

Conformity Assessment Framework Handbook – Release Saturn (Minor Release Titan)

Catena-X Automotive Network e.V.

18.03.2026



Table of contents

The Handbook on the Conformity Assessment Framework covers the central questions of certification

Table of contents of the CAF handbook

1. Abstract
2. CAB (Conformity Assessment Body)
 - a. Definition of the role CAB & tasks of the CAB
 - b. Requirements for a CAB
 - c. Relationship between the Catena-X association and CAB
3. CAF (Conformity Assessment Framework)
4. CX Standards in the context of CAF
 - a. CX Standards in context CAF – CX Standards
 - b. CX Standards in context CAF – Audience & Scope and normative references
 - c. CX Standards in the context of CAF – Conformity Assessment Criteria and proof of conformity
 - d. Roles in the Catena-X ecosystem
 - e. Certification objects: provider and solution
5. Modular certification system in the context of CX Standards
 - a. Guidance modular certification
 - b. Certification objects: modular system apps
 - c. Certification objects: modular system apps example
6. Certification catalog
 - a. Structure of the certification catalog
 - b. Structure of certification catalog – column content
7. Test procedures
 - a. Test procedures overview
 - b. Test procedures – inspection and observation
 - c. Assessment methods – self-assessment and inquiry
 - d. Test procedures – confirmation and recalculation
 - e. Test procedures– reperformance and analytical procedures
 - f. Test procedures - inherent testing
 - g. IPE – Information Produced by Entity
8. Certification process
 - a. Certification process
 - b. Process for certification over time
 - c. Example to test the semantic model
 - d. Example to check the API
 - e. Example to check other CAC
 - f. List of requirements and template
 - g. Self-assessment and template for declaration of completeness and correctness
 - h. Feedback from CAB
9. The Catena-X certificate
 - a. Catena-X certificate
 - b. Certification identification
 - c. Backward compatibility
10. Up-to-date status of certifications
 - a. The update process of the framework
 - b. Updating and maintaining the certification catalog
 - c. Decision tree for the update process
 - d. RASCI matrix on responsibilities
11. Miscellaneous
 - a. Redundancy-free information

List of abbreviations

Abbreviation	Designation	Abbreviation	Designation
API	Application Programming Interface	IoT	Internet of Things
BPDM	Business Partner Data Management	IPE	Information Produced/Provided by Entity
BPN	Business Partner Number	ISO	International Organization for Standardization
CAB	Conformity Assessment Body	OSIM	Online control and simulation
CAC	Conformity Assessment Criteria	PCF	Product Carbon Footprint
CAF	Conformity Assessment Framework	PLM	Product Lifecycle Management
CMC	Certification Management Center	PURIS	Predictive Unit Real-Time Information Service
CX	Catena-X Automotive Network e.V., the association	R&D	Research and Development
EDC	Eclipse Dataspace Connector	SD	Self Description
ESS	Environmental and Social Standards	SDE	Simple Data Exchanger
IAM	Identity and Access Management	SUS	Sustainability
ID	Identification		
IDSA	International Data Spaces Association		
IDW	Institut der Wirtschaftsprüfer in Deutschland e.V. [Institute of Public Auditors in Germany, Incorporated Association]		

Structure of the document

The Handbook on the Conformity Assessment Framework covers the central questions of certification

The individual chapters of the handbook provide an overview of the parties involved and the certification process. The chapters contain the following information:

The **Abstract** offers a first introduction to Catena-X and the certification.

The chapter on "**CAB**" explains what a CAB is, which tasks it performs in the Catena-X ecosystem, which requirements have to be fulfilled and how it relates to Catena-X. Following the CAB, the "**CAF**" and its components are explained. Building up on this, the chapter "**CX Standards in the Context of CAF**" first gives an overview of "Audience & Scope" as well as "Normative References". Furthermore, the "CAC" and the "Proof of Conformity" are defined in more detail. In addition, this chapter describes the certification objects "Provider and Solution" along with the "Roles" and "Use Cases".

The following chapter "**Modular system in the context of CX Standards**" defines the modular system and provides an explanation of how to use it on the basis of examples. Below the chapter "**Certification catalog**" shows the structure of the certification catalog and explains the individual column contents in more detail.

The „**Test procedures**“ are explained in detail. In addition, it is shown what an inherent test can look like and what the documents and proofs must look like according to IPE specifications.

The chapter "**Certification process**" describes the certification process from the request to the awarding of the certificate. Building on this, the certificate and its individual components are shown in the next chapter.

The chapter "**Up-to-date status of certifications**" explains the update process triggered by the existing standards and through the introduction of new standards, which are considered in the certification process.

The chapter "**Other**" gives an explanation of redundancy-free information.

In the last chapter the "**Innovation Board**" is presented and its definition as well as further information.



1. Abstract



Abstract



Catena-X is the automotive industry's first collaborative and open data ecosystem. Global and regional players can connect and form multi tier collaborations and eventually end-to-end digital twins of their respective business processes. To ensure simple, secure and independent participation in this data ecosystem, compliance with Catena-X specifications is verified and ensured by certificates. This certificate serves to strengthen trust in data exchange and ensure interoperability between the various players and solutions. Another fundamental aspect of Catena-X is self-sovereignty, which enables independent participation in the data ecosystem. Industry governance is ensured by the Catena-X Automotive Network e.V. (the association), which sets the standards, regulates the certification framework (CAF) and selects and commissions the Conformity Assessment Bodies (CABs).

A Catena-X certificate is based on the published Catena-X standards and the awarding of the certificate is uniformly regulated in the certification framework (CAF). The CAF includes, among other things, the Catena-X standards, the Conformity Assessment Criteria (CAC) and the testing methods. Compliance with these standards contributes significantly to interoperability in the ecosystem by defining uniform requirements for data formats and interfaces. The concepts of self-sovereignty are addressed, for example, by the requirements for identity and access management (IAM) in the standards. The trust that has been built up is strengthened by the transparent certification process and independent auditing by the CABs. Industry governance by the association ensures that the standards and the CAF are continuously developed and kept up to date.

Conformity Assessment Bodies (CABs) are companies selected and commissioned by Catena-X to carry out the certification of solutions and providers. The CABs work closely with Catena-X's Certification Management Centre (CMC) and within the limits of the CAF. They check compliance with the Catena-X standards, which specify the principles of interoperability, self-sovereignty and trust. The CABs thus contribute to the enforcement of industry governance by checking compliance with the rules laid down by the association (initial certification, re-certification and while usage).

Certification is carried out in a modular approach in accordance with the Catena-X standards and the CAF procedure. This modular approach enables certification applicants, with the support of Catena-X, to select the Catena-X standards relevant to them in order to obtain certification for their individual constellation. This flexible approach takes into account the different roles and use cases in the ecosystem, while at the same time ensuring the fundamental principles of interoperability, self-sovereignty and trust, governed by industry governance.

2. CAB (Conformity Assessment Body)



Definition of the role & tasks of the CAB

Conformity Assessment Bodies (CAB) carry out conformity assessments as part of the certification process in the Catena-X ecosystem

Conformity Assessment Body

Definition: CAB

Conformity Assessment Bodies are commissioned by the association* to carry out independent conformity assessments (certifications) according to the specifications of the Conformity Assessment Framework– consisting of a certification catalog and a certification handbook.

A CAB must meet certain eligibility requirements in order to be nominated as a CAB and to perform certifications for Catena-X. The requirements are defined under "Requirements for a CAB".

Tasks: CAB

- **Processing of certification requests** through the direct contact of certification applicants with the CAB (CABs are listed on the CX homepage)
- **Preparation of individual contract offers** between the CAB and certification applicants according to the specifications of the Catena-X Framework
- **Conducting the certification** or the re-certification according to the specifications of the Catena-X Framework
- **Preparation of an audit opinion** along with forwarding and announcement to Catena-X
- **Awarding the certificates on behalf of Catena-X** after successful assessments
- **Providing systematic feedback** of the experience gained from the completion of the certification and the applicability of the CX Standards

* In the following, the term „association“, "CX" or "Catena-X" always refers to the Catena-X Automotive Network e.V. Different designations are listed separately, e.g. Catena-X consortium

Requirements for a CAB

A company that wants to assume the role of the Conformity Assessment Body in the Catena-X ecosystem must meet the following minimum requirements and prove this to Catena-X



Relationship between the Catena-X association and CAB

The Conformity Assessment Body acts in close coordination with the Certification Management Center (CMC) of Catena-X and within the limits of the Conformity Assessment Framework

Certification Management Center | Catena-X:

- Publishes standards, incl. CAC
- Updates the certification catalog based on the standards
- Elects and nominates CABs
- Establishes contact – directly or via the homepage – between a CAB and certification applicants
- Defines the validity of the certificate
- Validates authenticity of certificates



CAB

- Acts in close coordination with Catena-X (CMC)
- Is being contacted directly by the certification applicant via an info on the CX homepage
- Prepares offers for certification of certification applicants
 - Certifies according to the specifications of the CAF
 - Hands over the certification result to Catena-X
- Provides certificates to Catena-X and awards certificates on behalf of Catena-X
 - Performs plausibility checks of the evidence

3. CAF (Conformity Assessment Framework)



CAF (Conformity Assessment Framework)

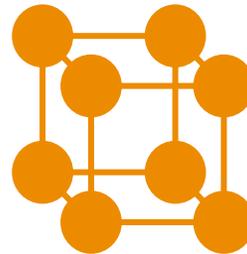
The Conformity Assessment Framework includes the certification catalog and the handbook

The CAF certification catalog is the basis and the core of the certification. The certification catalog includes

- CX Standards
- Addendums of the standards
- Application of the respective test procedure for a CAC
- Assignment of standards to certification objects

Certification Catalog

Conformity Assessment Framework



Handbook

The CAF handbook is used for operationalization of the certification catalog. The handbook defines the

- Conformity Assessment Body (CAB)
- Conformity Assessment Framework (CAF)
- Catena-X Standards in the context of the framework
- The modular system of certification with the integration of standards
- Certification catalog
- Test procedures
- Certification process
- The certificate
- Up-to-date status of certifications (update process)
- Redundancy-free information
- Innovation Board

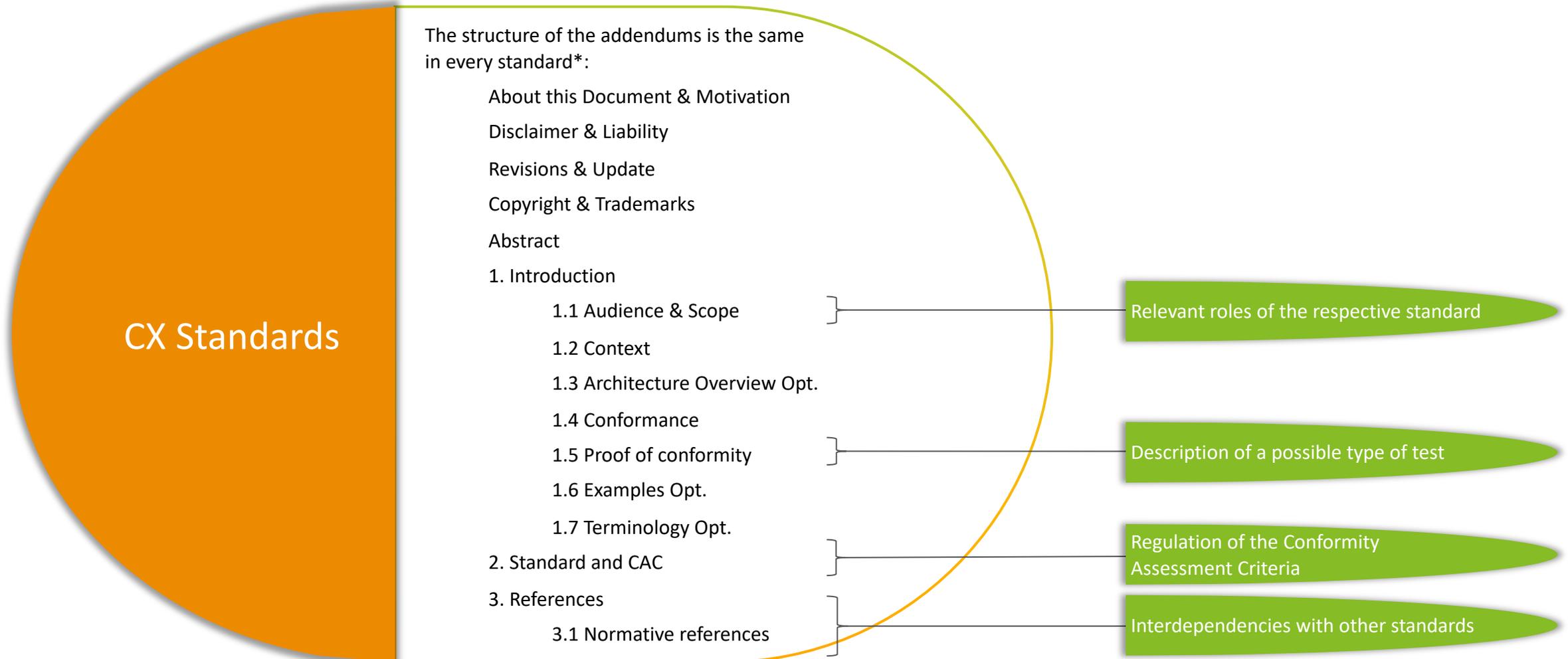
An event-based revision of the CAF is recommended (in particular, the modular approach, standards, and the CAC from the certification catalog) as well as after the end of the beta-phase in September 2023 by a task-force.

