



DATA SPACE 4.0

Technical Pillar: Data Space for Manufacturing Conformity & Certification

Begoña Laibarra

DATA SPACE 4.0 Final Event - 31st May 2024

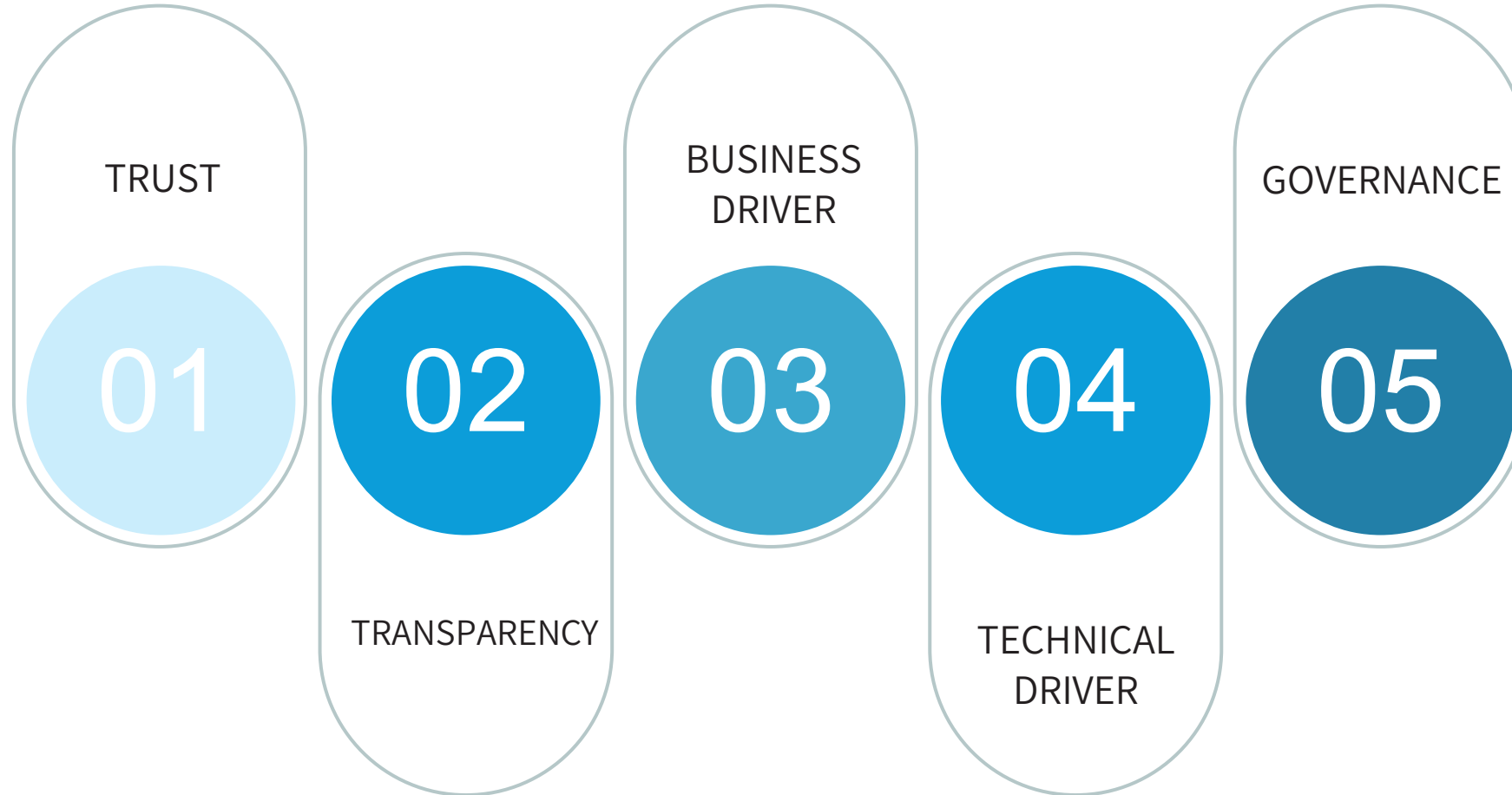


TRANSFORMING
MANUFACTURING
TOGETHER

Overview

- 01 Why is Certification a Pillar for the Manufacturing Data Spaces?
- 02 Existing Certification Schemes
- 03 Recommendations and Next Steps

Why Certification?

