CATENA-X

STANDARD

CX - 0015 IAM & ACCESS CONTROL PARADIGM FOR USERS AND CLIENTS

PLATFORM CAPABILITY: IDENTITY ACCESS MANAGEMENT (IAM)

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

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

As Identity and Access Management (IAM) is a mandatory basic infrastructure for every IT-System Catena-X will offer an implementation of an IAM solution of some sort for e.g., SMEs and rights/roles management within the CX network. 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…). Catena-X is intended to be a network-of-networks. Consequently, 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.

To realize this, a decentralized and dynamic IAM must be established. Here, for the interaction between a providing and a consuming company, the providing company must be able to grant access to a user of a consuming company. To realize this, a roles-and-rights concept must be realized that allows a dynamic authorization assignment to the user of a consuming company in a consistent way. To prevent a role explosion and ensure future scalability with the rising complexity, the dynamic access control will be based on consistent user attributes assigned to the user by the consuming company and processed by the providing company implemented by OpenID Connect and an attribute-based access control (ABAC) mechanism.

1. PURPOSE

The purpose of this standardization is to establish a decentralized and dynamic IAM for the interaction between a providing and a consuming company based on ABAC.

2. OPENID CONNECT

Apps define their rights-and-roles concept independently of Catena-X. The roles (not permissions) that the app uses are created/registered in Catena-X as part of the integration into the CX portal.

As soon as an end-user subscribes to an app, the corresponding roles can be assigned to him directly in the portal. Furthermore, member companies shall be able to federate their user base into the CX Network, so that the end-user has a seamless experience from the company network to the business app. Permission federation from member company IdPs into the CX IdP is currently out of scope.

The currently only used authentication protocol is OpenID Connect (OIDC). Here, OpenID Connect 1.0 is a simple 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. Its flow of actions is depicted in Fig. 4:

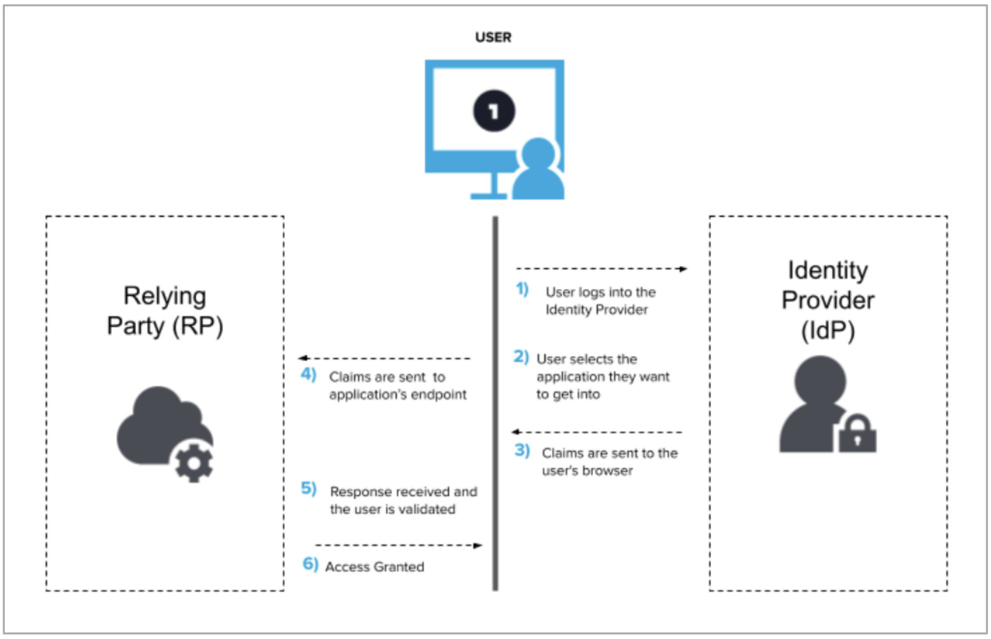

USER
1
Relying Party (RP)
Identity Provider (IdP)
1) User logs into the Identity Provider
2) User selects the application they want to get into
3) Claims are sent to the user's browser
4) Claims are sent to application's endpoint
5) Response received and the user is validated
6) Access Granted