4. CX Standards in the context of the CAF



CX Standards in the context of the CAF (1/3)

The standards of Catena-X entail central contents that are relevant for the Conformity Assessment Bodies



* It is also possible that the structure contains further chapters

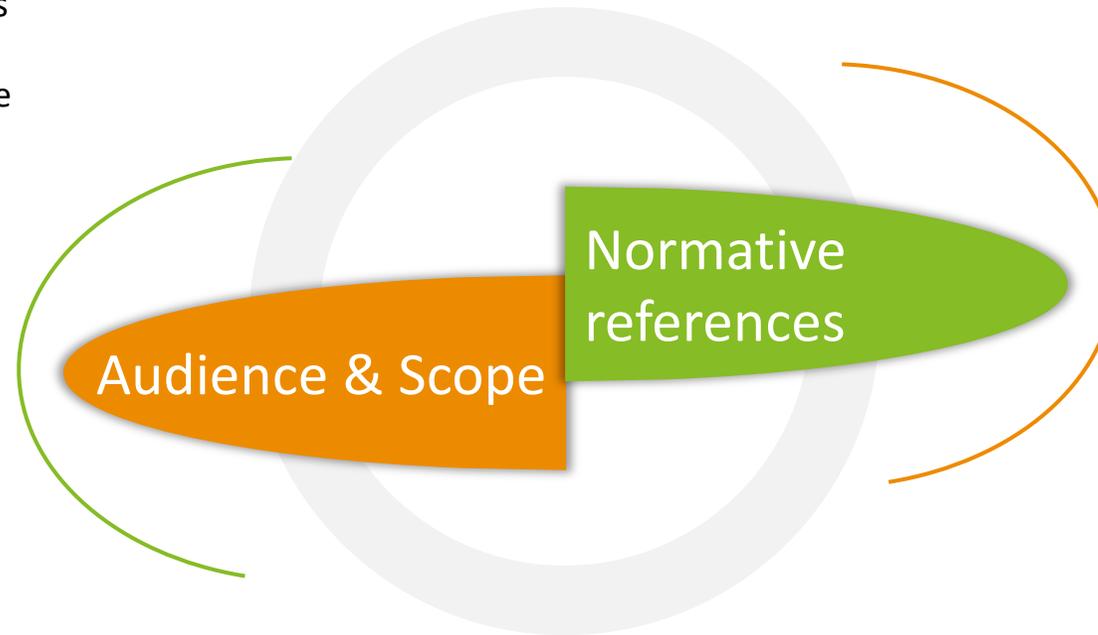
CX Standards in the context of the CAF (2/3)

Audience & Scope "WHO" and Normative References "WHAT" determine the scope of the certification activities

Audience & Scope (WHO)

Audience & Scope describes which roles are addressed and which scope of the standards is relevant. The roles from the Catena-X Operating Model Whitepaper Release V2 ([Link](#)) shall apply here:

- Core Service Provider
- Onboarding Service Providers
- Business Application Provider
- Enablement Service Providers
- Data Providers and Consumers*
- Consulting Service Provider*
- Conformity Assessment Body



Normative references (WHAT)

Normative references specify which other standards are relevant for the given standard. Normative references can refer to Catena-X Standards as well as to the standards outside the Catena-X Ecosystem (e.g., the IDSA protocol with the reference implementation EDC).

In this respect, normative references can also develop certification relevance and must therefore be fulfilled by the certification applicant.

* Currently not within the scope of CX certification

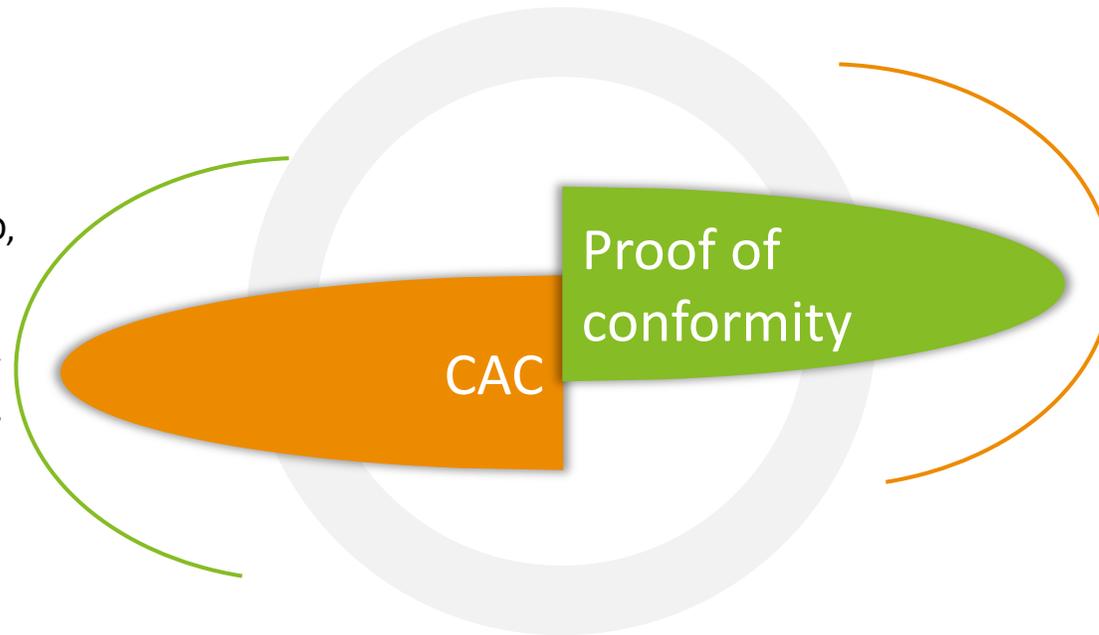
CX Standards in the context of the CAF (3/3)

The Conformity Assessment Criteria describe the "WHAT" and the proof of conformity represents a possibility of the "HOW"

Conformity Assessment Criteria (WHAT)

Standards contain criteria, the so-called CAC, which are checked in an assessment by the Conformity Assessment Body. The CAC can be identified by the keywords: MAY, MUST, MUST NOT, OPTIONAL, RECOMMENDED, REQUIRED, SHOULD and SHOULD NOT (cf. [BCP 14](#) [[RFC2119](#)] [[RFC8174](#)]). They are only relevant for certification if they appear in capital letters, as shown here. Only the keywords MUST and MUST NOT are subject to the certification and must therefore be fulfilled by a certification applicant.

Within the CAC, for example, implementations of API solutions or requirements for identification numbers are specified.



Proof of conformity (HOW)

The proof of conformity describes the type of compliance with the standard, which can be checked by the CAB in different ways.

For the certification applicant, this means that it, in turn, creates the prerequisite for testing according to the specifications of the proof of conformity.

Basically, the CAC is checked using various "[Test procedures](#)". For example, an implementation of the CAC can be proven by a verification document (test procedure: inspection).

Roles in the Catena-X ecosystem

Certification holders can fulfill a variety of roles within the Catena-X ecosystem

Core Service Provider

Core Service Providers run core services that enable the basic functionality of the Catena-X data ecosystem (e.g., Identity Provider, Marketplace). The Core Service Provider is responsible for the commercial provision, service operation and maintenance, and the release support of the core services in the data ecosystem. It actively markets the core services and is the contractual partner for partners such as Application Provider and Data Provider / Consumer. (For more information click [here](#))

Enablement Service Provider

Enablement Service Providers equip data ecosystem participants with solutions to provide or consume data within the Catena-X data ecosystem and operate data services e.g., connectors as managed services, that must be used by each data ecosystem participant depending on the use case. (For more information click [here](#))

Business Application Provider

Business Application Providers run business applications that solve a specific business problem (e.g., traceability, demand and capacity management, circular economy). Business applications can range from enterprise solutions to specialized solutions for small and medium sized enterprises (SMEs). (For more information click [here](#))

On-Boarding Service Provider

On-Boarding Service Providers enable Data Provider / Consumer to be integrated into the Catena-X network. This includes organizational and technical onboarding. (For more information click [here](#))

Advisory Provider*

An Advisory Provider offers advisory services in various areas, from strategy to operations to technology or business use cases for those interested in the Catena-X data space. Providing advisory services includes different kind of guidance, but does not include the operation of technical services. (For more information click [here](#))

Data Provider / Consumer*

Data Providers / Consumers (with and without a legacy system) provide, consume, and manipulate data to collaborate with other data ecosystem participants by means of core and data services as well as business apps. (For more information click [here](#))

White paper

* Currently not within the scope of CX certification

Certification objects: provider and solution

The Catena-X Operating Model Whitepaper contains the two certification objects Provider and Solution and describes them

Provider

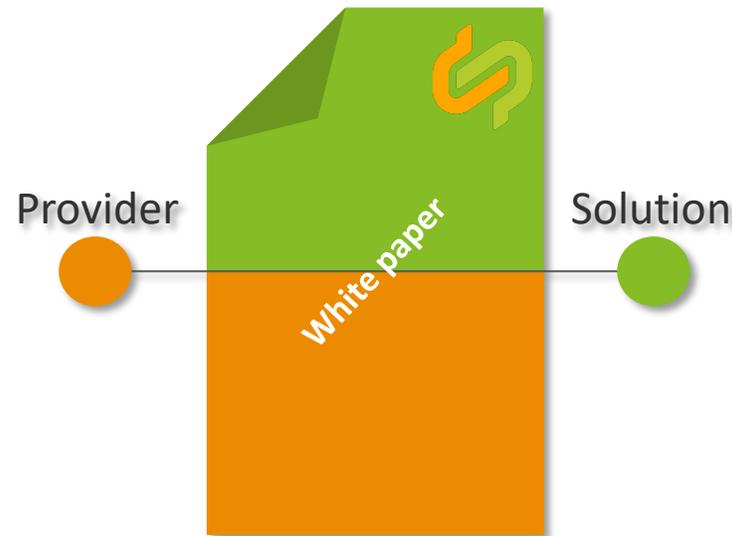
The certification object “Provider” is defined by standards for the general participation in the data ecosystem depending on their role.

The standards include but are not limited to the following standard types:
International standards (e.g., ISO 27001),
Catena-X Standards and Rules, Service-Level Agreements.

Recertification is required after one year or whenever there is a major change in any of the standards included. Revocation if misconduct.

The goal of the providers is to build an „available, secure and trustworthy framework“.

Provider criteria are listed [here](#).



Solution

The certification object “Solution” is defined by standards that focus on executable software based on business domain or platform capabilities and includes but is not limited to: Application Logic, Application Programming Interface Specification, Data Access (e.g., usage policies), Payload or Meta-Data, Processes (e.g., onboarding process), Business Logic (e.g., PCF Rulebook), Consulting Offerings, Conformity Assessment Requirements.

Solution criteria are listed [here](#).

5. Modular certification system in the context of CX Standards



Guidance modular certification (1/3)

The certification is based on a modular approach, with different levels to define the certification scope

Process of modular certification system:



Core Services

- This includes all standards that a core service provider must meet
- This certification scope is only relevant for the Core Service Provider (A & B) as a certification object , but must be taken into account by other roles

Middleware Solution

- Applies for the use case agnostic solutions e.g., the SDE

Onboarding Services

- All services and endpoints that the Core Service Provider and Onboarding Service Provider must fulfill are described here
- The Core Service Provider provides central components once available (e.g., BPN issuer) and the Onboarding Service Provider orchestrates the onboarding process (e.g., SD creation, wallet creation, etc.).

Guidance modular certification (2/3)

The certification is based on a modular approach, with different levels to define the certification scope

The **certification scope** is the **subset of standards to be met**.

Individual standards and CAC can be combined or certified separately.

The basic certification in the form of **Solution Base** and **Provider Base** contains all standards that must be met regardless of the use case, such as: ISO 9001 or Identity and Access Management (IAM).

