

CATENA-X
STANDARD



CX - 0023 Notification API v.1.2.2

Contact: standardisierung@catena-x.net

Table of Contents

CX - 0023 Notification API v1.2.2

Table of Contents

ABOUT THIS DOCUMENT & MOTIVATION

DISCLAIMER & LIABILITY

REVISIONS & UPDATE

COPYRIGHT & TRADEMARKS

ABSTRACT

1. INTRODUCTION

1.1 AUDIENCE & SCOPE

1.2 CONTEXT

1.3 ARCHITECTURE OVERVIEW

1.4 CONFORMANCE

1.5 PROOF OF CONFORMITY

1.6 EXAMPLES

Example 1: Quality Investigation

Example 2: Quality Alert

1.7 TERMINOLOGY

2 Quality Notification API

2.1 Preconditions and dependencies

2.2 API Specification

2.2.1 API-Endpoints

2.2.2 Available Data Types

2.2.3 API resources & endpoints

2.3 EDC Data Asset Structure

2.3.1 EDC Data Asset for Notification Receive Endpoint for Quality Investigation Receipt

2.3.2 EDC Data Asset for Notification Receive Endpoint for Quality Alert Receipt

2.3.3 EDC Data Asset for Notification Update Endpoint for Quality Investigation Update

2.3.4 EDC Data Asset for Notification Update Endpoint for Quality Alert Update

2.3.5 EDC Data Asset for Notification Resolve Endpoint / Quality Investigation Resolve

(OPTIONAL)

2.3.6 EDC Data Asset for Notification Resolve Endpoint / Quality Alert Resolve (OPTIONAL)

2.4 Error Handling

2.4.1 Error Messages & Explanation

3 REFERENCES

3.1 NORMATIVE REFERENCES

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-CENELEC/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

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.

ABSTRACT

By leveraging network enabled traceability applications in conjunction with Catena-X as a network, the industry will be enabled to exchange and act upon quality issues in a more standardised, integrated, accelerated and precise manner. In order to achieve these goals, the traceability applications require standardized communication endpoints to exchange notifications, for example for quality issues or investigation requests. This document describes specific API endpoints and their integration into IDSA conform data assets, which each participating solution **MUST** implement in order to receive updates from other participants as notifications. When sending a notification the messages **MUST** be sent by calling the API behind the recipients IDSA conform data asset.

1. INTRODUCTION

Notifications are - in contrast to classical data offers in Catena-X - a way to push data from a sender to a receiver. For now, these are limited to the sending and receiving of quality notifications as well as the update of the notification status (following a predefined status model).

This document describes the relevant API endpoints to be created by each traceability application and their integration into the IDSA Protocol and/or the Eclipse Dataspace Connector (EDC).

This documentation covers exclusively the illustration of the specific API endpoints. The minimal process an application needs to support such notifications will not be handled here, but in a separate standard request [CX-0022].

1.1 AUDIENCE & SCOPE

This section is non-normative

This standard is relevant for the following roles:

Data Provider / Consumer

Business Application Provider

For now, the notification API is limited to the sending and receiving of quality notifications as well as the update of the notification status (following a predefined status model).

This document describes the relevant API endpoints to be created by each traceability application and their integration into the IDSA Protocol and/or the Eclipse Dataspace Connector (EDC) as a reference implementation.

This standard covers exclusively the definition of the API endpoints. The minimal process an application needs to support for such notifications will not be handled here, but in a separate standard request [CX-0022].

Furthermore, this standard has not the scope and intention to be a general solution pattern for notifications across various use cases. For now, it is limited to the sending and receiving of quality notifications and investigations in a traceability context.

1.2 CONTEXT

This section is non-normative

The notification API is used as part of the notification process of traceability.

In this regard it is important to mention, that the API standardized here is not a central API to be called, but an API to be implemented into each participant's traceability solution or solution stack in order to be able to receive information related to quality issues and notifications in the first place.

1.3 ARCHITECTURE OVERVIEW

This section is non-normative

This document describes the Data Asset Structure within the participant who wants to be able to receive notifications and/or updates to notifications. As the notification process includes bi-directional status communication, both entities in a process **MUST** provide these Data Assets and a linkage to corresponding APIs.

On top the document describes the payload of the notifications for quality investigations and quality alerts.

