Expert Group Profile

Description of the Expert Group

Related Committee	Architecture Management Committee
Name of the Expert Group	Trusted AI
Association Contact	Thomas Obermeyer

Description / Challenge / Initial Situation:

Artificial Intelligence has become a decisive competitive lever across industries, driving efficiency gains, predictive capabilities, and new business models at unprecedented scale.
In the automotive sector specifically, AI is accelerating transformation across the entire value chain — from supply chain optimization and quality management to autonomous driving and sustainability reporting. However, as AI adoption grows, so does the urgency to ensure these systems are trustworthy, governed, and compliant — particularly considering legal frameworks.

In the context of this document, “Artificial Intelligence” refers to systems that algorithmically **analyze, transform, or interpret data to support decisions and interaction between users or other AI systems**. It may include, but is not limited to, technologies in the fields of machine learning, natural language processing, computer vision, generative forms of AI such as Large Language Models, AI Agents or others.

In a collaborative data space like Catena-X, trust is the prerequisite for data sharing and ecosystem value creation. Without Trusted AI, the promise of cross-company, AI-driven intelligence in the automotive industry cannot be realized at scale.

The Catena-X Expert Group on Trusted AI aims to establish the foundations for responsible, transparent, and sovereign AI use across the Catena-X automotive data ecosystem.

The core distinction: While conventional AI focuses primarily on performance and output, Trusted AI adds critical governance dimensions — including explainability, fairness, robustness, accountability, and regulatory compliance — ensuring AI systems are not just effective but also reliable and auditable.

Architecture Design Dimensions of Catena-X:

- **Data sovereignty:** AI models operating in Catena-X must strictly respect contractual data usage policies across company boundaries
- **Multi-party trust:** In a cross-organizational ecosystem spanning OEMs to SMEs, every participant must have confidence that shared data is not misused or inadvertently exposed by AI systems
- **Regulatory readiness:** Standardized trust criteria across the ecosystem prevent fragmented EU AI Act compliance and reduce legal risk
- **Adoption & value realization:** Critical use cases utilizing AI will only be accepted by users if participants trust the underlying AI
- **Interoperability:** Catena-X extends its standardization approach to AI model metadata, risk labels, and trust certifications, enabling comparable assessment of AI services

Goals:

The Trusted AI Expert Group establishes the foundation for responsible, transparent, sovereign, and auditable AI use in the Catena-X automotive data ecosystem. It defines the Catena-X-specific rules and patterns so that AI services can be registered, discovered, contracted, and governed across organizational boundaries. The expert group defines the boundaries of using AI across companies, aligned with Catena-X principles, governance frameworks and standards by:

- Conduct assessment/alignment of AI needs across CX business domains
- Translate assessment results into AI collaboration patterns
- Derive Conformity Assessment Body assessment criteria for AI CX standard(s)
- Ensure that usage of AI is transparently noticeable to the data space participants

The expert group covers AI collaboration patterns across companies, starting from but not limited to patterns already addressed in the AI Service KIT:

- Distributed Learning (Model Lifecycle Collaboration): e.g., Cross-organizational model training
- Distributed Inference: e.g., Inference across distributed datasets, confidential prompts
- Multi-Agent Interaction (Operational Collaboration Layer): e.g., Multiple AI agents acting on behalf of companies
- Policy-Governed AI Execution (Trust & Compliance Layer): e.g., Usage control policies (ODRL-style), contract-bound AI behaviors
- Ecosystem Intelligence & Optimization: e.g., Collaborative planning across supply chains & Multi-party optimization

For each pattern, the group specifies how AI assets are handled as dataspace assets—particularly how they are registered, discovered, contracted, and governed across organizations, with enforceable trust controls.

AI is a cross-cutting concern, so this expert group is closely aligning with Expert Groups like SSI, Data Space Connectivity and others.

Deliverables:

The group will provide a compact, normative foundation to be incorporated into the AI Service KIT, including:

- Overall Strategic Focus
  - Definition of AI scope including input from other expert groups (first 3 months)
  - Clusters of scenarios (technology, business) including risk assessment (hot spots of potential risk areas)
  - Develop Architecture reference patterns for trusted AI usage in Catena-X
  - Document challenges of deployment of AI in industrial context and propose solutions/recommendations

- Operational focus (CX Standards)
  - Policy and semantic specifications for AI usage constraints across companies,
  - Certification-relevant criteria (Conformity Assessment Criteria)
  - Define usage policy requirements and constraints, incl. practical examples based on Catena-X principles

- Define a minimal Trusted AI asset model (minimum metadata every Catena-X AI asset must expose), e.g., capability, usage purpose constraints, internal/external restriction, assumptions, provider/consumer roles, and responsibility boundaries.