The following certification scopes are included in the modular approach:

Solution Base

- A solution must only be initially certified one time as a solution, but for each individual use case in use

Example: an app is used for two use cases (e.g., Traceability and CO2), so this app must meet the Solution Base once and meet the standards of the two use cases

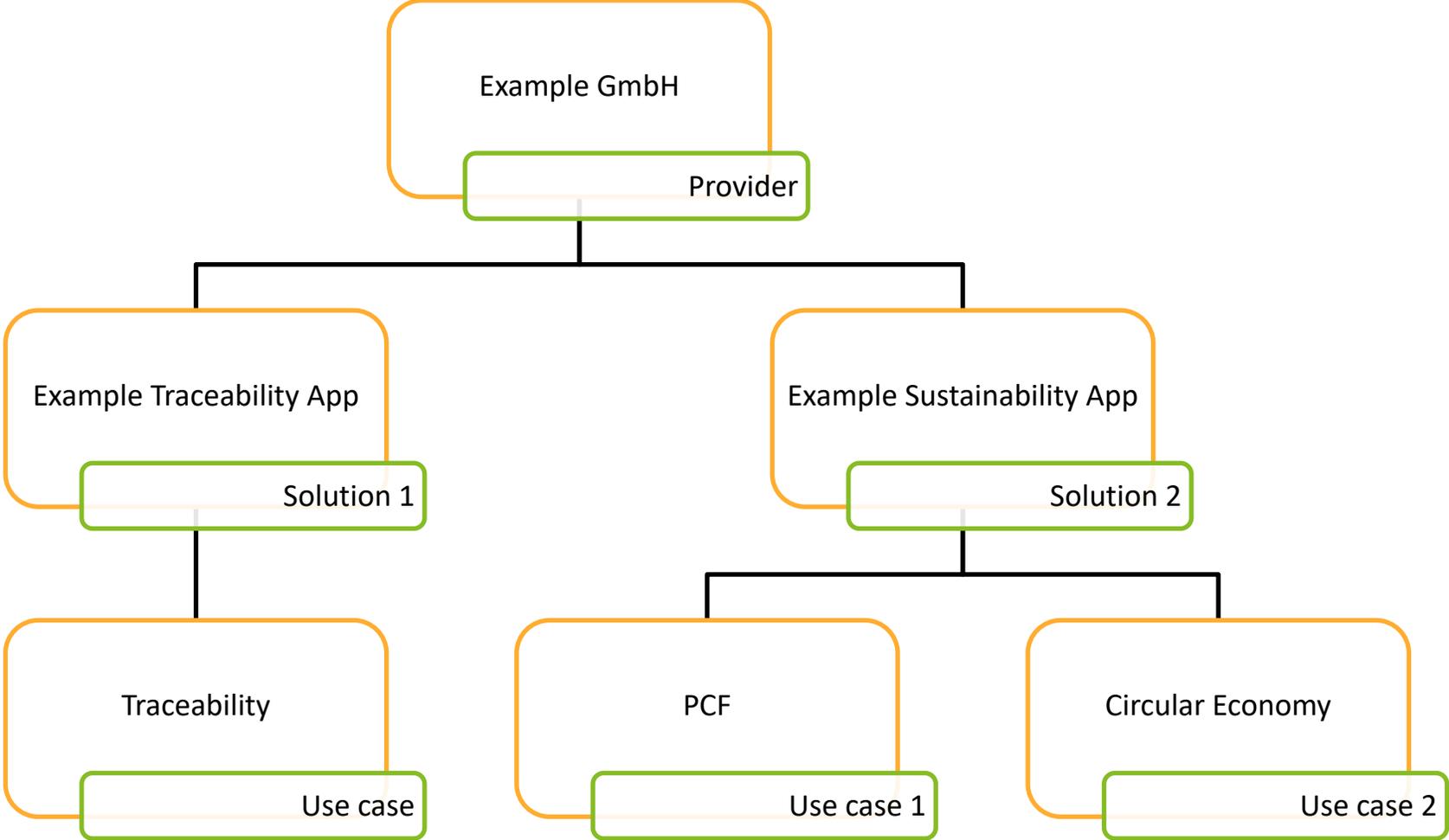
Provider Base

- As a provider of several solutions, a provider only has to be certified once according to the Provider Base and can then offer different solutions
- Solutions must be certified individually according to the Solution Base and its use cases

Example: if an app provider wants to offer two apps, e.g., for CO2 and for Quality, the provider has to meet the Provider Base only once, both apps have to meet the Solution Base and then their respective use case standards

Guidance modular certification (3/3)

The certification is based on a modular approach, with different levels to define the certification scope



Modular System – Overview

Modular System Catena-X Certification																											
Data Provider & Consumer		Enablement Service Provider			Business Application Provider																	Core Service Provider	Onboarding Service Provider	Sandbox Service Provider	Value Added Services		
Connector	Participant Wallet	Connector as a Service	Digital Twin Registry	Wallet as a Service	Quality	Traceability	Behavioral Twin	PCF	Circularity	Eco Pass	ESS	Logistics	MaaS	Modular Production	DCM	PURIS	OSIM	CCM	Tariffs	Engineering	SBOM	Material Accounting	Core Services	Onboarding Services	Sandbox Services	Value Added Services	
					<p>Connector: Every Solution must be enabled to use an EDC or have an integrated EDC</p> <p>Semantic: Digital Twin or Agents¹</p>																						
		Provider Base																									

¹ Each standard in the respective use case defines for itself which model may be used.

Detail View (2/3) – Remaining Roles

Modular System Catena-X Certification 								
	Data Provider & Consumer		Enablement Service Provider			Core Service Provider ⁴	Onboarding Service Provider ²	Sandbox Service Provider
Use Case	Connector	Participant Wallet	Connector as a Service	Digital Twin Registry as a Service	Wallet as a Service	Core Services	Onboarding Services	Sandbox Services ³
Role / Capability	When using a CX-certified solution, no separate certification is required	When using a CX-certified solution, no separate certification is required	Connector	Digital Twin Registry	Participant Wallet	CSP Wallet: CX-0049 CX-0050 CX-0149	CX-0006 CX-0009	Onboarding: CX-0006 CX-0009
Base Standard	CX-0018 CX-0152	CX-0149	CX-0018 CX-0152	CX-0002	CX-0149	Onboarding: CX-0006 CX-0009		BPDM: CX-0010 CX-0012 CX-0074
Additional¹	CX-0002 CX-0003 CX-0005 CX-0007 CX-0045 CX-0055 CX-0084 CX-0126 CX-0127		Backend Integration Pattern 1 CX-0002, CX-0003, CX-0055			Portal: CX-0001 CX-0053 Marketplace: CX-0054 BPDM: CX-0010 CX-0012 CX-0074 CX-0076		Identity Wallet: CX-0049 CX-0050 CX-0149
			Backend Integration Pattern 2 CX-0055, CX-0084					Portal: CX-0001 CX-0053
			Simple Data Exchanger CX-0007					Marketplace: CX-0054
			Data Chain CX-0005, CX-0045					Golden Record (optional): CX-0076
Provider Base: TISAX Level 2 is mandatory from July 2025, with grace period of 12 month, for all OSP, ESP and BAP. TISAX Level 3 is mandatory for CSP-A/B (as soon as the standard is adapted).								

¹ If "Additional" Standards are used or offered in a Solution, the certification of these Standards is required.

² Limitations Jupiter: this role currently only covers part of the registration process in the Catena-X data space. The currently available process is depicted in figure "General Onboarding Process".

³ Catena-X Sandboxes contain all services required for the operation of a minimum valuable Catena-X data space, namely: CSP-B services (excluding the cleansing service of BPDM and GXDCH integration) and OSP services.

⁴ Core Services B lists Core Services that can only be operated once in the Catena-X data space due to business reasons or technical limitations and are therefore tendered via the nomination process of the Association.

Detail View (3/3) – Remaining Roles

Modular System Catena-X Certification 						
Value Added Services ¹						
Value Added Service	Data Quality Dashboard	Bank Data Verification	Natural Person Screening	BPDM Fraud Prevention	Country Risk	Sanction Watchlist Dashboard
Standard	CX-0076 CX-0077	CX-0078	CX-0079	CX-0080	CX-0081	CX-0116
Provider Base	TISAX Level 2 is mandatory from July 2025, with grace period of 12 month, for all OSP, ESP and BAP. TISAX Level 3 is mandatory for CSP-A/B (as soon as the standard is adapted).					

¹ Can only be provided in combination with certified Core Services.



Certification objects: modular system apps example

Presentation of the process of the modular approach using the example of "Business Application Provider Traceability"

Modular System Catena-X Certification																				
Business Application Provider ²																				
Use Case	Quality		Traceability	Behavioral Twin			PCF		Circularity				Eco Pass	ESS	Logistics	MaaS		MP	DC	
Role / Capability	As OEM data provider	As Supplier data provider	Traceability Use Case	Behavioral Twin Assurance Predictor	Behavioral Twin Endurance Estimator	Behaviour Twin Health Indicator	PCF Exchange	PCF Calculation	Secondary Material Content	EoL / Dismantling Services	CE-Assistant	Secondary Marketplace ⁴	Asset Tracking	Use Case Circular Economy - Digital Product Passport	ESS Use Case	Logistics and Customs Use Case	Manufacturing Capability Exchange	Request for Quotation Exchange	Shop Floor Information Service	As a Supplier
Base Standard	CX-0123		CX-0125	CX-0059	CX-0138	CX-0141	CX-0136	PCF-Rulebook	/	CX-0053		CX-0117	CX-0105 CX-0045	CX-0143	CX-0144	CX-0150	CX-0115	CX-0129	CX-0142	CX-0
Additional	/	/	CX-0005 ¹	/	/	/	/	/	/	/	CX-0136 ⁶	/	/	/	/	/	/	/	/	/
Industry Core ^{5,6}	/	/	CX-0127	/	/	/	CX-0126	/	CX-0126 CX-0127		/	CX-0127 ⁷	CX-0126 CX-0127	/	CX-0126 CX-0127	/	/	/	/	/
Connectivity ³	CX-0018, CX-0152							/	CX-0018, CX-0152											
Semantic	Digital Twin CX-0002 or Agents CX-0084							/	Digital Twin CX-0002 or Agents CX-0084											
Provider Base	TISAX Level 2 is mandatory from July 2025, with grace period of 12 month, for all OSP, ESP and BAP. TISAX Level 3 is mandatory for CSP-A/B (as soon as the standard is adapted).																			

Process of modular approach:

1. Identify the role: **Business Application Provider**
2. Identification of the cert. scope with CAB: **Traceability**
3. CAB provides certification modules together: **requires Solution Base & requires Provider Base**

List of standards:

1. **Use Case Standard: CX-0125**
2. **Additional: CX-0005**
3. **Industry Core: CX-0127**
4. **Sovereign Data Exchange / Connector: TISAX Level 2** is mandatory from July 2025, with grace period of 12 month, for all OSP, ESP and BAP and TISAX Level 3 is mandatory for CSP-A/B (as soon as the standard is adapted).
5. **Semantic: Digital Twin CX-0002 or Agents CX-0084**
6. **Provider Base: CX-0008**

Modular System – Business Application Provider

Traceability ¹	CX-0125 Additional ² : CX-0005
Industry Core ^{4,5}	CX-0127: <i>It is tightly bound to the Industry Core, as Quality Alerts and Quality Investigation Requests should reference batches and/or serialized part instances as described in the standard CX - 0127 INDUSTRY CORE: PART INSTANCE.</i> <i>Regarding CX-0005: This standardization is built upon existing standards, such as CX-0127.</i>
Connectivity ³	CX-0018, CX-0152
Semantic	Digital Twin: CX-0002 or Agents: CX-0084
Provider Base	TISAX Level 2 is mandatory from July 2025, with grace period of 12 month, for all OSP, ESP and BAP and TISAX Level 3 is mandatory for CSP-A/B (as soon as the standard is adapted).

¹ Business Application Provider has to perform an interoperability check.

² If “Additional” Standards are used or offered in a Solution, the certification of these Standards is required.

³ If no EDC is implemented in the solution, at least the Data Management-API is subject of the certification.

⁴ Digital Twins have to contain the defined Specific Asset Ids. Additional use case specific data models have to be provided as Digital Twin submodels. If the respective data models are used, these have to be certified against the specification defined within the Industry Core standard.

⁵ When using certain features, the referenced section of the standard is required.