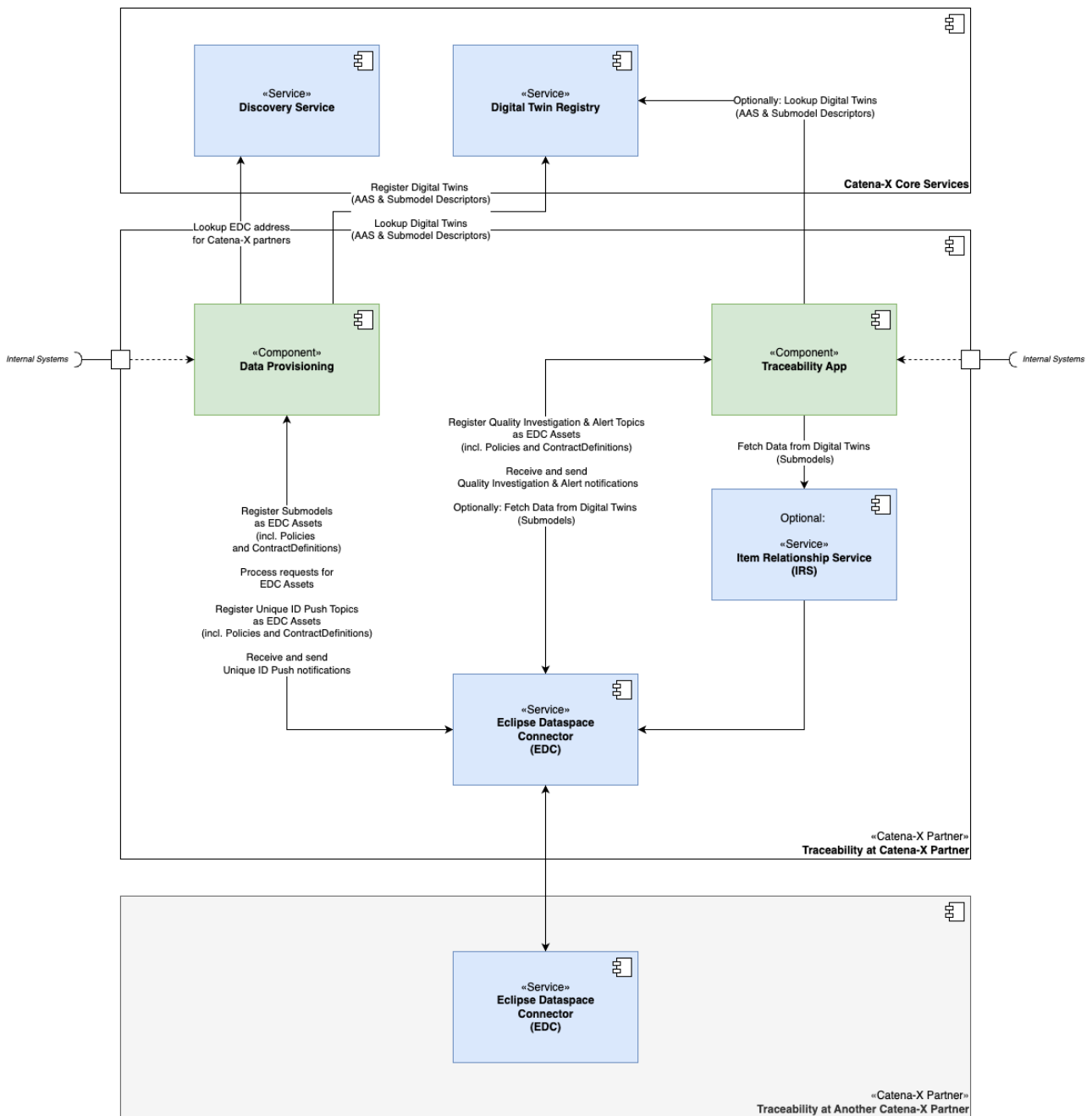


Figure 1: Architecture Overview

1.4 CONFORMANCE

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 app providers* and their solutions will need to prove, that they conform with the Catena-X standards. To validate that the standards are applied correctly, Catena-X employs Conformity Assessment Bodies (CABs).

In terms of conformity the openAPI specification of the application or endpoints being exposed via the EDC or any similar IDS conformant connector **MUST** be checked against the standardized openAPI specification.

Examples of data assets and contract offer structure in the EDC or any other IDS protocol compliant connector **MUST** correspond to the described structure.

