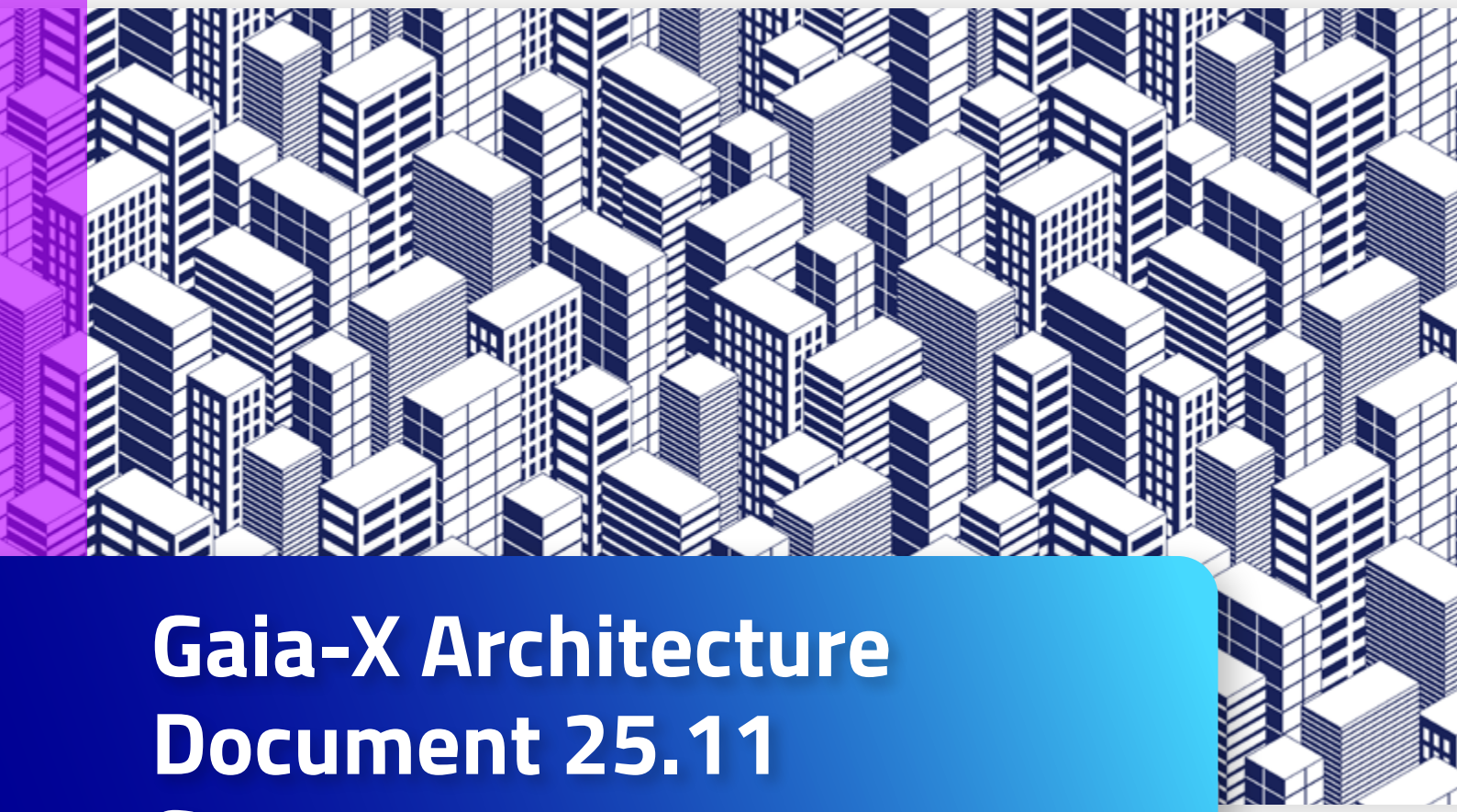

Gaia-X Architecture Document 25.11
Summary

Gaia-X European Association for Data and Cloud

November 2025

Contents

Gaia-X Architecture Document 25.11

Introduction

Every digital ecosystem is built on a set of explicit or implicit (governance) rules—often called an **ecosystem rulebook**. These rules follow the regulatory environment, reflect commercial and legal rules of participants and are aligned on technical and operational principles for realising the common value proposition of the ecosystem.

The Gaia-X Architecture Document specifies how digital ecosystems can establish and automate trust between participants and also between different ecosystems by defining interoperable mechanisms for the declaration and verification of an ecosystem rulebook.

