visibility (for the management review or auditing purposes), Catena-X-facing solutions should also provide an overview of all the data contracts (current, expired etc.).

7. NEXT STEPS AND EVOLUTION OF EDC

EDC is provided as a reference implementation to be used to ensure interoperability of the data exchange until the underlying standards are fully defined and documented. It serves to unify the approach to sovereign data exchange and to incorporate and extend existing IDSA standards via reference implementation of the connector (EDC). Finally, it provides an actual implementation of the evolving standard for data offers, policies and contracts as well as interfaces to exchange and negotiate contracts for data exchange.

At present, the EDC API includes several extensions and workarounds to the original IDSA specification v1. Therefore, we work with IDSA to drive evolution of the IDSA data exchange protocol and specifications to incorporate EDC additions. Once the IDSA official specification is extended, it will become our reference for data exchange.

To encourage dataspace evolution, in our long-term development we ensure that:

1. Industry-proven protocol is used for data exchange in C-X dataspace
2. Software vendors can create their own software offerings that will be interoperable with other connectors and applications that are compliant with the IDSA protocol
3. There is a proven standard and implementation that other dataspaces can follow to facilitate cross-industry data exchange.

ADDENDUM FOR CONFORMITY ASSESSMENT

DISCLAIMER

The following pages are not part of the standard documentation.

CATENA-X

ADDENDUM FOR CONFORMITY ASSESSMENT

CX – 0018 ECLIPSE DATA SPACE CONNECTOR (EDC)

PLATFORM CAPABILITY: SOVEREIGN DATA EXCHANGE

Contact: standardisierung@catena-x.net

Note: Please specify the platform capability in the subject line.

TABLE OF CONTENTS

About this Document & Motivation 1
Disclaimer & Liability 2
Revisions & Update 3
Copyright & Trademarks 3
Abstract 4
1 Introduction 5
1.1 Audience & Scope 5
1.2 Context 5
1.2.1 Definition of Data Sovereignty in Catena-X 6
1.3 Architecture Overview 7
1.4 Conformance 9
1.5 Proof of conformity 9
1.5.1 Data Providers and Data Consumers 9
1.5.2 Application Providers 10
1.5.3 Application Vendors 10
1.6 Examples 10
1.6.1 Example 1: Data Provider and Data Consumer exchanging Demand and Capacity Management data 11
1.6.2 Example 2: Software Vendor offering an integrated Traceability solution for Catena-X participants 11
1.6.3 Example 3: Software Vendor creating a competitive solution for C-X Quality use case 11
1.7 Terminology 12
1.7.1 Connector 12
1.7.2 Association (frame) contract 12
1.7.3 Contract Offer 12
1.7.4 Access Policies 12
1.7.5 Usage Policies 13
2 Eclipse data space connector [NORMATIVE] 15
2.1 Application Developers (Connector) 15
2.1.1 Development and implementation of connectors other than EDC 15
2.2 Application Developers (Business Applications) 16

2.3 Data Providers and Consumers 18
2.4 Application Providers 18
3 References 19
3.1 Normative References 19
3.2 Non-Normative References 19
3.3 Reference Implementations 19

ABOUT THIS DOCUMENT & MOTIVATION

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.

The addendum for conformity assessment clarifies the requirements and scope for each standard. It contains conformity assessment criteria (CAC) that specify how a participant can receive a certificate for the correct application of the standard.

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.[1]

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.

[1] https://catena-x.net/fileadmin/user_upload/Vereinsdokumente/Catena-X_IP_Regelwerk_IP_Regulations.pdf

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.[1]

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.[1]

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

COPYRIGHT & TRADEMARKS

Any and all rights to the present document or parts of it, including but not limited under copyright law, are owned by Catena-X and its licensors.

The contents of this document shall not be copied, modified, distributed, displayed, made publicly available or otherwise be publicly communicated, in whole or in part, for any purposes, without the prior authorization by Catena-X, and nothing herein confers any right or license to do so.

The present document may include trademarks or trade names which are registered by their owners. Catena-X claims no ownership of these except for any which are indicated as being the property of Catena-X, and conveys no right to use or reproduce any such trademark or trade name contained herein. Mention of any third-party trademarks in the present document does not constitute an endorsement by Catena-X of products, services or organizations associated with those trademarks.