FIGURE 1: OpenID Connect Flow of Actions

The corresponding authentication flow of users logging into Catena-X is then as follows:

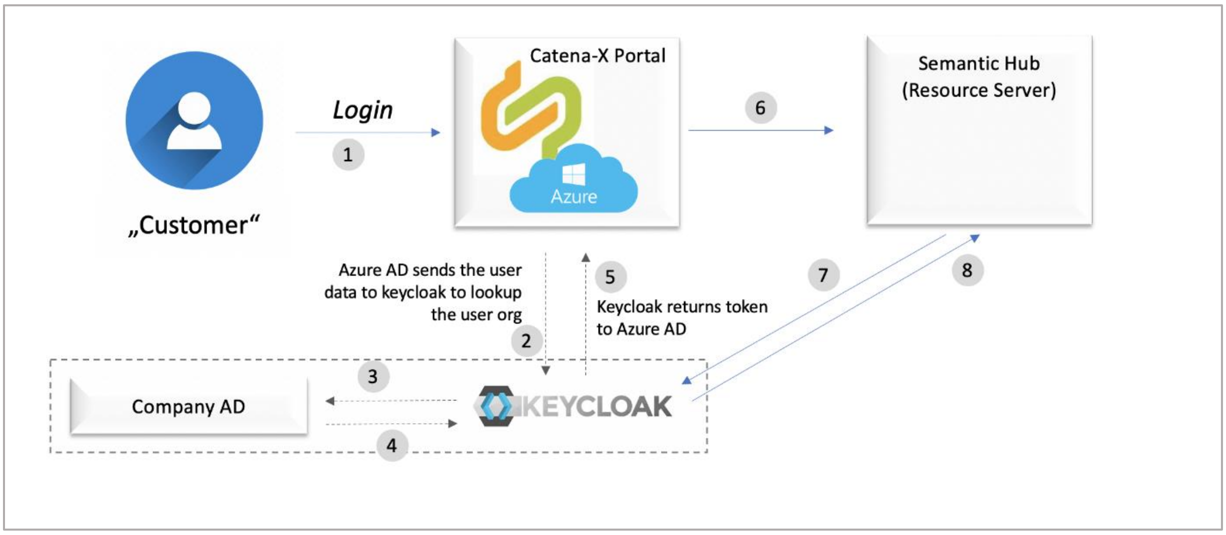

„Customer“
Login
1
Catena-X Portal
Azure
6
Semantic Hub (Resource Server)
Azure AD sends the user data to keycloak to lookup the user org
2
5
Keycloak returns token to Azure AD
7
8
3
4
Company AD
KEYCLOAK

FIGURE 2: Authentication Flow – User Login to Catena-X

In general, Keycloak is used as the single-sign-on solution for the OIDC implementation. Keycloak is an Open-Source IAM solution, this means that it is an authentication and authorization Java-based server. Keycloak is developed by Red Hat and can be deployed to OpenShift using its official Docker image. Red Hat is a trusted entity for IT Security, so this project is also trustable. In terms of features, Keycloak provides a login page that can be customized to match the app theme. Single-sign-on allows the user to log in once to access all the apps. Moreover, Keycloak follows standard protocols such as OAuth 2.0, OIDC 1.0, SAML 2.0 and supports multi-factor authentication as well as social logins, such as Google, Facebook, and Twitter. It provides centralized user management, which creates a single point of truth to set the permissions of users and roles and is also supporting directory services.

The main structure in Keycloak is called Realm. It is a container that stores all the other elements. Clients are applications that are to be secured, while Identity-Providers (IdP) give the possibility to log in via an external IdP. In addition, user federation uses the Keycloak login page with an external user store and themes modify Keycloak's login page to match the corporate solution. Moreover, Keycloak's login page uses Angular and users can be assigned to roles per Realm or per client.

