

**CATENA-X**  
STANDARD



## **CX - 0014 IDENTITY OF EMPLOYEES AND TECHNICAL USERS**

PLATFORM CAPABILITY: IDENTITY ACCESS MANAGEMENT (IAM)

Contact: [standardisierung@catena-x.net](mailto: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](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](mailto: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. Purpose .....	4
2. Identity of Technical User .....	4
3. Identity of Employees .....	6
Figure 1: IDS essential services and DAPS .....	5

## INTRODUCTION AND OVERVIEW

Identity and Access Management (IAM) is a mandatory basic infrastructure for every IT-System. The identity of any entity and actor (company, user, or technical client/connector) is the summary of the describing attributes (e.g., Company Name, Address, Tax Number, etc.). Catena-X is intended to be a network-of-networks which consequently means that there cannot be a single Identity Provider (IdP) for the company identities nested in one network. The company must be identifiable in an independent way and interoperable in all networks. The identity of users (employees of a company) and technical users (e.g., EDC) in Catena-X, must be bound to the company they are acting on behalf of.

### 1. PURPOSE

The purpose of this standardization request is to standardize the digital identity of technical users and employees who are bound to the company they operate for. The goal is to protect data. It ensures that permissions and users can be managed in all systems and applications.

### 2. IDENTITY OF TECHNICAL USER

A technical user is a non-generic user used for example for system-to-system communication such as the Eclipse Data Space Connector (EDC).

The digital identity of a user is always tied to the company for which the user acts within the context of Catena-X. For example, there is no "User A" acting within Catena-X, there is only "User A of Company Z".

Technical User	
IAM Tasks:	<ul style="list-style-type: none"><li>• Provision of Technical User ID</li><li>• Management of Technical User ID</li><li>• Provision of verifiable Technical User attributes</li><li>• Management of verifiable Technical User attributes<ul style="list-style-type: none"><li>○ Revoke</li></ul></li></ul>

	<ul style="list-style-type: none"> <li>○ Renew</li> <li>● Exchange of verifiable Technical User attributes</li> <li>● Authentication</li> </ul>
Defined Standards for sub-capability:	IDS (will be replaced by SSI)
Technical Components:	DAPS (will be replaced by Managed Identity Wallet)

International Data Spaces (IDS) is a distributed network of Data Endpoints (i.e., instantiations of the International Data Spaces Connector), allowing the secure exchange of data and guaranteeing Data Sovereignty. Figure 1 shows the Catena-X IDS Essential Services, which includes DAPS.

IDS connectors request a digitally signed JSON web token (JWT) from a central IDS component called Dynamic Attribute Provisioning Service (DAPS) to authenticate themselves. Without these DAPS tokens (DATs) no connector can participate in the IDS.

The repository is open source and can be accessed at GitHub:

<https://github.com/International-Data-Spaces-Association/omejdn-daps>

Further documentation about the IDS Identity Provider and DAPS can be seen here:

<https://github.com/International-Data-Spaces-Association/IDS-G/blob/main/Components/IdentityProvider/README.md>

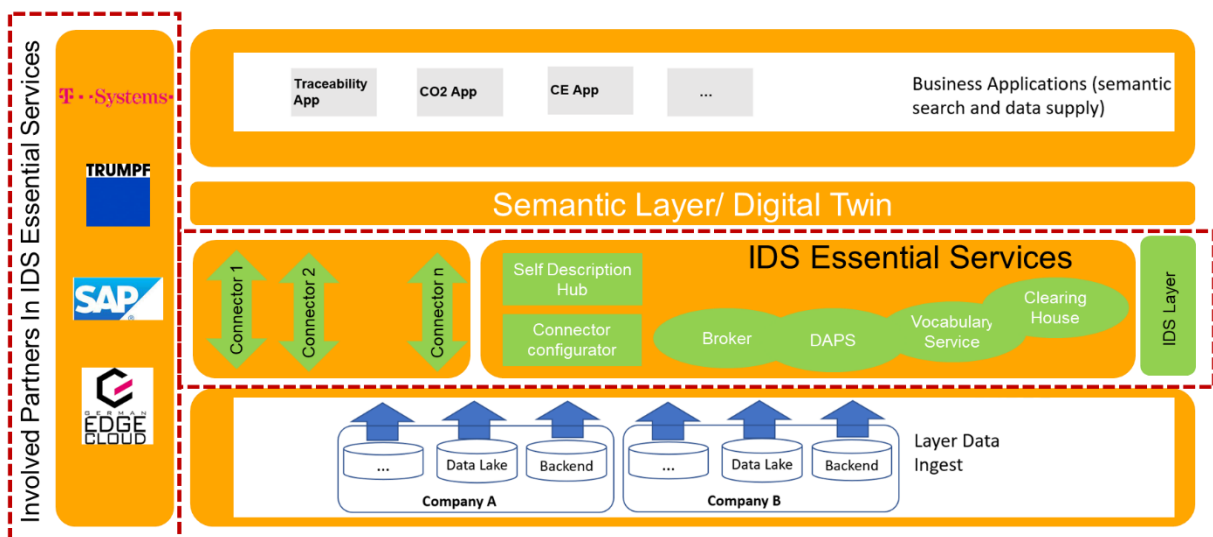


FIGURE 1: IDS ESSENTIAL SERVICES AND DAPS

However, Catena-X wants to move to Self Sovereign Identity (SSI) soon. This requires a wallet for each company to store their private keys to issue verifiable credentials. Not each company will own such a wallet when they join Catena-X. Therefore, during onboarding, each company shall receive a Custodian Wallet to store. SSI and the Custodian Wallet are described in detail in IAM-001 “Identity representing the company that is a member in Catena-x”.