"CATENA-X" is a trademark owned by Catena-X registered for its benefit and the benefit of its members. Using or reproducing this trademark or the trade name of Catena-X is expressly prohibited.
No express or implied license to any intellectual property rights in the present document or parts thereof, or relating to the use of its contents, or mentioned in the present document is granted herein.
The copyright and the foregoing restrictions extend to reproduction in all media.
© Catena-X Automotive Network e.V. All rights reserved.

[1] https://catena-x.net/de/standard-library

ABSTRACT

This document highlights the importance of data sovereignty and its rules in the context of Catena-X. It commences by defining the data sovereignty components within Catena-X, followed by the definition of the Access Policy in the EDC connector. Then it emphasizes on the requirements necessary to implement the access and usage policies, which are stored in the Eclipse Data Connector (EDC). The EDC components also orchestrate the data exchange in the dataspace. Therefore, although data sovereignty is a much wider concept that the EDC implementation would imply, the Sovereign Data Exchange C-X Platform Capability concentrates on the EDC as the main component enabling and governing the data exchange process between the dataspace entities.

The EDC is explained in this document from a technical viewpoint. The interaction with other provisioning applications is stressed out from two company perspectives, the large corporation's perspective and the SME perspective.

For more information regarding the EDC relationship to the IDSA standard and future development of EDC please refer to the last chapter of this document.

1 INTRODUCTION

1.1 AUDIENCE & SCOPE

This section is non-normative

Any data exchange within Catena-X dataspace can only take place if there is an existing contract between the participants of the exchange. Eclipse Data Connector is the tool where the presence of the contract is maintained and verified and it also performs a role of the data exchange orchestrator. Therefore, this standard is relevant to:

- Data Provider / Consumer
- Business Application Provider
- Application Developer (Vendor) (this entity is not identified in the Catena-X Operting Principles white paper but, nevertheless, is relevant within Catena-X)

Any company participating in the dataspace as either data provider or data consumer has to use a connector compliant with the EDC interoperability specification. This is also relevant to Application Providers who will need to deploy connectors if they host business applications for Catena-X network participants (such as Simple Data Exchanger or any other applications build for C-X use cases). Finally, the Application Vendors will need to ensure that the applications they develop are compliant with the standard.

1.2 CONTEXT

This section is non-normative

The Eclipse Data Connector (EDC) enables data exchange across Catena-X dataspace while maintaining conditions of data sovereignty and interoperability. The EDC is an open-source software project that aims to provide a secure, scalable, and interoperable data sharing platform for distributed data-driven systems. The project is designed to allow organizations to securely share data and collaborate on data-driven projects, while maintaining control over their data and preserving data sovereignty. The project leverages the Eclipse technology stack, including the Eclipse P2 repository, to provide a flexible and extensible platform for data exchange and collaboration.
There are two important considerations setting up the CURRENT context of the standard:

1. At present the only connector compliant with the requirements of data exchange in C-X is the Eclipse Data Connector provided as a reference implementation.
2. Since the source code of the connector is freely available, developing EDC alternatives is possible and allowed, however not encouraged until the interoperability protocols are fully defined, standardized and published. As stated in the final chapter, our expectation is that the next version of the IDSA specification will include EDC extensions and therefore the IDSA specification v2 will become the official standard. Furthermore, we encourage any company requiring additional connector functionality to actively participate in the EDC project instead of creating their own solution.

1.2.1 Definition of Data Sovereignty in Catena-X

In the Catena-X context, Data Sovereignty is defined as the sum of the statements below:

- Data providers can control who can see their contract offers via access policies implemented in the C-X Eclipse Data Connector (EDC).
- Ability to exchange data only with the electronic contract present and accepted by both data provider and data consumer.
- Ability to exchange data only with the verified participants of the dataspace (companies who signed the so called Frame Contract with the C-X Operating Company).
- Data providers have ability to define usage policies (as currently implemented in the C-X EDC) and link them to their data assets – these policies represent a legal obligation on the side of the data consumers (legal and trust-based enforcement of usage policies)
    - DS can be augmented with the technical enforcement of the usage policies (whenever possible) through functionality build into the consumer applications and other technical means (in the future)
- Ability to leave or change any aspect of the participation in the dataspace without losing control over one's data, realized through:
    - ability to change any service provider within C-X dataspace and move the data from the old provider to the new one
    - ability to pull out of the use case or service provider application with the full data deletion (no data left behind). This is not technically enforced but represented by legal obligation.