Different IdPs are available for Keycloak, whereas OIDC is selected for Catena-X as a connection to WebEAM.Next could be secured by using OIDC. With it, the WebEAM.Next login could authenticate the user and generate its token.

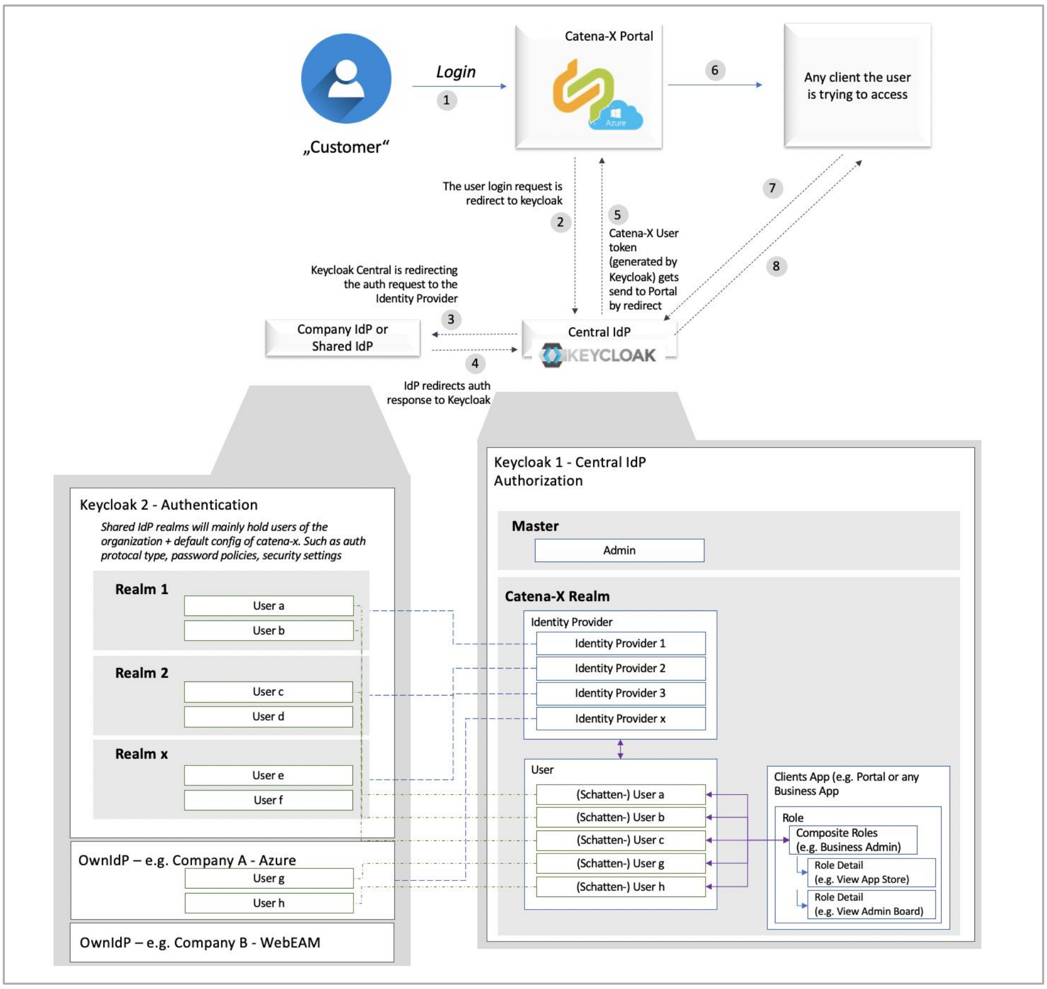
Furthermore, Quarkus has an extension to use Keycloak to manage OIDC. The extension will map the URIs of the protected resources of Keycloak and evaluate the permissions, accordingly, granting or denying access depending on the permissions that will be conferred by Keycloak. Following the official Quarkus/Keycloak guide, the Quarkus properties set the details of the connection between the two systems.