6. Certification catalog



Structure of the certification catalog

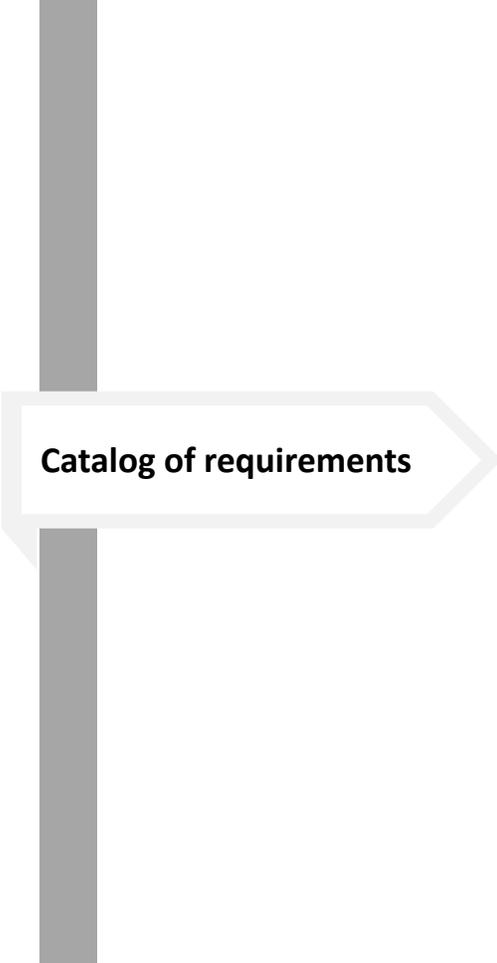
The certification catalog contains all certifiable standards in the Catena-X ecosystem. The CAB finds here the individual CAC required for the respective standards

Catalog of requirements									Risk	Test procedures		
CAC – ID NO.	Standard	Standard Version	Category	Platform Capability / Use case	Standard-title	Requirement (CAC)	Must / May / Should	...	Stages 1 - 4	Inspection	...	Analytical Procedures
CX-0019-CAC-001	CX-0019	V2.0	Semantic	Traceability	Batch	Tbd	MUST	...	3			
CX-0019-CAC-002	CX-0019	V2.0	Semantic	Traceability	Batch	Tbd	MUST	...	3			

In preparation for certification, the certification applicant receives an individual list of standards including the associated CAC

Structure of the certification catalog – column content (1/3)

Further columns of the requirements catalog contain all information of the standards that are relevant for certification



Catalog of requirements

CAC-ID-NR.

The CAC identification number is a uniquely assigned number that identifies the corresponding CAC. The CAC-ID-NR is used to identify the standard, the CAC within the standard and the version number of the CAC. The combination **CX-0002** stands for the referenced standard, the combination **CAC-001** is the ID number of the CAC within a standard and **.001** indicates which version of the CAC it is: **CX-0002-CAC-001.001**

Standard

The standard number is a uniquely assigned number for the assignment of standards. It indicates which standard is referred to in each row.

Standard Version

The version number of the standard indicates the status of the described standard. The standard and standard versions are updated with the release of a new version of the standard.

Category

CAC are divided into three categories based on their characteristics.

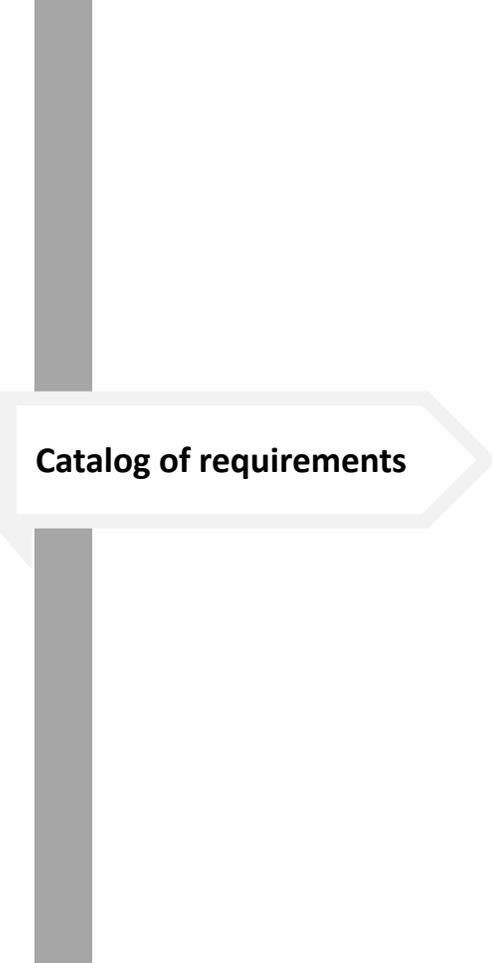
1. The category API indicates that the CAC criteria is an interface.
2. The category SEMANTIC indicates that the CAC criteria is a semantic model.
3. The DEFAULT category subordinates everything that cannot be assigned to SEMANTIC or API.

Platform Capability

The platform capability groups standards according to capabilities offered by the platform and used by the use cases.

Structure of the certification catalog – column content (2/3)

Further columns of the requirements catalog contain all information of the standards that are relevant for certification



Catalog of requirements

Default title

The default title describes the title of the respective standard. It serves as a specification of the platform capability.

CAC

CAC describe which requirements must be met in order to participate in the Catena-X ecosystem. They contain keywords that indicate whether a criterion must be met or whether it should be met. CAC provide more detailed information on how a requirement must/should be implemented.

Additional information

Additional information provides the CAB with more detailed information about the proper implementation of a CAC. The additional information contains links to websites with further relevant details.

MUST/SHOULD or MUST NOT/SHOULD NOT

The MUST/SHOULD column contains the keywords that are valid for the CAC. These can be either MUST or SHOULD or MUST NOT or SHOULD NOT. From this, the auditor can see whether a CAC must be implemented or should be implemented or should not be used.

Proof of conformity

The proof of conformity indicates which tests can be carried out to verify the implementation of the CAC. The basis for this are the test procedures.

Structure of the certification catalog – column content (3/3)

The other columns include the audit methods of the respective CAC, its risk classification and the corresponding normative reference to further CX or external standards

Test procedures

The test procedures are the methods used to verify the implementation of a CAC. They are divided into eight different individual options:

- | | |
|--------------------|--------------------------|
| 1. Inspection | 5. Confirmation |
| 2. Observation | 6. Recalculation |
| 3. Self-assessment | 7. Reperformance |
| 4. Inquiry | 8. Analytical Procedures |

The details of the individual test procedures are explained below.

Risk

The risk level is used to assess a test procedure. The risk ranges from level 1 (low risk) to level 4 (high risk) and is intended to give an assessment of how critical individual criteria of the catalog of requirements are. Currently, a risk assessment is not part of the certification catalog as requested.

7. Test procedures

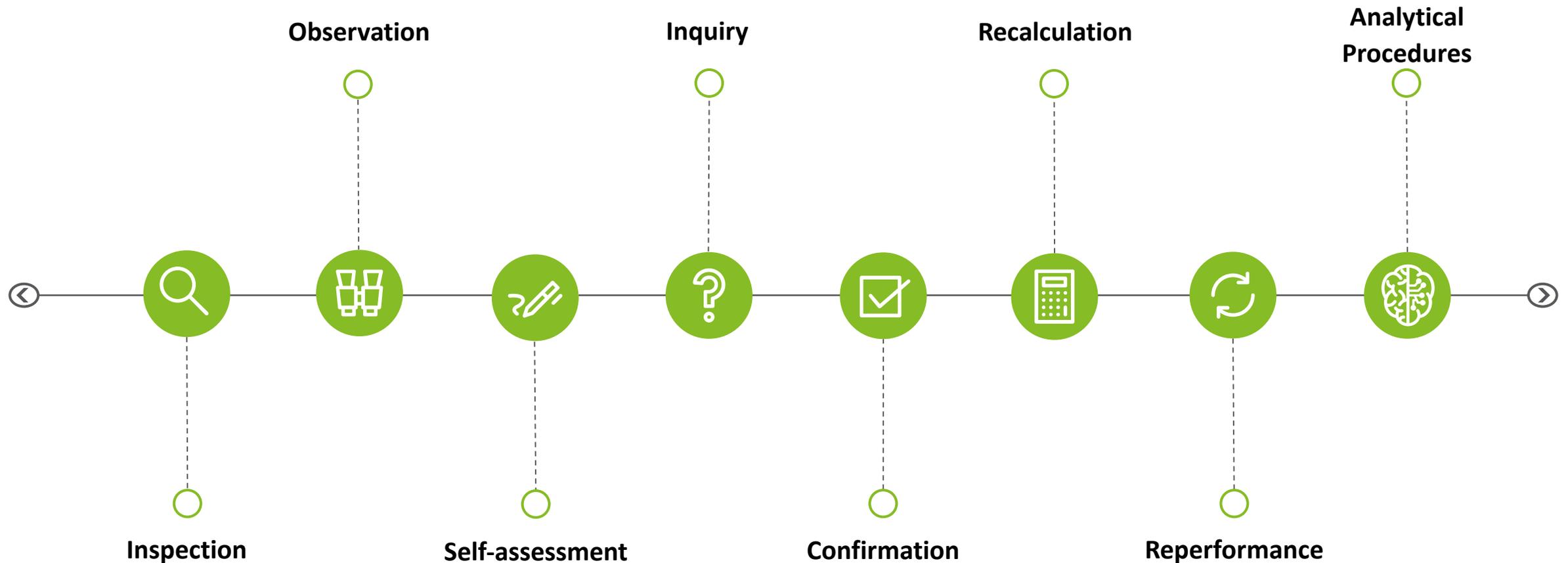


Test procedures (1/5)

Various test procedures are presented, of which the CAB uses a selection depending on the nature of the CAC

To check the CAC and thus the standards, the CAB uses the test procedures defined in the framework. Each CAC a test procedure is assigned in the catalog, which is shown and explained below.

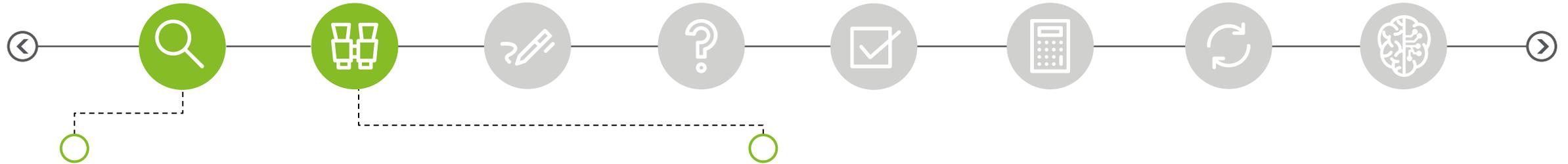
If a CAC or a standard is not applicable, e.g., because the solution does not use the semantic model, the CAC can be outsourced by the CAB with not applicable (n/a) and a justification.



Test procedures (2/5)

During the inspection, records and documents are checked by the CAB.

In observation, a process or procedure is observed by the CAB and thus the implementation is checked



Inspection

The audit includes the examination of records or documents in paper, electronic form or other media, or the physical documentation of an implementation.

E.g., screenshots of API code with timestamp

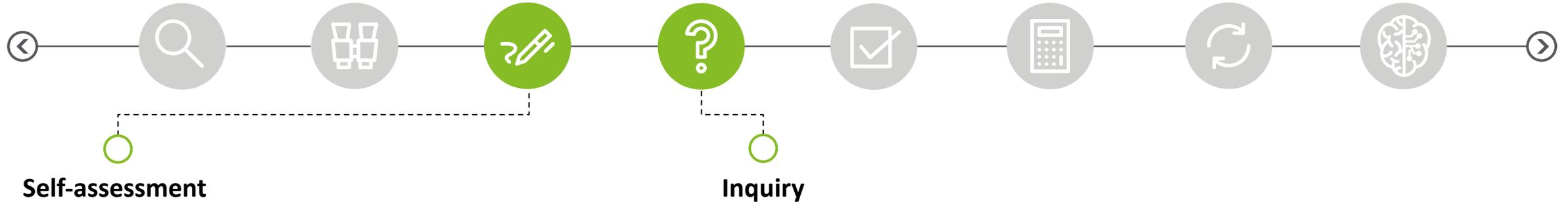
Observation

During observation, the requirement or control procedure to comply with the CAC is observed and controlled by the assessor. Observation may provide audit evidence of the conduct of a process or procedure, but evidence is limited to the time of observation and is also limited by the fact that observation may affect the conduct of the process or procedure.

E.g., support for the implementation of an onboarding process

Test procedures (3/5)

In the self-assessment, the certification applicant submits a self-disclosure about the implementation. The Inquiry includes the questioning of the certification applicant about the CAC



Within the self-assessment, the certification applicant gives written information provided by the authorized persons on the individual requirements or questions specified in the self-assessment. This information is then evaluated by the CAB.