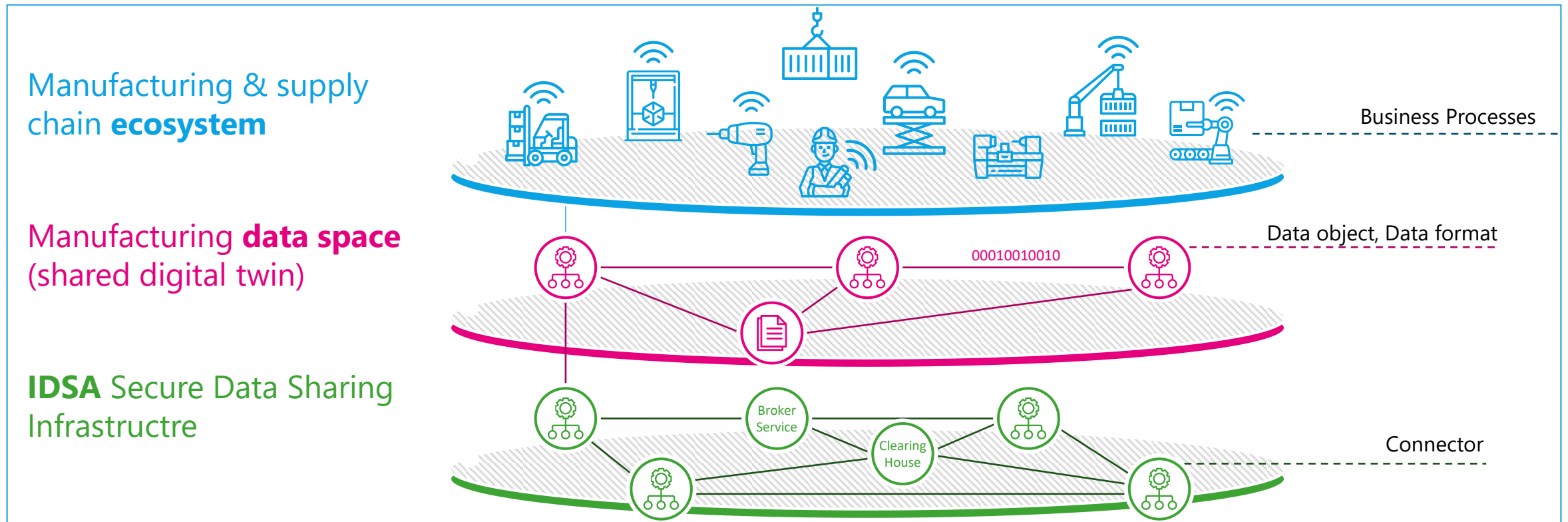


Certification Schemes



IDSA

IDS Reference Architecture Model (**IDS RAM**), the **IDS Rulebook**, and the **Dataspace Protocol**, constitute technical specifications for implementing data spaces.



Source: Boris Otto, Data Spaces Dialogue: Design Principles for European Data Spaces

IDSA Certification Principles

IDS certification defines **common security standards** for the technical components and the operational environment of data exchange. **Collaboration needs total Trust. Trust in the participating organization and Trust in the components**

ISO 27001, BSI C5

DIN27070

Operational Environment Certificate

With whom do I want to exchange my data?

The evaluation provides an assessment of the trustworthiness of the physical environment, defined processes and organizational rules.

Core Component Certificate

How secure is the component used?

The evaluation and certification of IDS core components is based on whether they provide the required functionality, interoperability and security regarding the security profiles.