Essentially, Keycloak authenticates the user at the first server the access with a username and password takes place. After the authentication, the user receives a Keycloak token that is valid for only one session. The token is used to identify the user on other servers in the same Domain Name System where the servers are configured to use Keycloak. Hence, the user enters a username and password only once, while there is also only one access to the user directory to verify the identity of that user.

To setup KeyCloak the following steps must be followed:

1. Install Keycloak
2. Load balancer / Cluster Concept
3. Configure Master
4. Create Realms
5. Create Clients
6. Define one or more Roles for the client. The roles correspond to EBICS Client permissions that are used by EBICS Client in access control. Note: In this version of EBICS Client, there is one unique, global-access role.
7. Optionally, you can create Groups, which are logical groupings or sets of permissions.
8. Create Users. These are the users who will be able to access the EBICS Client application.
9. Assign roles to the users.

Overall, the final interaction between Keycloak and CX web applications looks as follows:


„Customer"
Login
1
Catena-X Portal
Azure
6
Any client the user is trying to access
The user login request is redirect to keycloak
2
5
Catena-X User token (generated by Keycloak) gets send to Portal by redirect
7
8
Keycloak Central is redirecting the auth request to the Identity Provider
3
Company IdP or Shared IdP
Central IdP
KEYCLOAK
4
IdP redirects auth response to Keycloak
Keycloak 2 - Authentication
Shared IdP realms will mainly hold users of the organization + default config of catena-x. Such as auth protocal type, password policies, security settings
Realm 1
User a
User b
Realm 2
User c
User d
Realm x
User e
User f
OwnIdP – e.g. Company A - Azure
User g
User h
OwnIdP – e.g. Company B - WebEAM
Keycloak 1 - Central IdP Authorization
Master
Admin
Catena-X Realm
Identity Provider
Identity Provider 1
Identity Provider 2
Identity Provider 3
Identity Provider x
User
(Schatten-) User a
(Schatten-) User b
(Schatten-) User c
(Schatten-) User g
(Schatten-) User h
Clients App (e.g. Portal or any Business App
Role
Composite Roles (e.g. Business Admin)
Role Detail (e.g. View App Store)
Role Detail (e.g. View Admin Board)

Note: (Schatten-) User: The „Schatten-User" is defined as an empty User frame holding limited information. The actual user is managed in the respective Identity Provider. The Schatten-User are always federated identities.

FIGURE 3: INTERACTION BETWEEN KEYCLOAK AND C-X WEB APPLICATIONS

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/.

3. ATTRIBUTE-BASED ACCESS CONTROL (ABAC)

While role-based access control (RBAC) determines access based on a user's organizational role, ABAC uses user and object attributes to do this. The flexible use and combination of variables increase the flexibility and accuracy of authorization assignment and is used for the purpose of Catena-X.

ABAC in Catena-X is realized through eXtensible Access Control Markup Language (XACML) therefore five XACML roles are defined first, as follows:

Role-Abbr.	Role-Term	Role Description
PAP	Policy Administration Point	Point which manages access authorization policies
PDP	Policy Decision Point	Point which evaluates access requests against authorization policies before issuing access decisions
PEP	Policy Enforcement Point	Point which intercepts user's access request to a resource, makes a decision request to the PDP to obtain the access decision (i.e., access to the resource is approved or rejected), and acts on the received decision
PIP	Policy Information Point	The system entity that acts as a source of attribute values (i.e., a resource, subject, environment)
PRP	Policy Retrieval Point	Point where the XACML access authorization policies are stored, typically a database or the filesystem.

Given the XACML roles, the corresponding flow of actions is depicted in Fig. 7 along with their explanations.