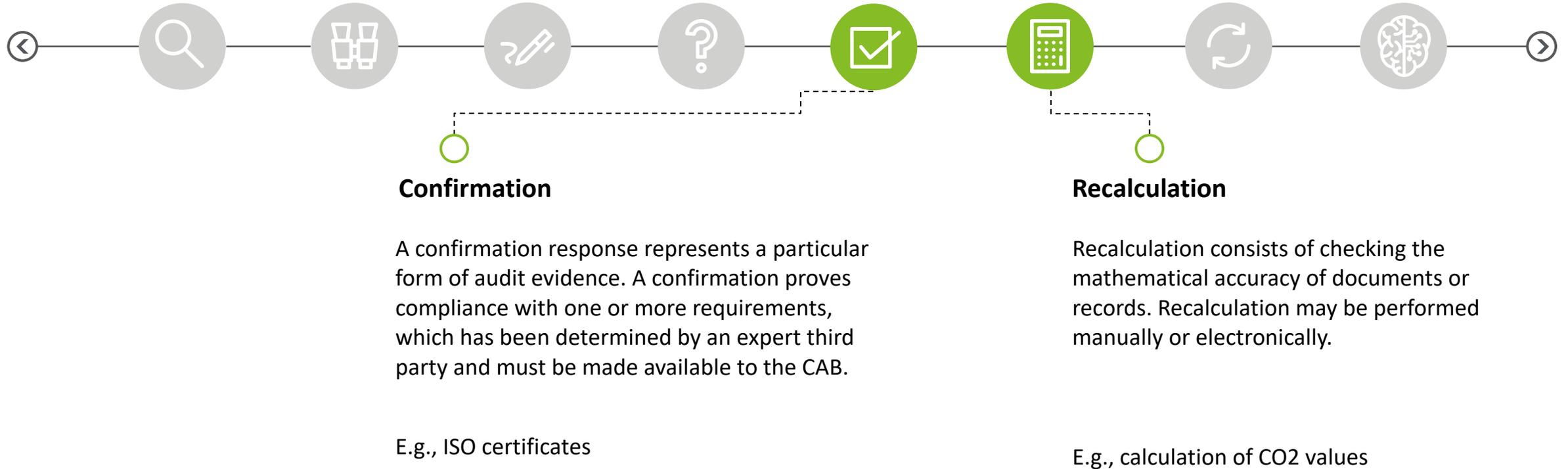
E.g., confirmation of the use of the correct semantic models

The inquiry consists of obtaining the information or verbal consent of ratified persons of the company. Inquiry may be performed throughout the audit in addition to other audit procedures. Inquiries may range from formal written inquiries to informal oral inquiries.

E.g., the certification applicant verbally assures to an assessor the compliance with the endpoints of an API

Test procedures (4/5)

In the case of the Confirmation the CAB receives proof of confirmation from a third party.
Recalculation is the recalculation of mathematically determined values



Test procedures (5/5)

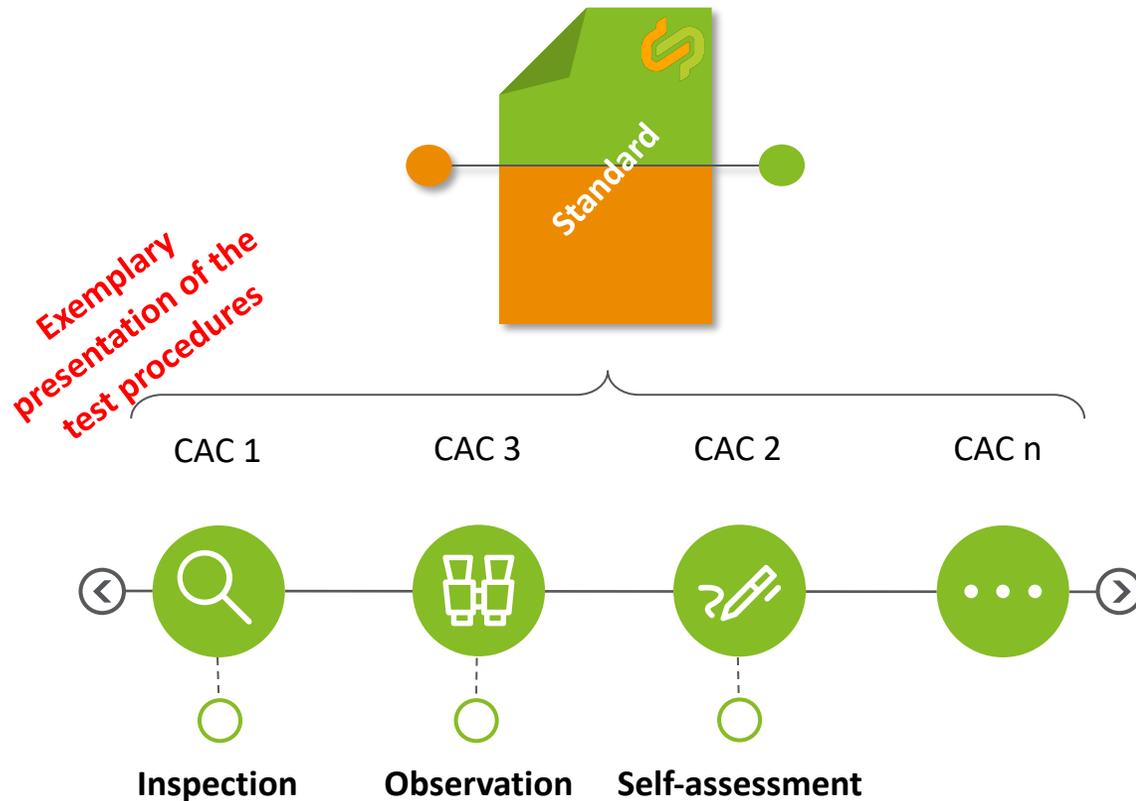
In reperformance, the CAB repeats a company's procedures through its own test. Analytical methods are the plausibility check of facts in relation to each other



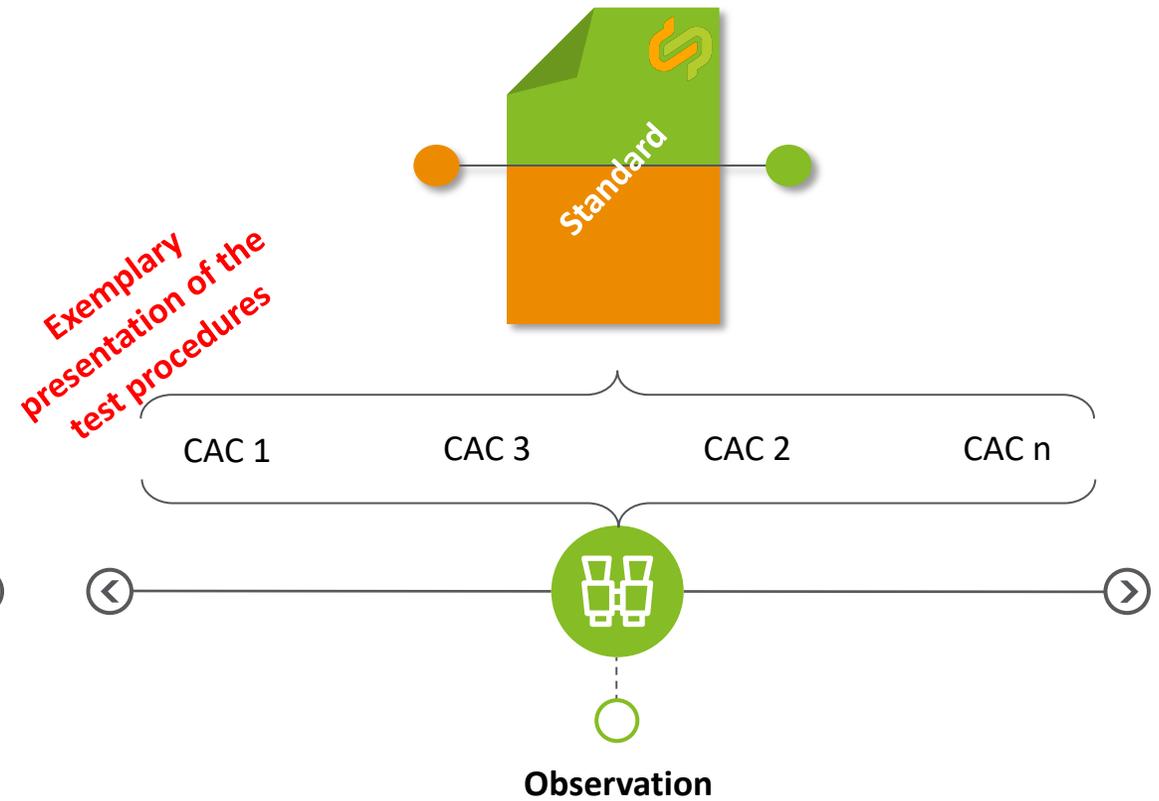
Test procedures - inherent testing

Testing of the CAC can be both direct and inherent. An inherent test covers individual CAC e.g., if the test is directed to a specific output

Testing of the CAC within the framework of individual test procedures



Inherent testing of individual CAC



IPE – Information Produced by Entity

Evidence and its origin can be submitted either automatically through test results or manually through screenshots, among other things. The plausibility of the evidence must be checked and validated by the CAB

Manually generated evidence

The manual assessment includes, for example, review of screenshots or other evidence created manually by the certification applicant. These evidence must cover following requirements:

- Entirety of the data to be checked
- Chronological order of the data to be checked
- Up-to-date status (version) of the data to be checked

Example: review of an API implementation based on various screenshots. These are checked for plausibility with the above-mentioned criteria and documented.

Automatically generated evidence

The testing of automatically generated evidence includes, for example, the review of test reports generated within a test environment published by third-parties / Catena-X. These evidence must cover following requirements:

- Versioning and up-to-date status of the test environment
- Versioning and up-to-date status of the solution to be certified
- Definition of the right parameters for the testing

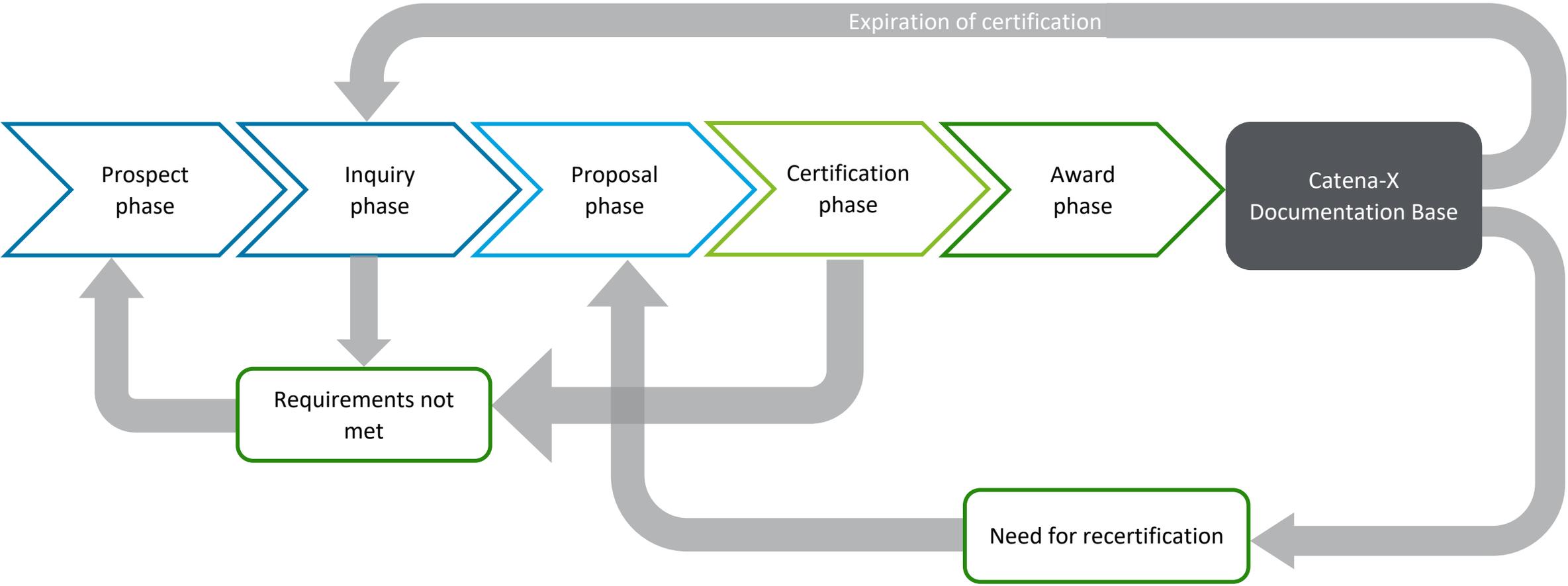
Example: the review of a test report on the implementation of the EDC. These are checked for plausibility with the above-mentioned criteria and documented.