IDSA Certification Principles

The Scheme identifies **3 different Trust and Assurance Levels** for Components and Participants

Operational Environments

Core Components

Evaluation and Assurance Effort

	Assurance Level 1 CheckList & Automated Interoperability Testing	Assurance Level 2 Concept Review, seguridad; funcionalidad	Assurance Level 3 Concept Review, Testing and Source Code Audit
Requirements Covered			
Trust Level 1 Interoperability	☑	Open For Certification ☑ Evaluation Facility	
Trust Level 2 Usage Control		☑ Evaluation Facility	☑ Evaluation Facility
Trust Level 3 Protection Against Internal Attacks		☑ Evaluation Facility	☑ Evaluation Facility

	Entry Level	Member Level	Central Level
Data Owner	Required	Recommended	Optional
Data Provider	Required	Recommended	Optional
Data Consumer	Required	Recommended	Optional
Broker Service Provider	–	Required	Optional
App Store Provider	–	Required	Optional
Vocabulary Provider	–	Required	Optional
Service Provider	–	Required	Optional
Clearing House	–	–	Required
Identity Provider	–	–	Required

IDSA Certification Principles

IDS certification of technical components and the operational environment is a **transparent process**.

The Certification Body

- ✓ Manages the certification process
- ✓ Defines the standardized evaluation procedures
- ✓ Supervises the actions of the evaluation facilities

The Applicant

- ✓ Provides the necessary resources
- ✓ Provides all necessary information and evidence to the Certification Body

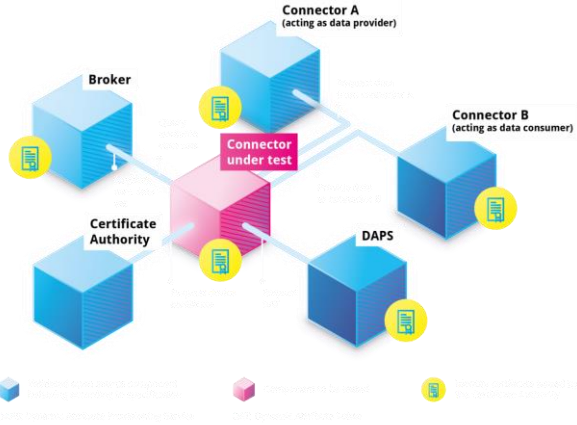
The Evaluation Facility

- ✓ Gets approved by the IDS certification body
- ✓ Carries out the actual assessment of an applicant