- Validate the deliverables with concrete use cases, including, but not limited to:
    a. shared data used as context for an internal AI system,
    b. shared data used to train or fine-tune an internal AI system
    c. share AI services using dataspace capabilities
    d. AI services to support data discovery and exchange over the dataspace.

Don't forget to work with Tractus-X regarding the implementation and alignment with other initiatives. For further information on the roles, have a look at the Working Model.

Rough planning – Milestones / Outcome / Deliverables (e.g., "Date & Activities & Outcome"):

- **09/2026: Kick-off**
- **12/2026: Definition of first AI scope** including reference scenarios
- **03/2027: Definition of Trust Model and Controls**
- **03/2027: Policy and Constraint Definition, First CX AI Standard**
- **12/2027: Controls adapted to selected regulatory scenarios**

Why should I participate?

Joining the Trusted AI Expert Group is an opportunity to actively shape how artificial intelligence is responsibly embedded into the automotive data ecosystem. As a member, you will directly influence the architectures, governance principles, and standards that will define trustworthy, sovereign, and auditable AI use across company boundaries. You will collaborate with an interdisciplinary network of leading experts from OEMs, suppliers, SMEs, and technology providers, gaining unparalleled insights into both cutting-edge AI patterns and emerging regulatory landscapes. Your contributions will translate directly into Catena-X standards, conformity criteria, and reference patterns — work that will be adopted by an entire industry.

What is expected of me?

As a expert group member *you contribute your subject matter expertise to the group and your actively participate in work group meetings, workshops etc. A more comprehensive list of* responsibilities and skill requirements can be found further below in the chapter "Competence description expert group member".

For more information on the responsibilities of an Expert Group, have a look at the Working Model.

Organisation

Selection Framework:

The expert group selection framework and criteria is aimed at selecting members who possess the right blend of expertise, commitment, and diversity to foster expansion of artificial intelligence in data space based ecosystems Please find below an outline of requirements for Expert Group members (section “Competence description expert group member"). When applying, please make a statement on the following criteria to outline your best fit.

- Proper expertise in the field of machine learning, generative AI, AI agents, explainability, robustness, or related trust-enabling technologies, experience with federated systems, cybersecurity, or trust infrastructures
- Minimum availability of 20 hours per month, more is a plus.
- Commitment to regular, active participation and active contribution.
- Subject matter expertise in the relevant areas (*see skills description above for further details*).
- Agile mindset highly welcome

We are searching for max. 10-15 members across the industry (suppliers of different sizes and materials, OEM, SME, technology providers).

We would like to offer optionally to complement our “core” expert group with a review group that provides feedback and functions as an extended expert base. If you cannot make the minimum regular time commitment for the core team, you are welcome to join the review team. The time commitment is 8 hours per month.

Additionally, we are searching for a lead and co-lead of this expert group, enabling the expert group to achieve the deliverables (internal and external alignment, preparation and steering of meetings). Please notify us via the application forms. The estimated amount of additional time for that role is around 4h per week.

The final composition as well as the final expert group lead will be defined after the application period.

Responsibilities

Responsibilities and tasks	• Contribute subject matter expertise to the definition of Trusted AI scope, reference scenarios, and architecture patterns • Co-develop Catena-X standards, including policy and semantic specifications, conformity assessment criteria, and the minimal Trusted AI asset model • Validate concepts against concrete use cases (e.g., shared data as AI context, training/fine-tuning, AI services in the dataspace) • Document outcomes clearly and ensure deliverables are integrated into the AI Service KIT • Actively participate in regular expert group meetings, workshops, and working sessions • Align cross-functionally with related expert groups (e.g., SSI, Data Space Connectivity) to ensure consistency • Represent the perspective of your organization and stakeholder group (OEM, supplier, SME, technology provider)

Competencies, knowledge and skills

We are looking for a **diverse blend of expertise** to ensure balanced, well-grounded outcomes. Applicants should bring proven knowledge in **at least one** of the following fields:

Catena-X foundation	solid understanding of its governance, operational, and architecture aspects
AI and trust technologies	subject matter expertise in machine learning, generative AI, AI agents, explainability, robustness, or related trust-enabling technologies
Systems & dataspace architecture	experience with federated systems, cybersecurity, or trust infrastructures
Regulatory expertise	familiarity with the evolving AI regulatory landscape and its implications for industrial AI deployment