8. Certification process



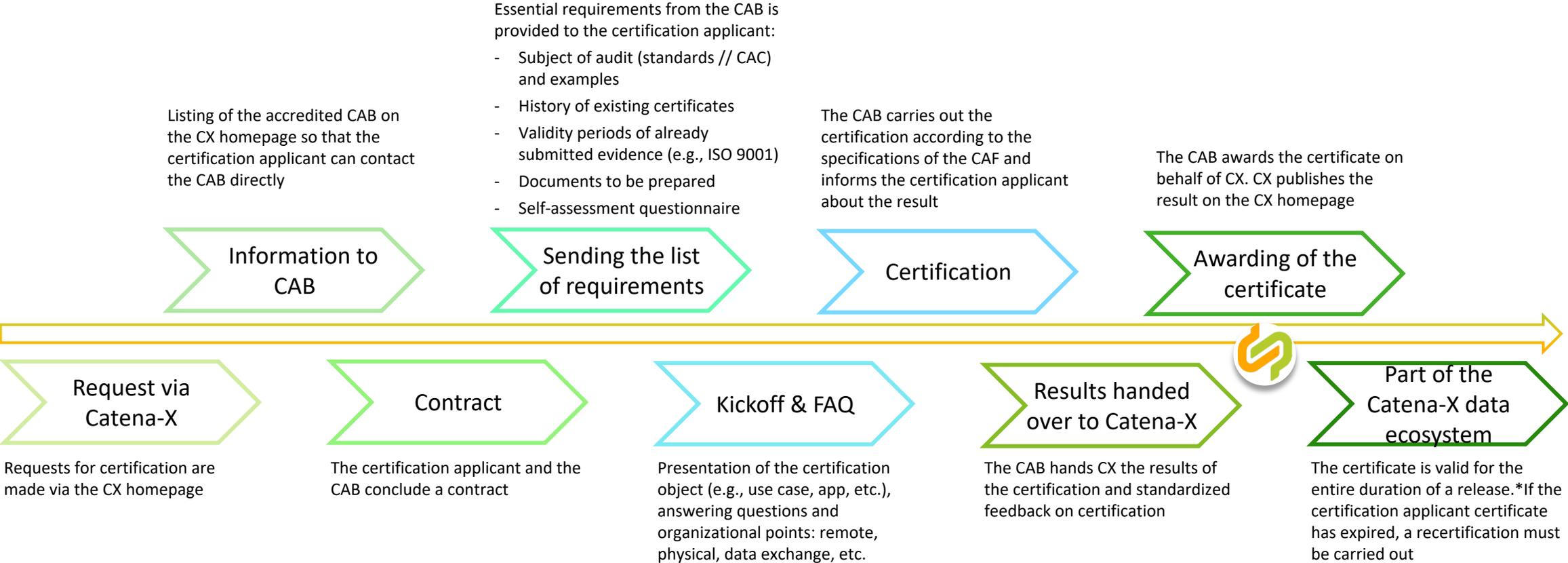
Certification process

As part of the certification process, certification applicants are guided through five phases. The phases are the prospect, inquiry, offer, certification and award phases



Process of certification over time

The following diagram is given to the certification applicant to explain the certification process



* current working premise, which will be verified during the beta phase.
 Upon expiration, the certificate will be removed from the CX homepage and participation in the CX data ecosystem will no longer be allowed. Thus, the renewal of the certificate is the responsibility of the certified company.

Example to test the semantic model

The CAB provides the certification applicant with examples of how to examine the CAC

CAC- ID No.	Platform Capability	Requirements (CAC)	Proof of conformity
CX-000X-CAC-00X	Semantic	Quality Gates MUST be fulfilled for the different model stages of an aspect model.	The resulting aspect models of modelling activities MUST be element of https://github.com/eclipse-tractusx/sldt-semantic-models with status "Released". It MUST be ensured that all modelling stages were successful. The modelling stages are ensured by GitHub actions and corresponding checklists (see also public documentation in GitHub: https://github.com/eclipse-tractusx/sldt-semantic-models/blob/main/documentation/GOVERNANCE.md)

The testing of the CAC with the number CX-000X-CAC-00X is carried out using the observation test procedure.

Audit activities:

1. In a joint meeting with the certification applicant, the CAB checks whether
 - a. the semantic models are published with the status "Released" in GitHub
 - b. the model phases have been successfully completed
 - c. the semantic models comply with the quality gates to be fulfilled for the different model phases of an aspect model
2. The evidences are created in the form of screenshots during the appointment and documented by the CAB. The screenshot should indicate the system, time of observation, etc. (compliance with IPE guidelines).
3. The CAB documents the fulfilment or non-fulfilment of the CAC.

Example to check the API

The CAB provides the certification applicant with examples of how to examine the CAC

CAC- ID No.	Platform Capability	Requirements (CAC)	Proof of conformity
CX-000X-CAC-00X	EDC Discovery API	The implemented service MUST use a Self Description (SD) storage like SD-Hub or Federated Catalog for storing the SD documents provided during the onboarding process.	A test case will be, that an EDC instance has to be onboarded for a specific participant identified by a BPN. The SD for the EDC must be visible in the supported SD storage. The query against this new registered EDC instance for the given BPN should provide the connector URL as stated in the SD document.

The testing of the CAC with the number CX-000X-CAC-00X is carried out using the inspection test procedure.

Audit activities:

1. Submission by the certification applicant of proof that:
 - a. the implemented service SD-Hub or Federated Catalog is used as the storage location for the Self Description (SD) documents
 - b. the EDC URL points to the correct BPN number
2. Verification of the authenticity of the documents (verified by the date stamp, data origin and creator of the document) by the CAB.
3. The CAB documents the fulfilment or non-fulfilment of the CAC.

Example to check other CAC

The CAB provides the certification applicant with examples of how to examine the CAC

CAC- ID No.	Platform Capability	Requirements (CAC)	Proof of conformity
CX-000X-CAC-00X	Onboarding	The respective roles MUST provide a proof that it – at the time of the assessment – are ISO 9001 certified or are in the process of receiving a (re-) certification.	Conformity with relevant standards during onboarding applies to the participant itself. The participant needs to prove that it follows Catena-X internal (e.g., data sovereignty guidelines) and Catena-X external (e.g., ISO 9001) standards independent of the business applications that it later wants to offer. For internal standards, a self-assessment that the internal standards are followed shall be conducted by the participant. A statement shall be issued that assures that the internal standards are followed. Note: As of Release 3.0 there aren't any internal standards that must be followed. This might change with one of the next releases. For external standards, the existing certificate/prove of conformity with the external standard shall be handed in to the CAB. The participant can finalize the onboarding only after successful verification of conformity.

The testing of the CAC with the number CX-000X-CAC-00X is carried out using the confirmation test procedure.

Audit activities:

1. Submission of ISO 9001 certificate or evidence about ongoing recertification by the certification applicant.
2. Validation of the authenticity of the certificate by the CAB.
3. Verification of the validity of the certificate by the CAB.
4. The CAB documents the fulfilment or non-fulfilment of the CAC.

Anforderungsliste vom CAB an den Zertifizierungsbewerber

Der CAB stellt dem Zertifizierungsbewerber eine Anforderungsliste der vorzubereitenden Unterlagen bereit

Anforderungsliste an Zertifizierungsbewerber

Übersicht der Softwarelösung:

Kurzbeschreibung der vom
Zertifizierungsbewerber verwendeten
Softwarelösung

CX-Zertifizierungsstandards:

Für den Zertifizierungs-Scope relevante
Zertifizierungsstandards

Anforderungen je Standard:

Auflistung der vom Zertifizierungsbewerber
vorzubereitenden Unterlagen



List of Requirements

Documents to be prepared by the certification candidate for the certification scope.

Certification applicant:

Muster GmbH
Musterstraße 1
65321 Musterstadt

Muster-X

Overview of the functionalities of the software
solution used:

Disclaimer: The CAB is required to verify compliance with all CAC marked as MUST. The CAB
commissioned by Catena-X reserve the right to request additional documents as part of the
certification process. A not applicable/not relevant CAC can be discussed with the CAB in specific
cases.

CX Standards	Requirements
CX-0002 Digital Twins in Catena-X	Provide an OpenAPI specification matching the API Structure in the standard, defined by the CAC in the Addendum of the standard. This can be found in the Catena-X Standard Library (https://catena-x.net/de/tractus-x/standard-library). Please indicate where compliance with the specific CAC can be found.
CX-0008 Conformity Assessment	Provide a Documentation of the required ISO/ TISAX Certifications. Further provide Documentation for the SHOULD CAC regarding the standard if they are fulfilled. The CAC can be found in the Catena-X Standard Library (https://catena-x.net/de/tractus-x/standard-library)
CX-0017 Company role represented by the connector	Provide a test report from a test bed proving the correct implementation of the standard. Additionally provide documentation that all MUST CAC regarding the standard, which are not met by the test report, are fulfilled. CAC can be found in the Catena-X Standard Library (https://catena-x.net/de/tractus-x/standard-library).
CX-0018 Eclipse Dataspace Connector	Provide the PDF report, of the IDS-Testbed, validating the functionality of the connector. The test bed can be found at https://github.com/international-data-spaces-association/IDS-testbed .
CX-0023 Notification API	Provide an OpenAPI specification matching the API Structure in the standard, defined by the CAC in the Addendum of the standard. This can be found in the Catena-X Standard Library (https://catena-x.net/de/tractus-x/standard-library).

Self-assessment and template for declaration of completeness and correctness

In the self-assessment, the certification applicant submits a self-assessment to the CAB about the implementation of requirements

Self-assessment of the certification applicant

Certification Scope:

Includes the certification standards for the desired certification

Conformity Assessment Criteria (CAC):

List of CAC relevant for the certification scope, which are checked via a self-assessment

Information from the certification applicant:

Information on the Individual requirements or questions specified in the self-assessment

Declaration of completeness and correctness

The certification applicant confirms the completeness and correctness of the information



Self-Assessment

Self-disclosure of the certification applicant about the implementation of the Criteria

Certification Applicant:
Musterfirma
Musterstreet 1
11111 Musterstadt

Traceability A (Traceability Notifications)

Required Standards:

CX-0005 Item Relationship Service API	CX-0021 Batch
CX-0008 Relevant Standards for Conformity Assessment	CX-0022 Notification Process
CX-0017 Company Role by the Connector	CX-0023 Notification API
CX-0018 Eclipse Data Connector (EDC)	CX-0060 Triangle Traceability Digital Twin ASBUILT
CX-0019 Aspect Model Serial Part	CX-0062 Traceability Notifications Triangle
CX-0020 Aspect Model SingleLevelBoMASBuilt	

Confirmation of the completeness and correctness of the self-assessment of the certification applicant. The certification applicant confirms in writing to agree with the values for interoperability and data sovereignty and to act accordingly to the standards of Catena-X in the data ecosystem. With their signature, the certification applicant confirms that they have implemented all the necessary specifications in the following table. The certification applicant assures that all information has been implemented correctly and completely and that all necessary documents have submitted to the CAB.

Disclaimer: The CAB is required to verify compliance with all CAC marked as MUST. The CAB commissioned by Catena-X reserves the right to request additional documents as part of the certification process. A not applicable/not relevant CAC can be discussed with the CAB in specific cases.

Contact Person: _____ Place, Date: _____



The following CAC are implemented according to the requirements of the standard, exceptions and changes concerning the Scope of the certification must be reported immediately to the Conformity Assessment Body within the scope of certification.

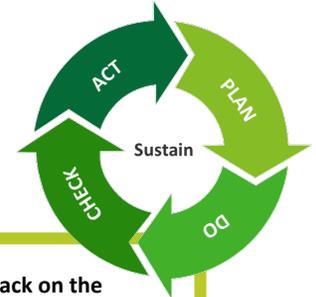
Standard	Requirement (CAC)
CX-0019	Every data provider of SerialPart data MUST provide the data conformant to the semantic model specified in this document.
CX-0019	The unique identifier of the semantic model specified in this document MUST be used by the data provider to define the semantics of the data being transferred.
CX-0019	Every certified business application relying on SerialPart data MUST be able to consume data conformant to the semantic model specified in this document.
CX-0019	This semantic model MUST be made available in the central Semantic Hub.
CX-0019	Data consumers and data provider MUST comply with the license of the semantic model.
CX-0019	The submodel data MUST be transferred using the IDS Protocol as described in CX-0018 and CX-0002.
CX-0019	Data providers MUST provide the data as part of a digital twin of the asset for serialized parts conformant to CX-0002 DIGITAL TWINS IN CATENA-X.
CX-0019	The JSON Payload of data providers MUST be conformant to the JSON Schema as specified in this document.
CX-0020	If a data provider decides to provide data for the SingleLevelBoMASBuilt Aspect Model they MUST provide the data conformant to the semantic model specified in this document.
CX-0020	The unique identifier of the semantic model specified in this document MUST be used by the data provider to define the semantics of the data being transferred.
CX-0020	Every certified business application relying on SingleLevelBoMASBuilt data MUST be able to consume data conformant to the semantic model specified in this document.