**Disclaimer: The operating model released by the Catena-X association will define the roadmap, content and scope for the certification process. This will include the roles, certification and further assessment procedures as well as the rollout phases.*

1.6 EXAMPLES

Example 1: Quality Investigation

I discover a quality issue during assembly with several parts of a specific supplier. I want to inform him to perform a quality investigation on his side and want to communicate this data securely and sovereign to my supplier.

Example 2: Quality Alert

I discover a problem with specific batches or serialized parts on my end affecting also parts already shipped and want to communicate this data securely and sovereign to my customers.

1.7 TERMINOLOGY

This section is non-normative

Eclipse Dataspace Connector (EDC)

A reference implementation of an IDS protocol compliant connector

**International Data Space / International Data Space Association

(IDS/IDSA)**

The International Data Spaces Association (IDSA) is on a mission to create the future of the global, digital economy with International Data Spaces (IDS), a secure, sovereign system of data sharing in which all participants can realize the full value of their data.

IDS enables new "smart services" and innovative business processes to work across companies and industries while ensuring that the self-determined control of data use (data sovereignty) remains in the hands of data providers.

Application Programming Interface (API)

An application programming interface (API) is a way for two or more computer programs to communicate with each other.

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

Business Partner Number (BPN):

A BPN is the unique identifier of a partner within Catena-X.

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

2 Quality Notification API

This section is normative

2.1 Preconditions and dependencies

Application providers **MUST** proof their conformity by providing:

An openAPI specification of the endpoints described.

Examples of the data asset and contract definition structure in their EDC or any other IDS protocol compliant connector.

The notification API **MUST** be published towards the network using a Data Asset/Contract Definition in terms of the IDSA Protocol as described by the reference implementation [CX - 0018 Eclipse Data Space Connector (EDC)].

The Eclipse Dataspace Connector as a reference implementation **SHOULD** BE used and is referenced in this document. Other connectors fulfilling the same standards towards Catena-X **MAY** be leveraged as well.

It is of importance to mention, that there **MUST** be an API available behind each of the data offers described in the EDC, which works according to the openAPI specifications description.

Nevertheless, the APIs are **OPTIONAL** to follow the same structure, as there could even be APIs taking over the job of several of the endpoints mentioned.

The EDC **SHOULD** act as a reverse proxy towards those APIs, as it holds the Data Offers linked to the respective implemented endpoints.

2.2 API Specification

2.2.1 API-Endpoints

The notification API **MUST** be implemented as specified in the openAPI documentation as stated here: [openAPI](#)

The notification API **MUST** implement four endpoints similar to:

- POST /qualityinvestigations/receive
- POST /qualityinvestigations /update
- POST /qualityalert /receive
- POST /qualityalert/update

In addition, the notification API **MAY** implement two endpoints similar to:

- POST /qualityinvestigations /resolve
- POST /qualityalert/resolve

In fact, it is **OPTIONAL** to implement the endpoint paths exactly as described above. The reason is that those endpoints are not called from any supply chain partner directly. Rather, they are called from the Eclipse Dataspace Connector (EDC) as part of EDC data assets. In that sense, it is just important to implement endpoints that can process the defined request body and respond with the HTTP status codes and - if required - reply with the defined response body.

The EDCs data assets will act similar to a reverse proxy for the notification endpoints, therefore rather the EDC data assets are of significance, which **SHOULD** be exposed towards Catena-X through the Data

Offer Catalogues in the EDC or any other IDSA Protocol compatible connector.

2.2.2 Available Data Types

The notification API **MUST** use JSON as the payload transported via HTTP.

2.2.3 API resources & endpoints

The HTTP POST endpoints introduced in this standard **MUST** be called via Data Space Protocol.

The sending and receiving of notifications **MUST** be built on the basis of HTTP POST endpoints.

2.3 EDC Data Asset Structure

2.3.1 EDC Data Asset for Notification Receive Endpoint for Quality Investigation Receipt

When using the EDC, the following asset **MUST** be registered. Other connectors implementing the IDSA Protocol require a similar data asset with the same structure and provisioning towards Catena-X.

```
{
  "@context": {},
  "asset": {
    "@type": "Asset",
    "@id": "qualityinvestigationnotification-receipt",
    "properties": {
      "asset:prop:id": "qualityinvestigationnotification-receipt",
      "asset:prop:name": "Asset to receive quality investigations",
      "asset:prop:contenttype": "application/json",
      "asset:prop:type": "notification.trace.qualitynotification",
      "asset:prop:notificationtype": "qualityinvestigation",
      "asset:prop:notificationmethod": "receive"
    }
  },
  "dataAddress": {
    "@type": "DataAddress",
    "baseUrl": "https://{httpServerWhichOffersTheHttpEndpoint}/qualityinvestigations/receive",
    "proxyMethod": "true",
    "proxyBody": "true",
    "proxyPath": "true",
    "type": "HttpData"
  }
}
```

The variable `{httpServerWhichOffersTheHttpEndpoint}` **MUST** be set to the HTTP server that offers the endpoint. The path `/qualityinvestigations/receive` **MAY** align with the HTTP POST path as stated in Section 2.2.1. In that sense it can change dependent on the traceability application.