On a very general level, data sovereignty aims to allow users to keep control over their data.

Data sovereignty is a principle that spans multiple layers of the dataspace ecosystem. These layers range from identity and attributes of the C-X network participants and services that are trusted and verifiable, through middleware provisions for DS such as ability to define access and usage policies, sign contracts

and verify the validity of the conditions before the data exchange takes place, and finally the end-user applications on both data consumer and data provider sides being able to integrate with the C-X services to read and enforce usage policies.

1.3 ARCHITECTURE OVERVIEW

This section is non-normative

The Eclipse Dataspace Connector provides a framework for sovereign, inter-organizational data exchange. It will implement the International Data Spaces standard (IDS) as well as relevant protocols associated with GAIA-X. The connector is designed in an extensible way in order to support alternative protocols and integrate in various ecosystems. The EDC is built in a simple and efficient way with as little external dependencies as possible, to avoid third party dependencies as much as possible. The connector is a plain Java application built with Gradle, but it can be embedded into any form of application deployment.
General information about the EDC and its components (see figure 1) can be found on the following GitHub webpage:
https://eclipse-dataspaceconnector.github.io/docs/#/README
More details about the setup can be accessed on this page:
https://github.com/eclipse-dataspaceconnector/DataSpaceConnector

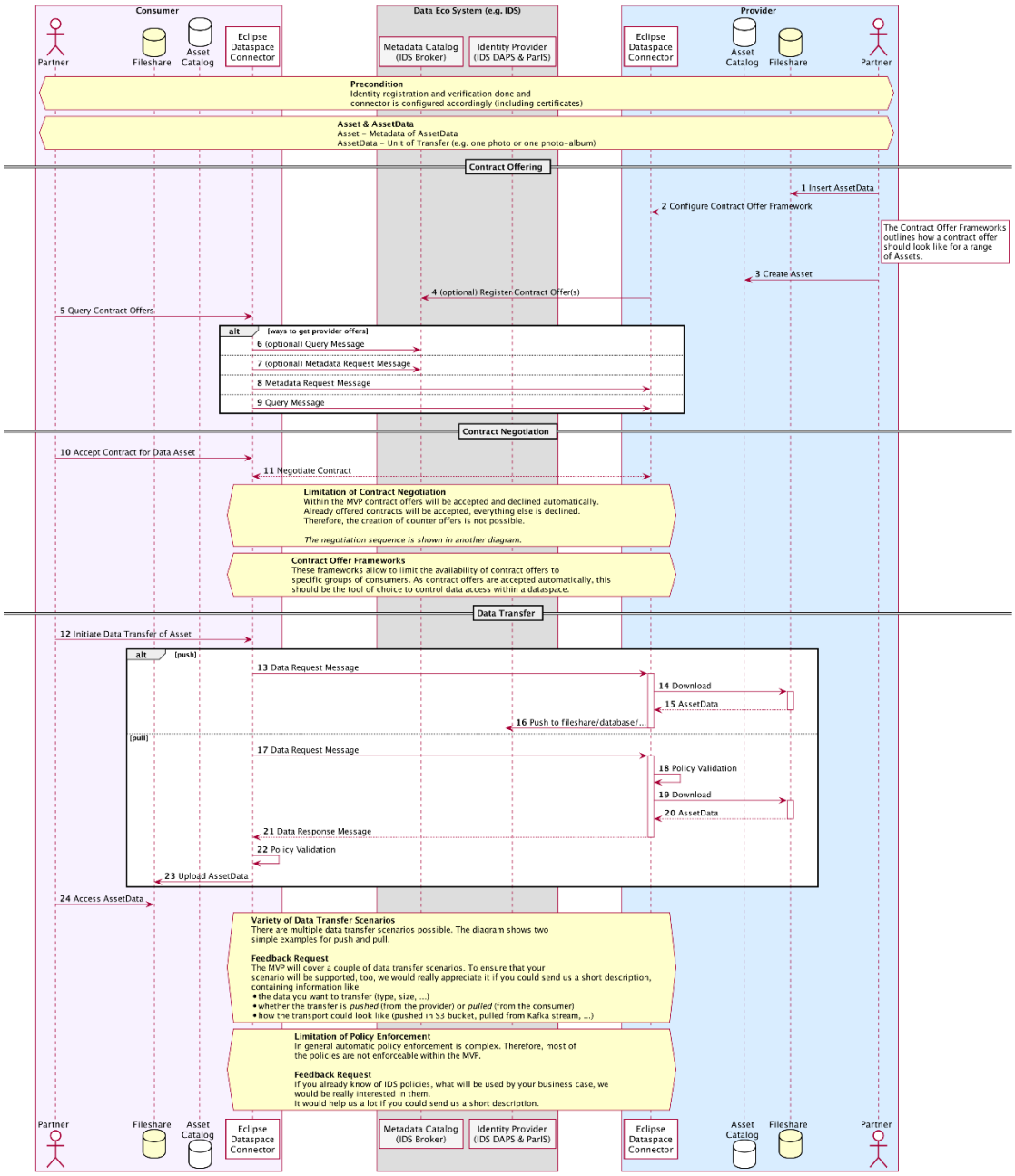


Figure 1: EDC Architecture

The Catena-X Product EDC Repository creates runnable applications out of EDC extensions from the Eclipse DataSpace Connector repository. When running an EDC connector from the Product EDC repository there are three setup options to choose among. They only vary by using different extensions for:

- Resolving of Connector-Identities
- Persistence of the Control-Plane-State
- Persistence of Secrets (Vault)

The instructions to the Connector Setup and to additional Documentation can be found at:
https://github.com/catenax-ng/product-edc/tree/develop/docs

The EDC consists of a Control Plan and a Data Plan Application. The Data Plane handles the actual Data transfer, and the Control Plane is responsible for:

- Resource Management
- Contract Offering and Contract Negotiation
- Data Transfer Coordination / Management

There are several confidential settings that should not be part of the actual EDC configuration file.

As it is possible to configure EDC settings via environment variables, one way to do it would be via Kubernetes Secrets. For other deployment scenarios than Kubernetes equivalent measures should be taken.

Information about the EDC REST API and data policy creation is located here: https://eclipse-dataspaceconnector.github.io/docs/submodule/Connector/docs/swaggerui/index.html

1.4 CONFORMANCE

This section is non-normative

As well as sections marked as non-normative, all authoring guidelines, diagrams, examples, and notes in this specification are non-normative. Everything else in this specification is normative.