IDS Certification Assets

1

IDS Reference Testbed



2

Self Assessment Questionnaire



3



TCK for IDS Data Space Protocol

Incubator

IDSA Qualification Professionals

Consultancy
Guide companies on the adoption

DATA SPACES BUSSINESS CONSULTANT

DATA SPACES TECHNICAL CONSULTANT

Data Space Operation
Operate and maintain Data Spaces

DATA SPACES OPERATOR

DATA SPACES AUDITOR

Development
Develop components

BoK

IDS CORE COMPONENT DEVELOPER

IDS TEST MANAGER

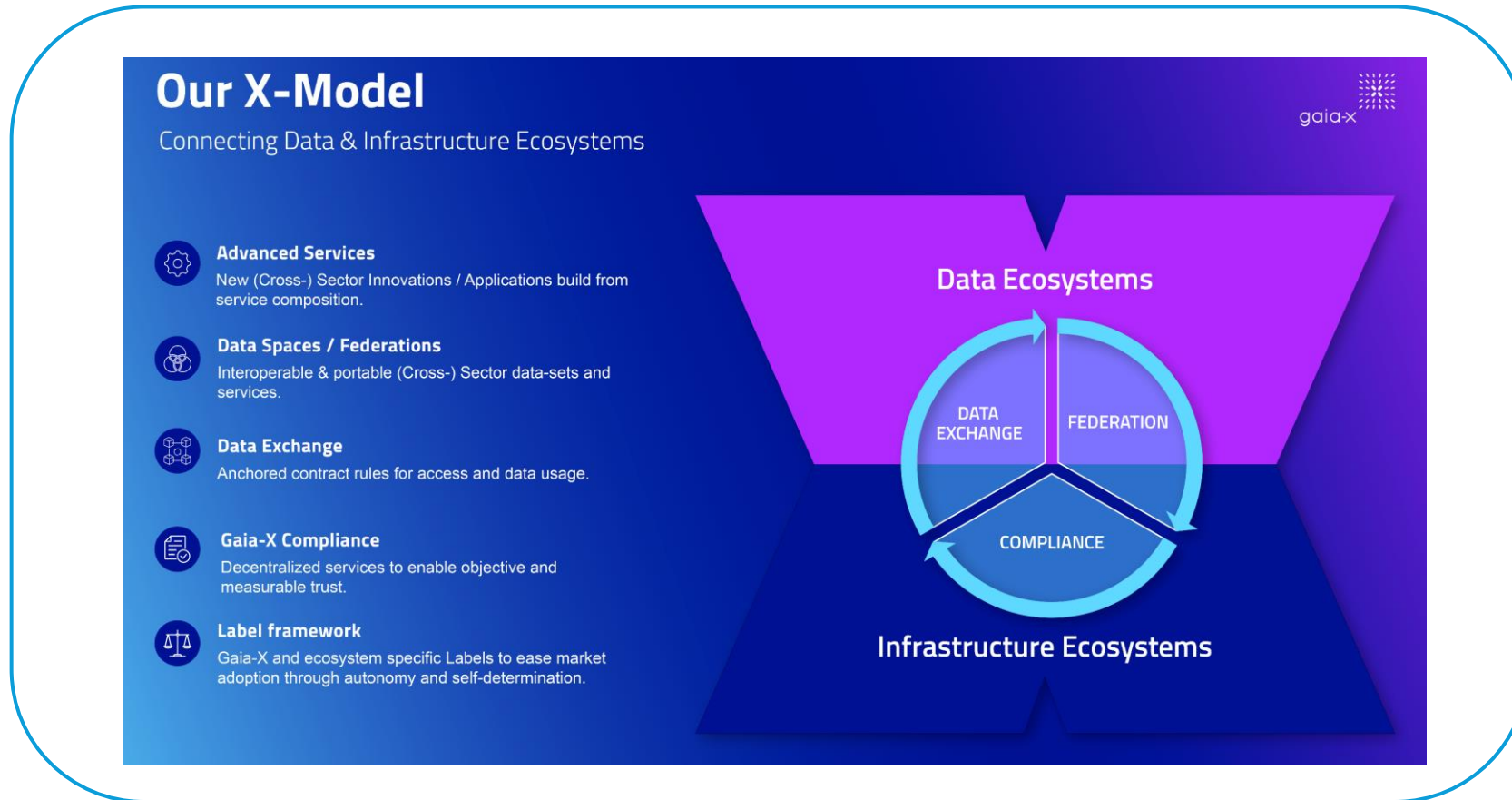
IDS approved

Core Foundation
Begin your professional Journey

DATA SPACES FUNDAMENTALS

GAIA-X

European initiative for a **Secure and Federated** data infrastructure. **GAIA-X Compliance**.



GAIA-X Labelling Framework

Label Level 1

Label Level 2

Label Level 3

Compliance Criteria

This level ensures compliance with basic requirements related to data protection, transparency, security, portability, and flexibility

This advanced label extends the basic requirements from Label Level 1 and includes a higher level of security and transparency regarding applicable legal rules and potential dependencies.

This level aims to meet the highest standards for data protection, security, transparency, portability, and flexibility, as well as European control.

Requirements

These requirements are based on the rules defined in the Gaia-X Policy Rules Document and a set of technical requirements derived from the Gaia-X Architecture Document.

It extends the requirements of Label Levels 1 and 2 and includes criteria that ensure immunity to non-European access and a strong degree of control over vendor lock-in.

Service Location

The option of a service location in Europe must be provided to the consumer.

A service location in Europe is mandatory at this level

Cybersecurity

For cybersecurity, the minimum requirement is to meet ENISA's European Cybersecurity Scheme - Basic Level.