### 3.IDENTITY OF EMPLOYEES

An employee is a regular generic user whose digital identity is also always tied to the company for which he or she acts in the context of Catena-X. The tasks of the IAM are the same as those for technical users, but the technical components are different.

Employee / User	
IAM Tasks:	<ul style="list-style-type: none"> <li>• Provision of User ID</li> <li>• Management of User ID</li> <li>• Provision of verifiable User attributes</li> <li>• Management of verifiable User attributes               <ul style="list-style-type: none"> <li>○ Revoke</li> <li>○ Renew</li> </ul> </li> <li>• Exchange of verifiable User attributes</li> <li>• Verification of User attributes</li> <li>• Authentication</li> </ul>
Defined Standards for sub-capability:	OpenID Connect (OIDC)
Technical Components:	Keycloak

OpenID Connect (OIDC) is an identity layer on top of the OAuth 2.0 protocol. It allows clients to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User in an interoperable and REST-like manner.

Keycloak is an open-source Identity and Access Management tool, which is used as the single sign-on solution for the OIDC implementation.

Publicly available developer documentation can be found on <https://www.keycloak.org/> and GitHub (<https://github.com/keycloak/keycloak>). Moreover, there is also documentation for OpenID Connect available: <https://openid.net/connect/>. Moreover, OIDC and Keycloak are described in detail in IAM-003 “Identity and Access Management & Access control paradigm for users and clients”.

**ADDENDUM FOR CONFORMITY ASSESSMENT**

**DISCLAIMER**

**The following pages are not part of the standard documentation.**

**CATENA-X**

ADDENDUM FOR CONFORMITY  
ASSESSMENT



## **CX - 0014 EMPLOYEES AND TECHNICAL USERS**

PLATFORM CAPABILITY: IDENTITY & ACCESS MANAGEMENT (IAM)

**Contact:** [standardisierung@catena-x.net](mailto:standardisierung@catena-x.net)

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



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
1.3 Conformance .....	5
1.4 Proof of conformity .....	5
1.5 Terminology.....	6
2 Main Content .....	7
3 References .....	8
3.1 Normative References .....	8

## 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.<sup>1</sup>

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.

---

<sup>1</sup> [https://catena-x.net/fileadmin/user\\_upload/Vereinsdokumente/Catena-X\\_IP\\_Regelwerk\\_IP\\_Regulations.pdf](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.<sup>1</sup>

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.<sup>1</sup>

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

---

<sup>1</sup> <https://catena-x.net/de/standard-library>

## **ABSTRACT**

Identity and Access Management (IAM) is a mandatory basic infrastructure for every IT-System. The identity of any entity and actor (company, user, or technical client/connector) is the summary of the describing attributes (e.g., Company Name, Address, Tax Number, etc.). Catena-X is intended to be a network-of-networks which consequently means that there cannot be a single Identity Provider (IdP) for the company identities nested in one network. The company must be identifiable in an independent way and interoperable in all networks. The identity of users (employees of a company) and technical users (e.g., EDC) in Catena-X, must be bound to the company they are acting on behalf of.

# 1 INTRODUCTION

## 1.1 AUDIENCE & SCOPE

*This section is non-normative*

List for which roles the standard is relevant:

- Core Service Provider
- Data Provider / Consumer
- Business Application Provider
- Enablement Service Provider
- Onboarding Service Provider
- Consulting Services Provider

This Standard applies to all participants and their representative that interact with each other. The representatives can either be the employees –or users of a participant- or the technical users –in case of Catena-X the EDCs- of a participant.

## 1.2 CONTEXT

*This section is non-normative*

Standardization of the digital identity of technical users and employees who are bound to the company they operate for. The goal is to protect data. It ensures that permissions and users can be managed in all systems and applications.

## 1.3 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.

## 1.4 PROOF OF CONFORMITY

*This section is non-normative*

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

A test bed must be set up, to prove the correctness of the data provisioning. A generic test set of data must get processed, to prove the expected results.

## **1.5 TERMINOLOGY**

*This section is non-normative*

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

## 2 MAIN CONTENT

**This standard is not certifiable yet (only release 3.1 onwards)**

Core Service provider MUST prove that they apply to the OIDC standard found on the spec [Specifications | OpenID](#) to manage the identities and access policies described in **CX - 0015 IAM & ACCESS CONTROL PARADIGM FOR USERS AND CLIENTS** which

- must be reachable by other partners
- ownership must be verifiable

Core Service provider MUST prove that they provide a managed identity solution based on OIDC. Core Service provider MUST prove that they make the use for a self-hosted IdP based on OIDC possible for any participant. If a core service provider provides an OIDC service he MUST prove that every customer has its own delimited area for his users and that no users of any customer has access to any data of another customer. The users of a specific customer must be assignable to only the customer they belong to.

To validate these criteria for the OIDC service please collect the following documents:

- Arch42 Documentation explaining the architecture, access management and process flows of the implementation
- The URI / URL of the OIDC instance

Hand this documentation to the conformity assessment body

An operating environment which provides an OIDC service SHOULD operate an OIDC instance that supports Attribute Based Access Control described in the following standard [[Guide to Attribute Based Access Control \(ABAC\) Definition and Considerations \(nist.gov\)](#)]

A technical user (e.g. EDC) MUST provide at least the BPN of the Data Consumer/ Producer as an attribute inside the OIDC token at any interaction.

To validate these criteria for the OIDC service please collect the following documents:

- Arch42 Documentation explaining the architecture, access management and process flows of the implementation

Hand this documentation to the conformity assessment body



## 3 REFERENCES

### 3.1 NORMATIVE REFERENCES

- CX - 0015 IAM & ACCESS CONTROL PARADIGM