The key words MAY, MUST, MUST NOT, OPTIONAL, RECOMMENDED, REQUIRED, SHOULD and SHOULD NOT in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

1.5 PROOF OF CONFORMITY

This section is non-normative

All participants and their solutions will need to prove, that they are conforming with the Catena-X standards. To validate that the standards are applied correctly, Catena-X employs Conformity Assessment Bodies (CABs). Please refer to: [!LINK Conformity Assessment] for the process of conformity assessment and certification.

1.5.1 Data Providers and Data Consumers

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

Connectors. At present the only connector implementation compliant with the standard is Catena-X EDC.

1.5.2 Application Providers

Application Providers need to ensure that the applications they offer as a managed services (AaaS or PaaS) comply with the standard of Catena-X. Therefore these applications MUST always use a connector for data exchange orchestration and the connector MUST be interoperable with other connectors deployed in the space via usage of the common protocol (IDSA v1 plus EDC project extensions). In the future the interoperability of the connectors will be governed by the IDSA Protocol V2).

1.5.3 Application Vendors

Business Application developed for use in Catena-X MUST follow IDSA specification for creating Data Assets, Contract Offers and orchestrating Data Exchange through connectors which are compliant with the EDC for interoperability. They also need to support the EDC Data Management API that provides an interface between the business applications and the connectors. The only exception from this rule is in case of the application vendor providing their applications along with their version of the connector with the management API optimized for the specific application. The API documentation for Business Application to Connector communication is available here:
https://eclipse-dataspaceconnector.github.io/docs/submodule/Connector/docs/swaggerui/index.html

1.6 EXAMPLES

This section is non-normative

The following examples are described based on the following dataspace participants:

1. Florence-Bens AG (FBAG) – major auto manufacturer
2. Hieronymus AG – tier 1 automotive supplier providing parts for DMW cars
3. SOAP AG– major software vendor providing business applications for the automotive industry
4. David GmbH – small software vendor creating niche software for specialized applications for C-X use case(s)
5. Magenta Systems – service provider for Catena-X

1.6.1 Example 1: Data Provider and Data Consumer exchanging Demand and Capacity Management data

FBAG and Hieronymus participate in the DCM use case that requires regular data exchange between them. Since they are active Catena-X members they decided to use the dataspace ecosystem to exchange the DCM data. Both sides MUST use a dataspace connector to maintain electronic data exchange contracts as well as to orchestrate the exchange. Since at present the only connector ensuring interoperability of the data exchange is EDC, this is the only option FBAG and Hieronymus can select to conform to the Sovereign Data Exchange standard.