For cybersecurity, the minimum requirement is to meet ENISA's European Cybersecurity Scheme - Substantial Level.

For cybersecurity, the minimum requirement is to meet ENISA's European Cybersecurity Scheme - High Level.

GAIA-X Clearing House

The GXDCH offers **automated compliance checks** against Gaia-X rules, facilitating the onboarding of new participants into the Gaia-X ecosystem. This involves validating credentials and issuing a Gaia-X Compliance Credential if requirements are met.

Gaia-X Lab		
Compliance	Registry	Notary
1.13.1	1.9.2	1.6.2
UP	UP	UP

Aruba		
Compliance	Registry	Notary
1.11.2	1.9.2	1.6.2
UP	UP	UP

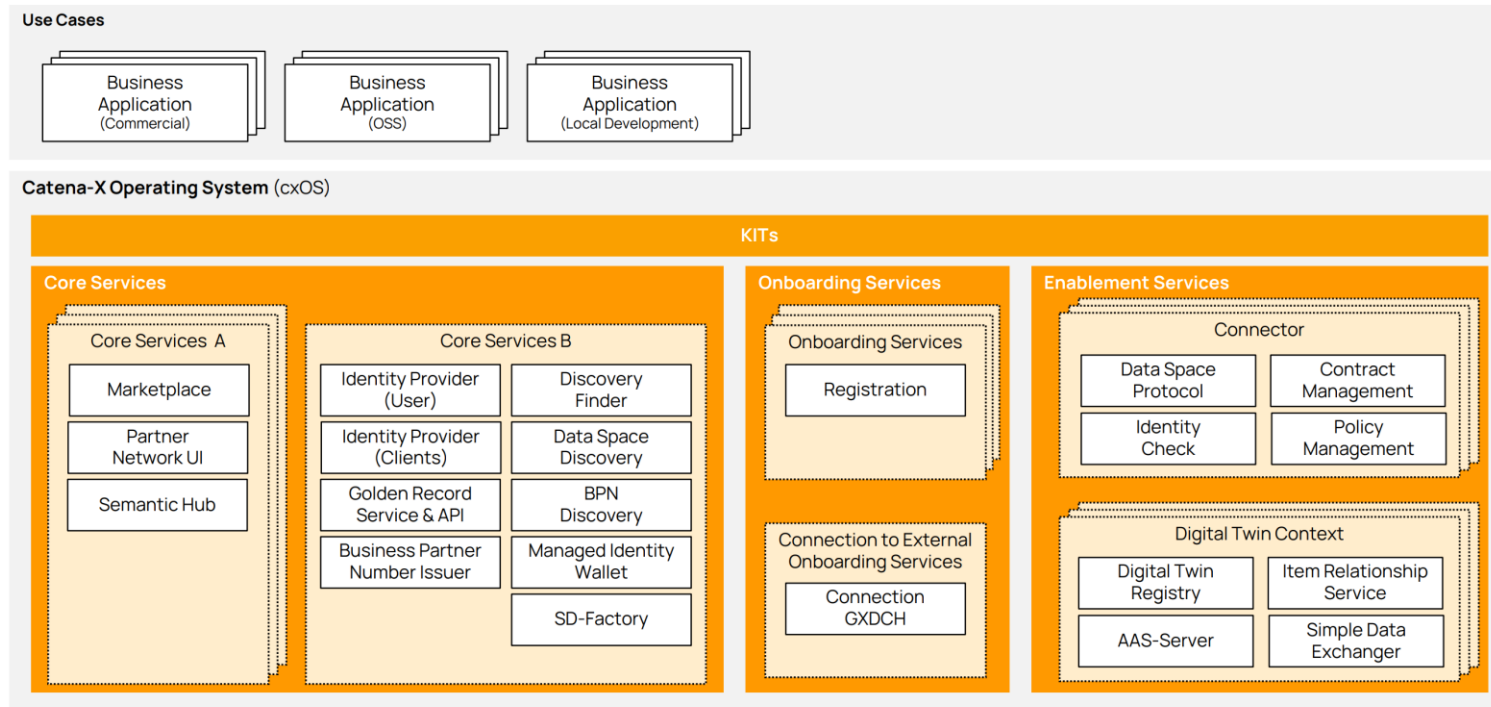
T-Systems		
Compliance	Registry	Notary
1.11.2	1.9.2	1.6.2
UP	UP	UP