2.3.2 EDC Data Asset for Notification Receive Endpoint for Quality Alert Receipt

When using the EDC, the following asset **MUST** be registered. Other connectors implementing the IDSA Protocol require a similar data asset with the same structure and provisioning towards Catena-X.

```

{
"@context": {},
"asset": {
"@type": "Asset",
"@id": "qualityalertnotification-receipt",
"properties": {
"asset:prop:id": "qualityalertnotification-receipt",
"asset:prop:name": "Asset to receive quality alerts",
"asset:prop:contenttype": "application/json",
"asset:prop:type": "notification.trace.qualitynotification",
"asset:prop:notificationtype": "qualityalert",
"asset:prop:notificationmethod": "receive"
}
},
"dataAddress": {
"@type": "DataAddress",
"baseUrl": "https://{{httpServerWhichOffersTheHttpEndpoint}}/qualityalert/receive",
"proxyMethod": "true",
"proxyBody": "true",
"proxyPath": "true",
"type": "HttpData"
}
}

```

The variable `{{httpServerWhichOffersTheHttpEndpoint}}` **MUST** be set to the HTTP server that offers the endpoint. The path `/qualityalerts/receive` **MAY** align with the HTTP POST path as stated in Section 2.2.1. In that sense it can change dependent on the traceability application.

2.3.3 EDC Data Asset for Notification Update Endpoint for Quality Investigation Update

When using the EDC the following asset **MUST** be registered. Other connectors implementing the IDSA Protocol require a similar data asset with the same structure and provisioning towards Catena-X.

```

{
"@context": {},
"asset": {
"@type": "Asset",
"@id": "qualityinvestigationnotification-update",
"properties": {
"asset:prop:id": "qualityinvestigationnotification-update",
"asset:prop:name": "Asset to update quality investigations",
"asset:prop:contenttype": "application/json",
"asset:prop:type": "notification.trace.qualitynotification",
"asset:prop:notificationtype": "qualityinvestigation",
"asset:prop:notificationmethod": "update"
}
},
"dataAddress": {
"@type": "DataAddress",

```

```

"baseUrl": "https://{{httpServerWhichOffersTheHttpEndpoint}}/qualityinvestigation/update",
"proxyMethod": "true",
"proxyBody": "true",
"proxyPath": "true",
"type": "HttpData"
}
}

```

The variable `{{httpServerWhichOffersTheHttpEndpoint}}` **MUST** be set to the HTTP server that offers the endpoint. The path `/qualityinvestigation/update` **MAY** align with the HTTP POST path as stated in Section 2.2.1. In that sense it can change dependent on the traceability application.

2.3.4 EDC Data Asset for Notification Update Endpoint for Quality Alert Update

When using the EDC the following asset **MUST** be registered. Other connectors implementing the IDSA Protocol require a similar data asset with the same structure and provisioning towards Catena-X.

```

{
"@context": {},
"asset": {
"@type": "Asset",
"@id": "qualityalertnotification-update",
"properties": {
"asset:prop:id": "qualityalertnotification-update",
"asset:prop:name": "Asset to update quality alerts",
"asset:prop:contentType": "application/json",
"asset:prop:type": "notification.trace.qualitynotification",
"asset:prop:notificationtype": "qualityalert",
"asset:prop:notificationmethod": "update"
}
},
"dataAddress": {
"@type": "DataAddress",
"baseUrl": "https://{{httpServerWhichOffersTheHttpEndpoint}}/qualityalert/update",
"proxyMethod": "true",
"proxyBody": "true",
"proxyPath": "true",
"type": "HttpData"
}
}

```

The variable `{{httpServerWhichOffersTheHttpEndpoint}}` **MUST** be set to the HTTP server that offers the endpoint. The path `/qualityalerts/update` **MAY** align with the HTTP POST path as stated in Section 2.2.1. In that sense it can change dependent on the traceability application.