2

Feedback from the CAB

Information on certification is transmitted to Catena-X per standard in a regulated format with feedback and is part of the award phase

The Conformity Assessment Body is obliged to forward the certification result per standard to the association after certification in order to actively support the PDCA cycle (see chapter 10 “Up-to-date status of certifications”). The feedback from the certification can then be used by the association and passed on to the standardization process.



Provider	Solution	Certification number	Standards	Version of the certified standard	CAC	Feedback on the certified standard
Doe GmbH	Sample application	CX-ABC-000001	CX-0001	1.0	<ul style="list-style-type: none"> The implemented service MUST use a Self Description (SD) storage like SD-Hub or Federated Catalog for storing the SD documents provided during the onboarding process. The provided SD documents MUST be GAIA-X compliant, i.e. MUST provide a compliance credential issued from GAIA-X AIBSL. The implemented service SHOULD use the SD storage as source of truth The EDC Discovery API MUST be implemented as specified in the openAPI documentation as stated here: https://... The API MUST use JSON as the payload transported via HTTP. The following HTTP response codes MUST be defined for HTTP POST endpoints 	For example: difficult to comply with a CAC, does not describe the minimum requirements
Doe GmbH	Sample application	CX-ABC-000001	CX-0002	1.0	<ul style="list-style-type: none"> The submodel endpoints registered for a digital twin MUST be published towards the network using a Data Asset in terms of the IDS Protocol following the Catena-X Standard CX-0018. The API MUST be implemented as specified in the openAPI specification as stated here This API is independent from the architecture, i.e. the same API MUST be provided for the centralized and decentralized approach of Digital Twin Registries. The API MUST use JSON as the payload transported via HTTP. Error response 501 Not Implemented MUST be used for parameter values not yet supported. 	n/a

9. Catena-X certificate



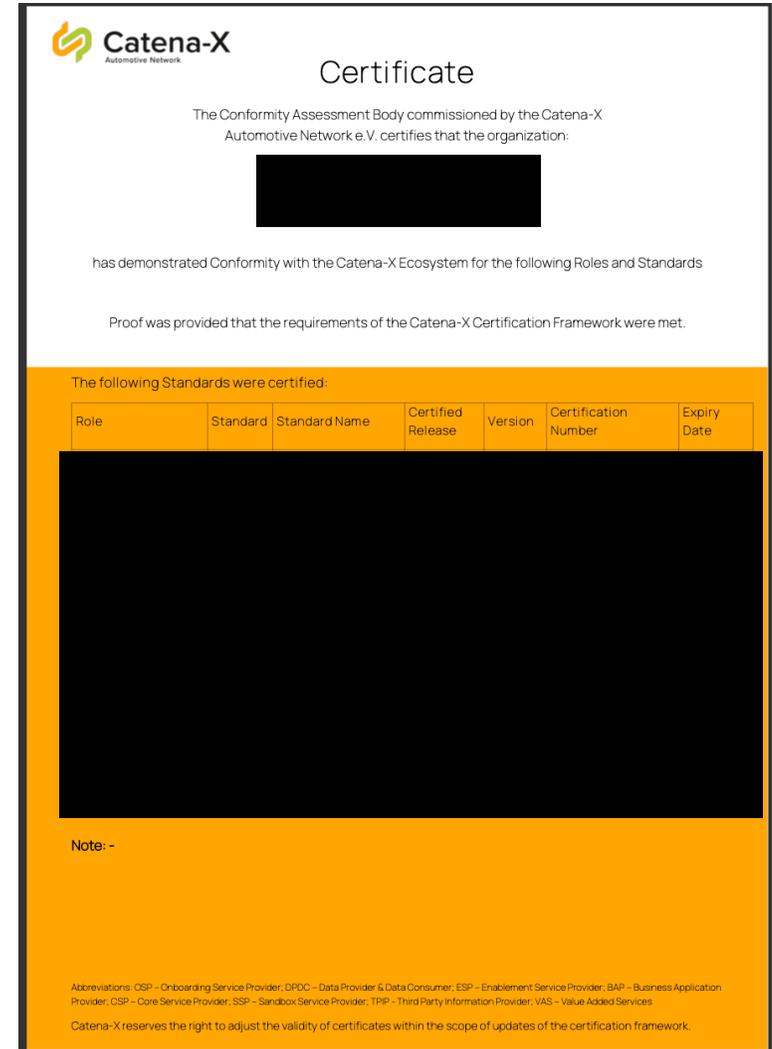
Catena-X certificate

The requirements for the certificate provide a complete overview and traceability of certification

Requirements for the Catena-X certificate

Catena-X certificate includes following content:

- Full company name of the certified company
- Role of the company in the ecosystem in connection with certification scope
- Fulfilled Catena-X Standards with versioning
- If applicable, notes such as "ISO 9001 must be submitted to Catena-X within 12 months to meet the CX-0008 standard"
- Validity (respective Release)
- Certification expiration date
- Certification number



Certification identification

The unique certificate number connects the CAB to the certification recipient and can be verified at CX

The certificate number

CATX-ABC-0000001

of the Catena-X certificate consists of and provides information on...

- = Abbreviation for the content-related connection with Catena-X
- = Unique abbreviation assigned per CAB to identify a CAB commissioned by Catena-X. Outsiders cannot link any names of CABs via the abbreviation
- = Sequential number for one-time certificates

Depending on the point in time, there will be three different identification options for certified apps and companies:

In the first iteration for identification, certification objects can receive information by e-mail. A request can be sent via the Catena-X contact page (<https://catena-x.net/de/kontakt>) in form of an e-mail.

The first specification of the information on the certification objects is provided by a verification website of Catena-X ([link follows](#)). Here, companies and partners can independently find certified companies in the database by entering the certificate number.

In the final stage, an electronic certificate is stored as a QR code on the certificate. This allows a clear identification of a certified provider/solution.

Backward compatibility

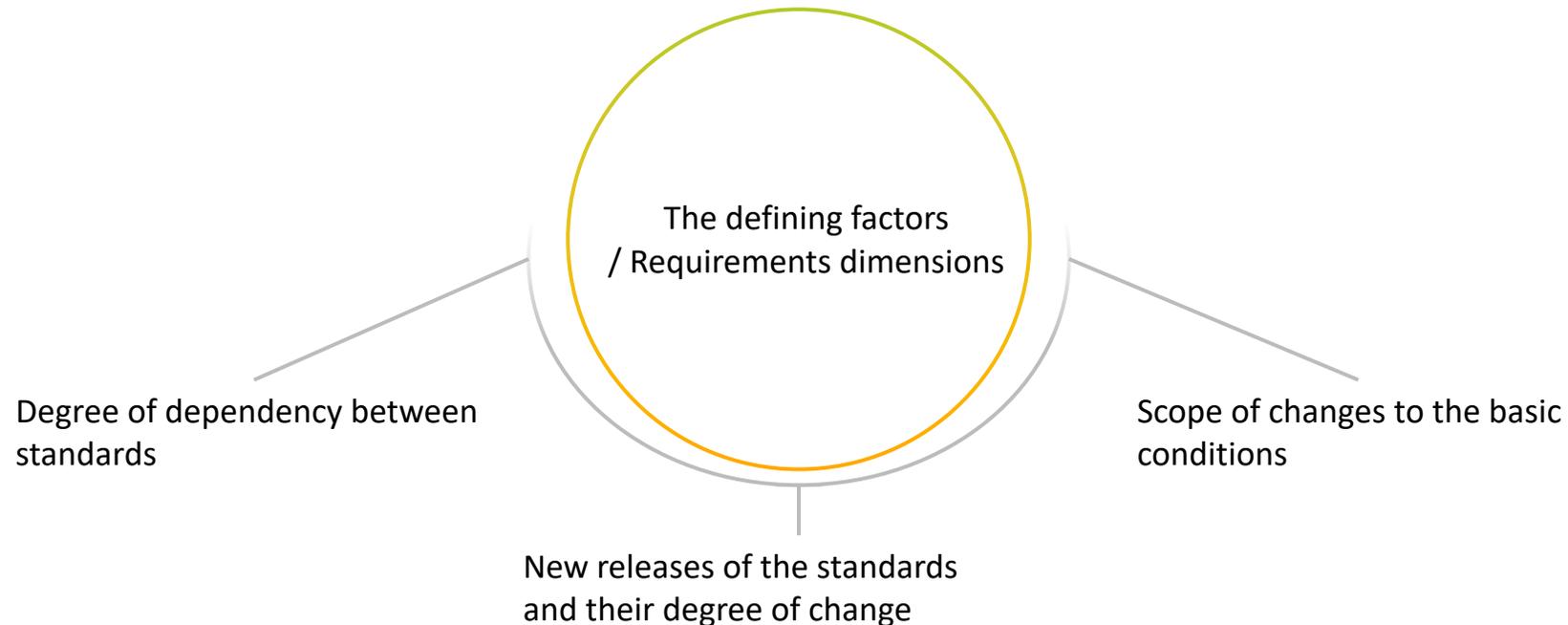
Backward compatibility determines the timeline for recertification

Backward compatibility is intended to determine the temporal extent of a recertification requirement and the validity of the current certification in the CX ecosystem, taking into account compliance with the requirement dimensions*.

Changes in requirements, e.g., new relevant standards for the use case or new CAC lead to recertification.

At the end of the transitional period the certified person will be deprived of the right to operate in the CX ecosystem.

The backward compatibility and thus the transition period can be suspended by Catena-X if necessary**.



* Requirements/requirement dimensions are described in the next chapter

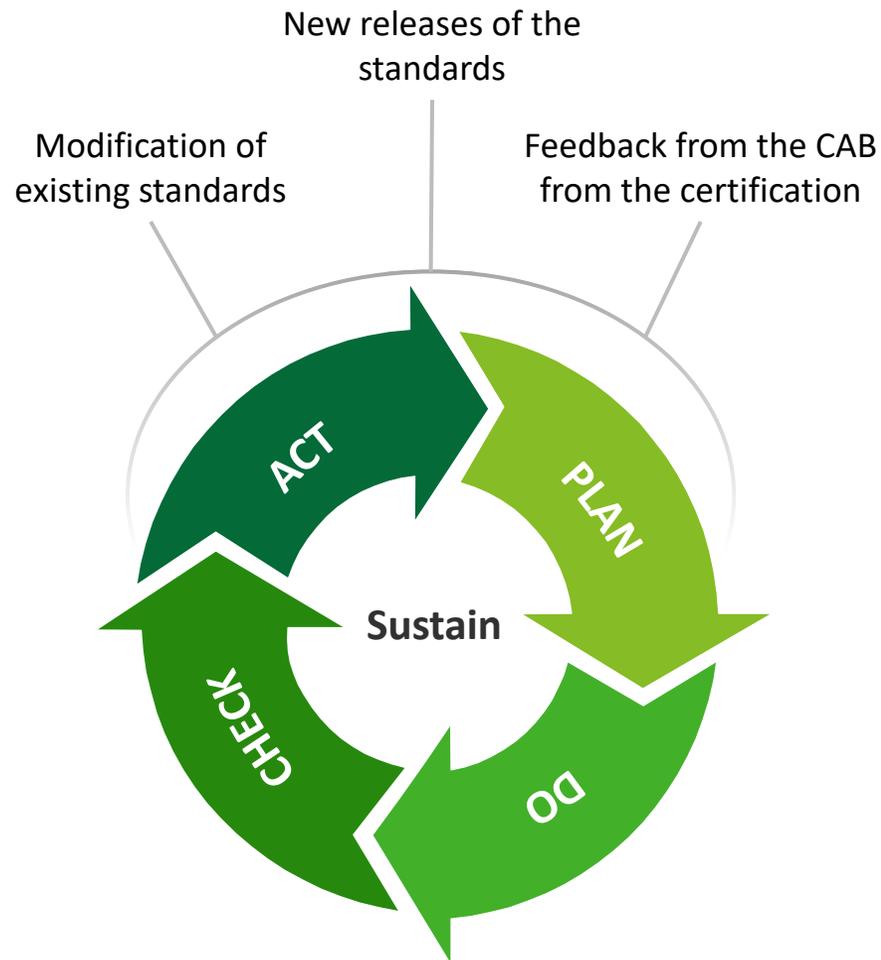
** The suspension of the transition period can take place, for example, by the introduction of a major release.