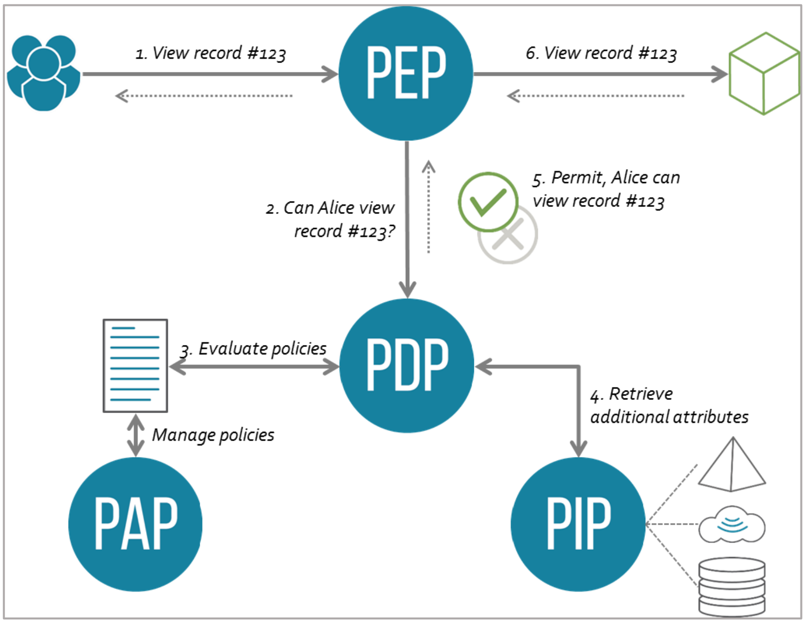

1. View record #123
PEP
6. View record #123
2. Can Alice view record #123?
5. Permit, Alice can view record #123
3. Evaluate policies
PDP
4. Retrieve additional attributes
Manage policies
PAP
PIP

FIGURE 4: FLOW OF ACTIONS (XACML)

1. A user sends a request which is intercepted by the Policy Enforcement Point (PEP)
2. The PEP converts the request into an XACML authorization request
3. The PEP forwards the authorization request to the Policy Decision Point (PDP)
4. The PDP evaluates the authorization request against the policies it is configured with.
5. The policies are acquired via the Policy Retrieval Point (PRP) and managed by the Policy Administration Point (PAP).
6. If needed it also retrieves attribute values from underlying Policy Information Points (PIP).

7. The PDP reaches a decision (Permit / Deny / NotApplicable / Indeterminate) and returns it to the PEP

The presented approach is realized in Catena-X as follows:

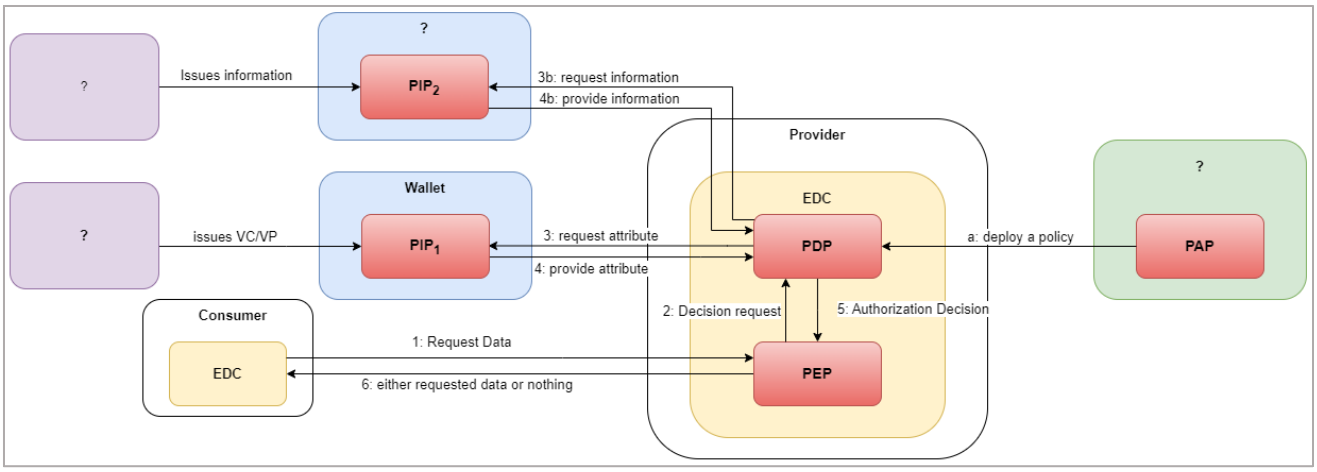


FIGURE 5: XACML REALIZATION IN CATENA-X

Further Information about XACML in the context of international data spaces can be found in the position paper by the IDSA:

https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-Position-Paper-Usage-Control-in-the-IDS-V3..pdf.

In addition, GitHub contains frontend and backend developer documentation with regards to the IAM:

GitHub Frontend: https://github.com/catenax-ng/product-portal-frontend

GitHub Backend: https://github.com/catenax-ng/product-portal-backend

ADDENDUM FOR CONFORMITY ASSESSMENT

DISCLAIMER

The following pages are not part of the standard documentation.

CATENA-X

ADDENDUM FOR CONFORMITY
ASSESSMENT

CX - 0015 IAM & ACCESS CONTROL PARADIGM

PLATFORM CAPABILITY: IDENTITY & ACCESS MANAGEMENT

Contact: standardisierung@catena-x.net
Note: Please specify the platform capability in the subject line.

TABLE OF CONTENTS

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.

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

ABSTRACT

As Identity and Access Management (IAM) is a mandatory basic infrastructure for every IT-System Catena-X will offer an implementation of an IAM solution of some sort for e.g., SMEs and rights/roles management within the CX network. 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…). Catena-X is intended to be a network-of-networks. Consequently, 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.

To realize this, a decentralized and dynamic IAM must be established. Here, for the interaction between a providing and a consuming company, the providing company must be able to grant access to a user of a consuming company. To realize this, a roles-and-rights concept must be realized that allows a dynamic authorization assignment to the user of a consuming company in a consistent way. To prevent a role explosion and ensure future scalability with the rising complexity, the dynamic access control will be based on consistent user attributes assigned to the user by the consuming company and processed by the providing company implemented by OpenID Connect and an attribute-based access control (ABAC) mechanism.

INTRODUCTION

1.1 AUDIENCE & SCOPE

This section is non-normative

List for which roles the standard is relevant:

- Data Provider / Consumer
- Business Application Provider
- Onboarding Service Provider

1.2 CONTEXT

This section is non-normative

Standardization for the establishment of a decentralized and dynamic IAM for the interaction between any participant based on ABAC.

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

All Business Application Provider SHOULD provide an identity and access management for the users of the Data Consumers and Service Customers that

- SHOULD NOT have a static Access Management like
  - An Access Control List (ACL)
  - A Role Based Access Control (RBAC) method
- SHOULD have a dynamic access management based on policies rules and attribute repositories

If a dynamic access management is not provided then it SHOULD be either

- An Access Control List (ACL)
- A Role Based Access Control (RBAC) method

An application provided by a Business Application Provider SHOULD have an implementation of the following four building blocks

- Policy Administration Point
- Policy Decision Point
- Policy Information Point
- Policy Enforcement Point

These building blocks can be a single dedicated function in the application.

Every Application provided by a Business Application Provider MUST prevent unauthorized access to the Application. Especially valuable goods must be protected from unauthorized access by a 3rd party.

To proof that these the access management compo, please collect the following documentation so that conformance with the standard can be validated:

- Arch42 Document explaining the architecture of the implemented solution
- openAPI specification of the APIs of the implemented solution.

Hand in this documentation to the conformity assessment body.

https://github.com/eclipse-tractusx/item-relationship-service

3 REFERENCES

3.1 NORMATIVE REFERENCES

- INCITS 565-2020 - Information Technology - Next Generation Access Control (NGAC): webstore.ansi.org

3.2 NON-NORMATIVE REFERENCES

- Guide to ABAC: Guide to Attribute Based Access Control (ABAC) Definition and Considerations (nist.gov)