2.3.5 EDC Data Asset for Notification Resolve Endpoint / Quality Investigation Resolve (OPTIONAL)

When using the EDC, the following asset **MUST** be registered. Other connectors implementing the IDSA Protocol require a similar data asset with the same structure and provisioning towards Catena-X.

```

{
"@context": {},
"asset": {
"@type": "Asset",
"@id": "qualityinvestigationnotification-resolve",
"properties": {
"asset:prop:id": "qualityinvestigationnotification-resolve",
"asset:prop:name": "Asset to resolve quality investigations",
"asset:prop:contenttype": "application/json",
"asset:prop:type": "notification.trace.qualitynotification",
"asset:prop:notificationtype": "qualityinvestigation",
"asset:prop:notificationmethod": "resolve"
}
},
"dataAddress": {
"@type": "DataAddress",
"baseUrl": "https://{{httpServerWhichOffersTheHttpEndpoint}}/qualityinvestigations/resolve",
"proxyMethod": "true",
"proxyBody": "true",
"proxyPath": "true",
"type": "HttpData"
}
}

```

The variable `{{httpServerWhichOffersTheHttpEndpoint}}` **MUST** be set to the HTTP server that offers the endpoint. The path `/qualityinvestigations/resolve` **MAY** align with the HTTP POST path as stated in Section 2.2.1. In that sense it can change dependent on the traceability application.

2.3.6 EDC Data Asset for Notification Resolve Endpoint / Quality Alert Resolve (OPTIONAL)

When using the EDC the following asset **MUST** be registered. Other connectors implementing the IDSA Protocol require a similar data asset with the same structure and provisioning towards Catena-X.

```

{
"@context": {},
"asset": {
"@type": "Asset",
"@id": "qualityalertnotification-resolve",
"properties": {
"asset:prop:id": "qualityalertnotification-resolve",
"asset:prop:name": "Asset to resolve quality alerts",
"asset:prop:contenttype": "application/json",
"asset:prop:type": "notification.trace.qualitynotification",
"asset:prop:notificationtype": "qualityalert",
"asset:prop:notificationmethod": "resolve"
}
},
"dataAddress": {
"@type": "DataAddress",

```

```

"baseUrl": "https://{{httpServerWhichOffersTheHttpEndpoint}}/qualityalert/resolve",
"proxyMethod": "true",
"proxyBody": "true",
"proxyPath": "true",
"type": "HttpData"
}
}

```

The variable `{{httpServerWhichOffersTheHttpEndpoint}}` **MUST** be set to the HTTP server that offers the endpoint. The path `/qualityalerts/resolve` **MAY** align with the HTTP POST path as stated in Section 2.2.1. In that sense it can change dependent on the traceability application.

2.4 Error Handling

HTTP standard response codes **MUST** be used.

2.4.1 Error Messages & Explanation

The following http response codes **MUST** be defined for HTTP POST endpoint to receive a quality alert and quality investigation notification:

Code	Description
201	Quality notification was received successfully
400	Request body was malformed
401	Not authorized
403	Forbidden
405	Method not allowed
409	Could not accept the send quality notification, because a quality notification with that notificationId already exists
422	Could not accept the send quality notification even though it is syntactically correct. The quality notification is not accepted, because of semantic reasons (e.g., an affected item is not known by the receiver)

The following http response codes **MUST** be defined for HTTP POST endpoint to update a quality alert and quality investigation notification:

Code	Description
200	Quality notification was updated successfully
400	Request body was malformed
401	Not authorized
403	Forbidden
404	Could not update the quality notification, because a quality notification with that notificationId does not exist
405	Method not allowed

422	Could not update the quality notification even though the request is syntactically correct. The quality notification update is not accepted, because of semantic reasons (e.g., status cannot be changed)
-----	---

The following http response codes **MUST** be defined for HTTP POST endpoint to resolve a quality alert and quality investigation notification:

Code	Description
200	Quality notification was resolved successfully. The response body has properties, which are listed in the table below.
400	Request body was malformed
401	Not authorized
403	Forbidden
404	Could not resolve the quality notification, because a quality notification with that notificationId does not exist
405	Method not allowed

3 REFERENCES

3.1 NORMATIVE REFERENCES

CX - 0022 NOTIFICATION PROCESS

CX - 0018 ECLIPSE DATA SPACE CONNECTOR (EDC)

EDC Reference Implementation -

<https://github.com/eclipse-tractusx/tractusx-edc>