1.6.2 Example 2: Software Vendor offering an integrated Traceability solution for Catena-X participants

SOAP decided to enhance their software portfolio by building the integrated solution for C-X Traceability use case that combines business functionality with the connector data exchange functions (i.e. business software with embedded connector). Since this solution is very tightly coupled, SOAP decided to create their own version of the data management API as an internal product to interface business functions with the connector functions. However, they still MUST ensure that their solution can communicate with other applications in the Traceability use case via the connectors deployed by the Catena-X participants. To ensure that, SOAP reverse-engineered current EDC code and extensively tested interoperability of their solution. In the future (once IDSA V2 is released) they will not need to reverse-engineer EDC but MUST ensure that their product is compliant with IDSA V2 via test bed provided by the EDC project.

1.6.3 Example 3: Software Vendor creating a competitive solution for C-X Quality use case

David GmbH created a competitive application offering a cognitive model that will significantly enhance the quality analysis performance for the users in Catena-X dataspace. Since David GmbH promotes this application to a multitude of companies participating in the dataspace, they designed their application to support the EDC Data Management API (EDC DM) that is used in the majority of the connectors deployed in Catena-X. It was not mandatory to use the EDC DM API as David could design their own connector and their own proprietary Data Management API (as SOAP did in the previous example). However, this would drastically increase the development costs and reduce the potential market penetration of their application as some of the potential clients would not want to add yet another version of the connector to their C-X infrastructure.

1.7 TERMINOLOGY

This section is non-normative

1.7.1 Connector

The Eclipse Dataspace Connector is an open-source software project that aims to provide a secure, scalable, and interoperable data sharing platform for distributed data-driven systems. The project is designed to allow organizations to securely share data and collaborate on data-driven projects, while maintaining control over their data and preserving data sovereignty. The project leverages the Eclipse technology stack, including the Eclipse P2 repository, to provide a flexible and extensible platform for data exchange and collaboration.

1.7.2 Association (frame) contract

Every company participating in the Catena-X dataspace will sign the membership contract that will state that the participant will be legally bound to observe the data policies associated with each data offer that the company will use. Each data offer can have a separate set of access and usage policies assigned to it.

1.7.3 Contract Offer

There will be no data exchange within the C-X unless both parties electronically sign data offer contract. The creation of this contract is triggered by the data consumer user accepting the data offer created previously by the data provider. Once the approval is made, an electronic contract is created by the EDC connector control plane which will include statements on all policies that the provider defined for this particular data offer. By accepting this offer, the data consumer company accepts the contract conditions and policies and agrees to be legally bound by them. After the contract is electronically signed, it is stored in the both data consumer and provider connectors.

1.7.4 Access Policies

Data provider will be able to create a set of standardized access policies in the process of creating a data offer. These access policies will limit who can see and access the data offers. There will be several criteria used in the access policies based on attributes that each participant of C-X will have. So, it will be possible to limit access to the data offer based, for instance, on the role of the data consumer and/or on the location of the company. An example of such a policy would be to limit access to the offer to a specific recycler based in Germany (location attribute). Since the access policies are based on attributes that can be read by the connector, they will be technically enforceable in the future (as opposed to most of the usage policies).

In preparation for the PI5, only a rudimentary set of access policies will be available but will be expanded during the PI5.

1.7.4.1 Clarification of Access Policies enforcement

Access policy in the connector does not mean that the connector will enforce back-end system data access rules (ACLs). Instead, the EDC Data Offer Access Policy limits who (which companies - or rather which connectors registered in DAPS) can access the data offers and data contracts. The scenario below illustrates that concept with the BPN-restricted access policy.