**10. Up-to-date
status of
certifications**



The update process of the framework

The PDCA cycle is initiated both from the innovation or adaptation of the standards, and via feedback from the CAB from the certification applicants



PLAN

- Anticipatory planning of the new standards in cooperation with standardization (backward compatibility with older versions of standards)
- Identify certifications that are subject to recertification
- Start the update process with publication of the standards in the association (45 days – opt-out)

DO

- Improvement/amendment of certification steps based on the new/changed Conformity Assessment Criteria

CHECK

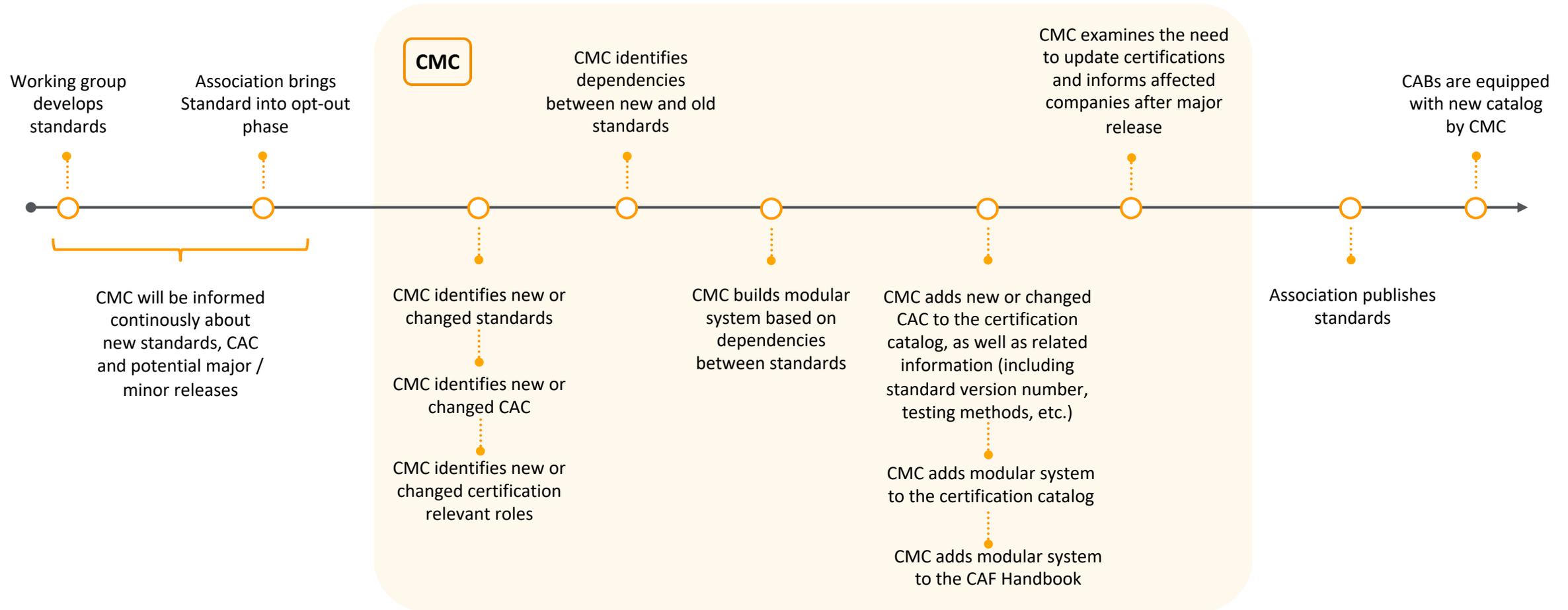
- Discussion and review of an adapted framework with Catena-X and introduction of the results from the discussion
- Proof of concept of the adapted standard in the framework

ACT

- Implementation of the amendments of the standards into the framework
- Notification of providers and certificate holders on re-certification need (tracking)
- Set implementation deadlines

Updating and maintaining the certification catalog

The certification catalog is updated according to a uniform process

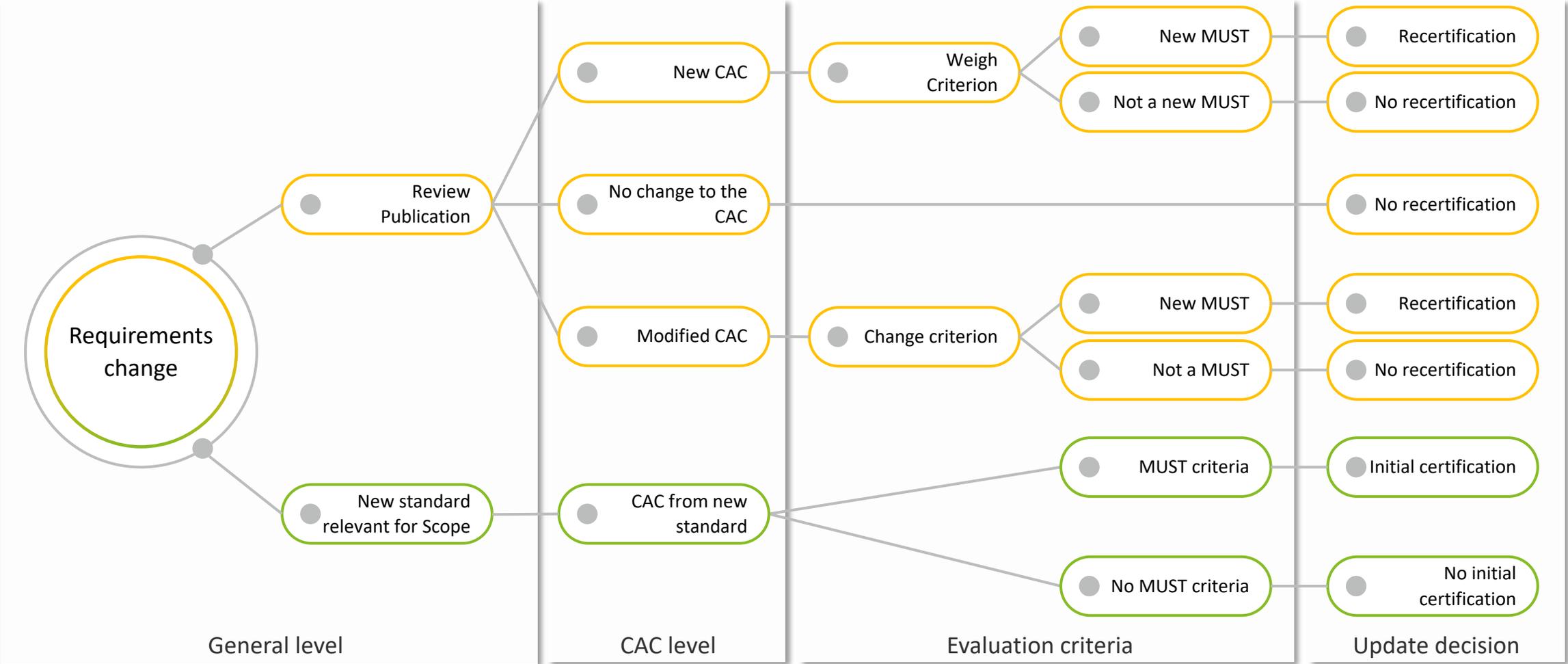


Roles in the process:

1. Maintainer of the framework: Certification Management Center (CMC)
2. Publisher of the standards: Catena-X Association
3. Creators of the default candidates: Catena-X consortium later association
4. Certifiers: Conformity Assessment Body

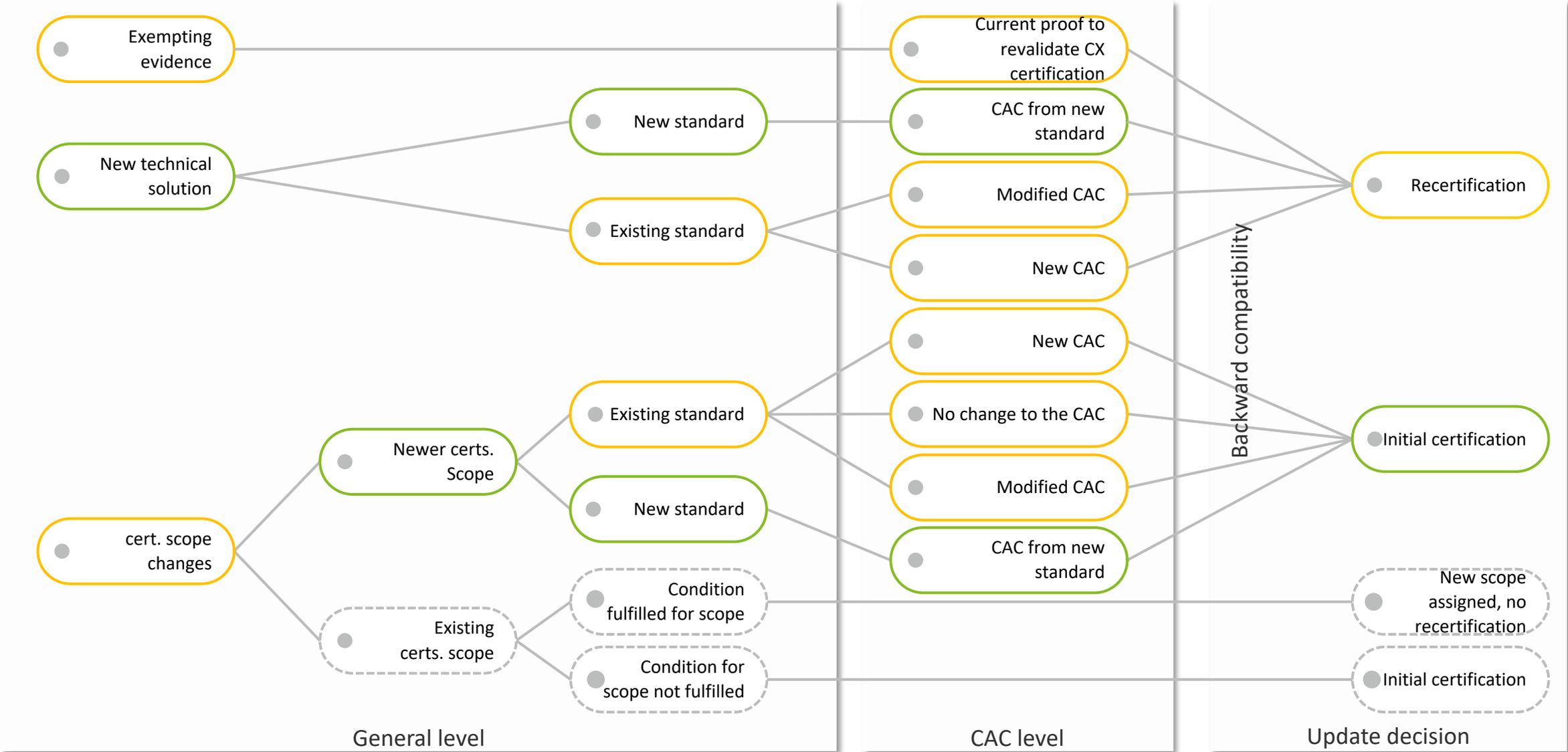
Decision tree for the update process – CAC changes

The update process is necessary due to changing requirements



Decision tree for the update process – other changes

The update process follows the decision tree for recertification



RASCI matrix on responsibilities (consortium time and post-consortium)

The role of the Certification Management Center (CMC) and its interaction with other participants of the certification process is described in a RASCI matrix

Extract illustrating the role of the CMC	CMC	Association's Board	TC4S *	Applicant	CAB	Consortium
Setting Major Changes	C	A	R		I	R
Bringing the standards into opt out	C	A	R		I	R
Publishing standards	C	A	R	I		C
Maintenance of the framework	R	A	C		I	S
Transfer from the latest Catalog	R	A	C	I	I	
Determine the need for update process	R	A	C		I	C
Certification	C	A		S	R	
Securing certificates	R	A			S	
Publication of certification results	R	A			S	
Maintenance of accredited CAB	R	A		I	I	
Answering questions from certification applicants	R	A			S	

* Technical Committee for Standardization

After the dissolution of the consortium, the standardization department in the association takes over the responsibilities for determining major changes from the consortium.

- **Responsible:**
Who are the stakeholders who carry out the tasks and who makes the decisions
- **Accountable:**
Who bears the responsibility and supervises the tasks and is ultimately responsible for the tasks
- **Support:**
Who supports the responsible team
- **Consulted:**
Who advises the responsible team
- **Informed:**
Who is kept informed at all stages of the project

11. Miscellaneous



Redundancy-free information

The Conformity Assessment Framework (CAF) does not define any terms related to the standardization of Catena-X



Catena-X defines the following in connection with conformity assessment:

- Catena-X Standards
- Addendum to standards
- Conformity Assessment Criteria
- Proof of conformity
- Roles within Catena-X
- Use cases of Catena-X

**Single
Point of
Truth**

The terminology for **Conformity Assessment Framework** is defined here in the handbook and in the corresponding certification catalog.

The CAF only defines terms within the handbook. These terms can be found in the glossary of the framework.

At points where the origin and accuracy of information is questioned, the single point of truth lies with the Catena-X Automotive Network e.V.

**Catena-X publishes standards and other documents through defined processes.
This only defines the single point of truth.**