Aire Networks		
Compliance	Registry	Notary
1.11.2	1.9.2	1.6.2
UP	UP	UP

[Learn more about Gaia-X Clearing House](#)

CATENA-X


Catena-X is an open and collaborative data space for the automotive industry with the aim of **solving industry problems together, and built on two major principles “Interoperability” and “data sovereignty”**. It provides services and use cases. At the moment, **10 uses cases & solutions are available**.



CATENA-X Certification Principles

Supported by a **Library of Standards** developed and maintained by CATENA-X Associations








Capabilities	Version	Title	Download
Data Discovery Services	1.0.2	CX - 0001 EDC Discovery API	Download file
Semantics	2.1.0	CX - 0002 Digital Twins in Catena - X	Download file
	11.0	CX - 0003 SAMM Aspect Meta Model	Download file
Data Chains	2.0.0	CX - 0005 Item Relationship Service API	Download file

[Back to Top](#) 

CATENA-X Certification Principles

Role-based and Modular based

(1) Core Service Providers, (2) Enablement Service Provider, **(3) Business Application Provider**, (4) On-Boarding Service Provider, **(5) Consulting Provider**, (6) Data Provider and Consumer, and (7) Conformity Assessment Body.

Modular System Catena-X Certification																	
Data Provider & Consumer	Enablement Service Provider		Business Application Provider ²										Core Service Provider	Value Added Services ¹	Onboarding Service Provider		
Connector	Connector As a Service	Digital Twin Registry	PLM & Quality	Traceability	Behavioral Twin	PCF	Circularity	Eco Pass	MaaS	Modular Production	DCM	OSIM	PURIS	Core Services	Value Added Services ¹	Onboarding Services Provider	
																	
			<p>Connector: Every Solution must be enabled to use an EDC or have an integrated EDC</p> <p>Semantic: Digital Twin or Agents</p>														
<p>Provider Base</p>																	

¹ Can only be provided in combination with certified Core Services

² Business Application Provider has to perform an interoperability check

CATENA-X Certification Principles

A Marketplace of Providers and Solutions

Certified Operating Company (CSP-A/CSP-B)



Certified Provider (e.g., BAP, ESP, OSP)



Certified Solution (e.g., Business App, Service...)