1. A data provider created a data offer and a BPN-restricted access policy associated with this data offer. The access policy stated that only connectors registered with Mercedes-Benz and BMW BPNs can see the data offer.
2. Since data provider connector control plane will only allow MB and BMW to see the data offer, only connectors of those companies can accept the data offer and sign a data contract.
3. From that point on, only the connectors with valid data contract for that data offer, can establish the connection to the provider's data. However, both BMW and MB connectors will be treated by the EDC as valid data exchange partners for this offer and both will be directed to the same endpoint.
4. From that point on - it is the back-end data provider app's responsibility to respond to the data request with appropriate payload (that is with the MB-relevant data for MB and with BMW-relevant data for BMW) - this is important!

1.7.5 Usage Policies

Similar to access policies, a data provider will be able to create a set of standardized usage policies in the process of data offer creation. They will be able to select pre-defined usage polices and modify their attributes or parameters and, if the pre-defined policies are not enough for the data to be shared, we will implement a free-form policy that will allow the data providers to add any number of text policies to the data offer.

It is important to note that, since these policies govern HOW the transmitted data can be used, these policies are not technically enforceable at present. However, since they are included in the data contract signed by both data exchange parties, the data consumer is legally bound to observe the policies and to execute them according to their conditions. An example of such a non-technically enforceable policy would be a policy stating that the transmitted data can only be used for a given number of days after which the data has to be deleted.

To provision for the technical enforcement of the usage policies in the future, we are planning to define a certification process for the vendor applications that would verify that the applications can access, read the usage policies and, most importantly, enforce them within their business logic implementation. This certification process would, most likely, be optional but it could be a supporting

factor in market penetration of the commercial application that is certified to comply with C-X usage policies.

Additional terminology used in this standard can be looked up in the glossary on the association homepage.

2 ECLIPSE DATA SPACE CONNECTOR [NORMATIVE]

2.1 APPLICATION DEVELOPERS (CONNECTOR)

For all companies which develop connectors (either as forks of the EDC project or new developments):

1. The IDS Protocol V.2 [LINK] MUST be implemented for Connector– to-Connector interoperability. Therefore, any connector deployed in the dataspace after the IDSA Protocol V2 is finalized MUST be compatible with that standard and the conformity will need to be confirmed by the software house which developed the given connector by testing it against the IDSA test bed.
    a. Clarification: since the IDSA Protocol V.2 is not available yet, any connector deployed in the C-X dataspace at present MUST be interoperable with the C-X EDC. This can be achieved by using the EDC itself or creating a competitive connector based on the reverse-engineered EDC functionality for interoperability. Please refer to the Context section of this document more information.

2.1.1 Development and implementation of connectors other than EDC

Eclipse Data Connector (EDC) is an open-source software project that aims to provide a secure, scalable, and interoperable data sharing platform for distributed data-driven systems. The project leverages the Eclipse technology stack, including the Eclipse P2 repository, to provide a flexible and extensible platform for data exchange and collaboration. Therefore, to reinforce the statement made previously in this document (Context section), developing EDC alternatives is possible and allowed, however not encouraged until the interoperability protocols are fully defined, standardized and published. The next version of the IDSA specification will include EDC extensions and therefore the IDSA specification v2 will become the official standard. Furthermore, we encourage any company requiring additional connector functionality to actively participate in the EDC project instead of creating their own solution.

1. All of the connectors (including EDC) MUST be compliant with the IDSA V.2 specification (long-term). Since this specification is not finalized, they MUST be interoperable with the existing Catena-X reference EDC implementation UNTIL the IDSA V.2 is published.
    a. The interoperability with the EDC MUST be confirmed using the following (or equivalent) process:
        i. Build a test environment with the EDC deployed

   ii. Test the full process of data asset and contract offer creation (including the currently implemented access and usage policies) as well as contract negotiation and data exchange execution.
   iii. Document the results
   iv. Submit the results for the CAB review
2. If the connector is a standalone connector designed to be compatible with business applications from other vendors, it SHOULD be compatible with the EDC Data Management API (documented here.

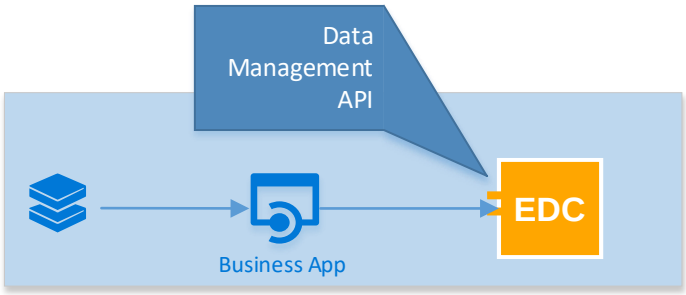
   https://eclipse-dataspaceconnector.github.io/docs/submodule/Connector/docs/swaggerui/index.html)

   a. If the vendor decides to implement their own version of the Data Management API AND the connector is to be used as a standalone connector to work with applications from multiple other vendors, the API specification MUST be published
   b. If the vendor decides to implement their own version of the Data Management API AND the connector is designed to work with their own business applications, the API specification MAY be published.
3. If the connector is developed by a vendor to work exclusively with the business application(s) from the same vendor (either standalone or embedded), it CAN use the EDC-defined data management API or it CAN use the vendor's own, proprietary API for data management.
4. Once the IDSA v2 is finalized and published, ALL of the connector products MUST be recertified for compliance with the new specification!

2.2 APPLICATION DEVELOPERS (BUSINESS APPLICATIONS)

The main requirement: the application MUST use a connector certified for Catena-X for any data exchange within the dataspace.

Data Management is the API that the business applications use to connect to the Connector for various tasks related data offer and data transfer orchestration.



Companies creating business application for Catena-X use cases typically have two choices of their implementation of the Data Management API:

1. Ensure that the application communicates with the connector using the reference Data Management API (DM API as implemented in EDC). In this case the application MUST be tested for its compliance with the DM API. DM API specification is available here:
   https://eclipse-dataspaceconnector.github.io/docs/submodule/Connector/docs/swaggerui/index.html)
   and the Application Developer MUST document that their application uses reference DM API
2. Develop their own version of the connector along with their business application and:
   a. Use the reference DM API as deployed in EDC and this MUST be documented
   b. Develop their own, proprietary version of the DM API and use it for communication between their Business Application(s) and their own Connector. In this case the connector MUST be compliant with the IDSA V.2 specification (long-term). Since this specification is not finalized, it MUST be interoperable with the existing Catena-X reference EDC implementation UNTIL the IDSA V.2 is published.
      The interoperability with the EDC MUST be confirmed using the following (or equivalent) process:
      i. Build a test environment with the EDC deployed
      ii. Test the full process of data asset and contract offer creation (including the currently implemented access and usage policies) as well as contract negotiation and data exchange execution.
      iii. Document the results
      iv. Submit the results for the CAB review
   c. Embed the connector functionality in the Business Application. In this case the vendor MUST ensure that the business application (via its embedded connector) is compliant with the IDSA V.2 specification (long-term). Since this specification is not finalized, it MUST be

interoperable with the existing Catena-X reference EDC implementation UNTIL the IDSA V.2 is published.
The interoperability with the EDC MUST be confirmed using the following (or equivalent) process:

v. Build a test environment with the EDC deployed
vi. Test the full process of data asset and contract offer creation (including the currently implemented access and usage policies) as well as contract negotiation and data exchange execution.
vii. Document the results
viii. Submit the results for the CAB review

2.3 DATA PROVIDERS AND CONSUMERS

The companies participating in the Catena-X data exchange MUST demonstrate that for the use cases within Catena-X dataspace they use:

1. Business applications that utilize Catena-X certified connector to manage and orchestrate data assets and data exchanges in the dataspace.
2. Only Catena-X-certified versions of the connectors – THIS IS OF PARAMOUNT IMPORTANCE as connectors are the gateways and gate keepers of the data exchange.

2.4 APPLICATION PROVIDERS

Similar to data providers and consumers, application providers hosting applications and connectors (as PaaS, SaaS) MUST demonstrate that for the Catena-X use cases they use:

1. Business applications that utilize Catena-X certified connector to manage and orchestrate data assets and data exchanges in the dataspace
2. Only Catena-X-certified versions of the connectors – THIS IS OF PARAMOUNT IMPORTANCE as connectors are the gateways and gate keepers of the data exchange.

3 REFERENCES

3.1 NORMATIVE REFERENCES

Link to the IDSA Specification V2: (awaiting the standard to be finalized)

3.2 NON-NORMATIVE REFERENCES

This section is non-normative

Link to the current IDSA DIN SPEC 27070 Specification: DIN SPEC - International Data Spaces

3.3 REFERENCE IMPLEMENTATIONS

This section is non-normative

The Catena-X Eclipse Data Connector reference implementation of this standard can be found at: ‹link›