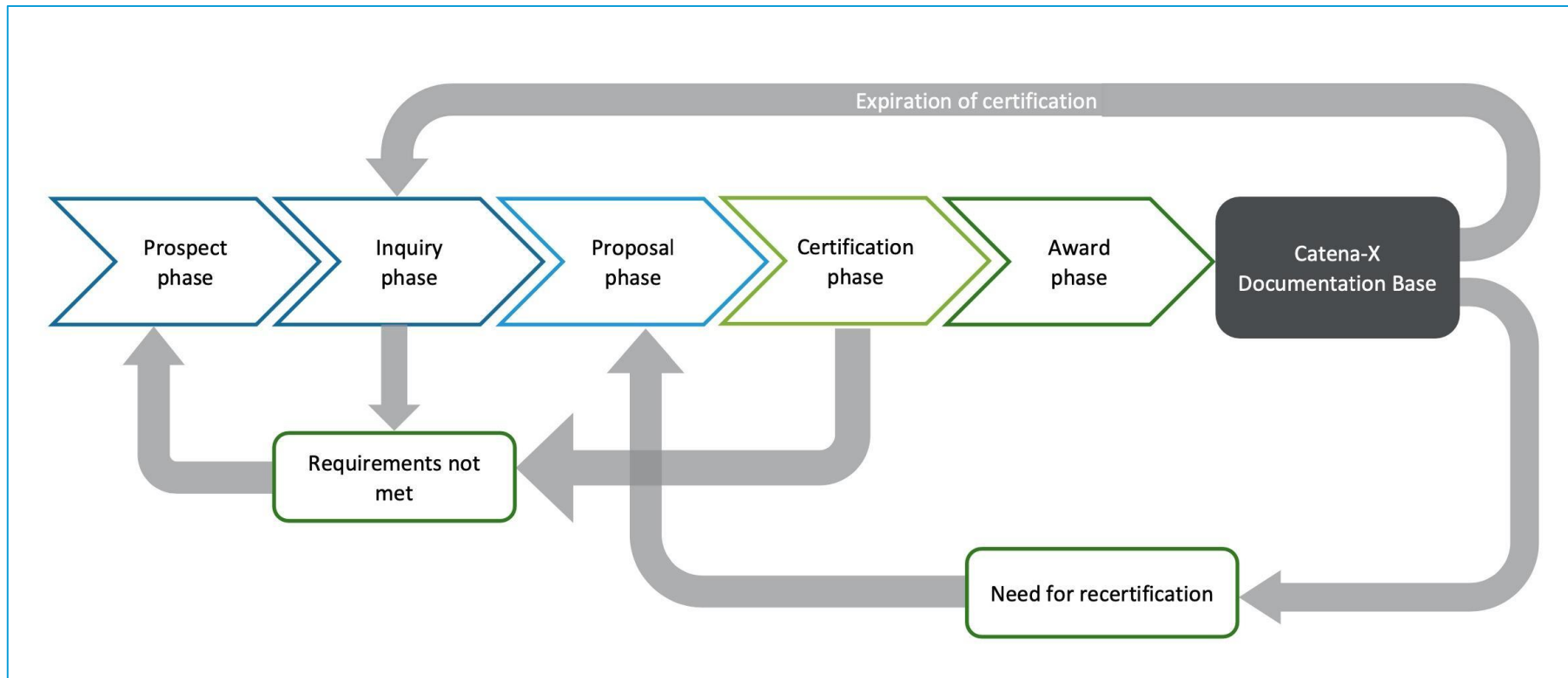


Qualified Advisor (Advisory Provider)



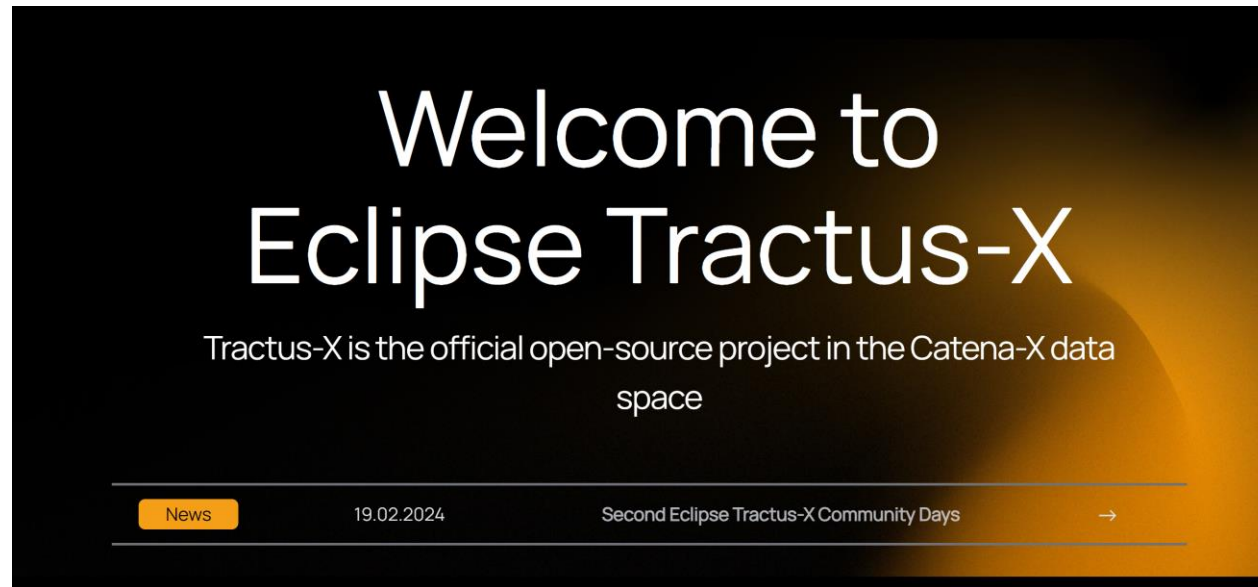
CATENA-X Certification Principles

Independent Compliance Process implemented through **Accredited CABs**



CATENA-X Certification Principles

Tractus-X, accelerate adoption, contribute to rapid scaling and **facilitate certification.**



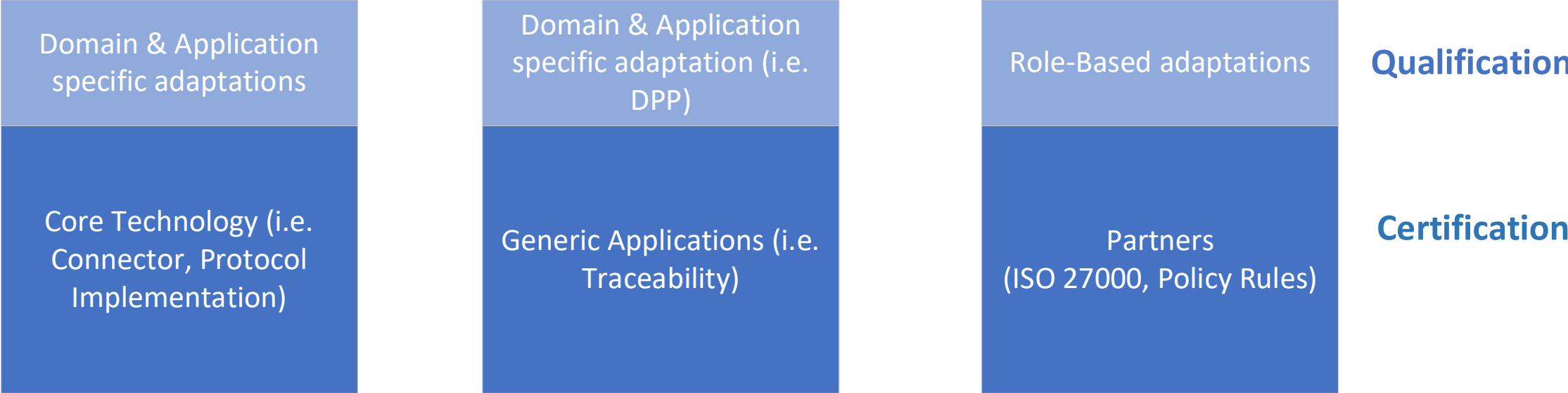
Recommendations

#	Description
1	The Standardisation and Certification Programme has to be a <u>Governance BB, with well defined roles and responsibilities</u>
2	Produce <u>Reference Specifications prepared for compliance certification</u> , aligned with Design and Operational strategies and decisions and with the MDS Development and Evolution Plan
3	Show alignment and actively contribute with global standardisation Initiatives (i.e. DSP)
4	Promote the “Acceptance” and “Mutual Recognition” of third-party Certifications, as far as possible!
5	Supported by Automated tools and based on Automated Specifications.
6	Establish different levels of assurance: certification vs qualification

Recommendations

#	Description
7	Use Reference Standards and Reference and Open Specifications. Identify and incorporate industry specific regulations
8	Cover technology, participants, applications and processes
9	Transparent Information to the Community
10	Provide Access to "Trustful" Assets
11
12

Evolution



DATA SPACE 4.0

**GRACIAS, THANKS, MERCI, DANKE, GRAZIE, DANK JE,
OBRIGADO**