Its **target audience** are technical stakeholders, such as business analysts, enterprise (IT) architects, system architects and technically inclined project managers designing digital infrastructure, service ecosystems, or data spaces with the need to establish an interoperable trust infrastructure.

This trust infrastructure provides:

- standards, protocols, and procedures for completely automating trust-related processes,
- support for a decentralized set up,
- interoperability with existing methods of establishing trust,
- trust-related interoperability across systems and participants within an ecosystem,
- interoperability with other ecosystems regarding trust and trust requirements.

Two Pillars of Trust: Compliance and Technical Compatibility

Trust is a multi-faceted and ramified interdisciplinary topic that is hard to define and even more difficult to formalise. However, it is an "important lubricant of a social system" and an extraordinary efficiency driver (Kenneth J. Arrow). For our purposes we have adopted the following definition of trust:

> *Trust is a favourable decision made by a relying party (often called 'trustor'), based on a risk assessment of potentially negative consequences, that another party ('trustee') will perform a particular action important to the relying party.*

Trust frameworks then specify means and conditions allowing a more efficient and reliable assessment of the potential negative impacts associated with such a decision.[1]

From a structural point of view, trust frameworks in general and the **Gaia-X Trust Framework** in particular, discriminate a technology-agnostic rules layer (captured in the so-called «rulebook») and a rule-agnostic technical compatibility layer for (potentially) full automation of conformity assessment within the scope of the rulebook.

---

1 For brevity reasons, we will not further explore these conditions in more depth, for instance, how a trustor may legally obtain the information on which their risk assessment is based (e.g., potentially requiring data usage agreements). We also will not elaborate deeper on the subtlety that, in digital ecosystem trust frameworks, trustors characteristically do not directly rely upon a trustee's actions but "trust" the validity and correctness of certain assertions articulated by the trustee. This is, for instance, reflected in the trust definition adopted by eIDAS.

An ecosystem rulebook characteristically defines criteria to achieve compliance with external (e.g., regulatory) requirements or criteria reflecting individual agreements within an ecosystem for technical, legal and standard conformity. For the Gaia-X Trust Framework, these rules are captured in the **Gaia-X Compliance Document**, defined and issued by the Gaia-X Policies and Rules Committee (PRC). It contains an extensive set of criteria based on regulatory requirements and the objective to ensure data protection (e.g., GDPR), sovereignty, cybersecurity and portability of services.

The **Gaia-X Architecture Document** complements it and defines the technical means, standards, and protocols to issue arbitrary credentials for any ecosystem rulebook in an automated and interoperable way, in particular but not at all limited to participant and service ("Label") credentials as specified in the Gaia-X Compliance Document.

Gaia-X Architecture: Scope and Usage

The Gaia-X architecture defines

- the mechanism to define rulebooks, rules, individual criteria and their means of automated validation the logical connection and dependencies between rules and criteria
- the structure of traditional and digital validation methods
- the digital proof of compliance
- the architecture and operationalization of services required for Trust Service Providers (like the Gaia-X Digital Clearing Houses)
- how federation of trust can be achieved between different sovereign and autonomous ecosystems such as Gaia-X itself and with other trust frameworks

Digital ecosystems, data spaces, applications, and IT systems use the Gaia-X architecture specification **to automate trust** by using the digital proof to:

- validate the identity of participants
- ensure that services (XaaS) and applications offered to the ecosystem are genuine and compliant to the agreed ecosystem rulebook
- validate any other entity and their properties relevant to the ecosystem (e.g., IoT devices, data space connectors, AI agents)
- validate claims by participants during contract negotiation of trusted data transactions
- These trust infrastructure services are then typically aggregated by ecosystem orchestrators in to higher level services
- to automate onboarding of participants to an ecosystem, or
- to create a marketplace where individual offerings can express proven compliance with agreed criteria (e.g. the Gaia-X Label Levels defined in the Gaia-X Compliance Document).

Gaia-X Architecture: Technical Foundation

The Gaia-X Architecture is rooted in the foundational standards of the W3C:

- **DID** (Decentralized Identifiers) for establishing and verifying digital identifiers
- **VC** (Verifiable Credentials Data Model 2.0) defining, validating, and verifying arbitrary claims about any subject
- **JWT** (Java Web Tokens – in the form of VC-JWT) for representing cryptographically signed (verifiable) credentials
- **RDF** (Resource Description Framework) and OWL 2.0 (Web Ontology Language) for defining data schemas and ontologies
- **SHACL** (Shape Constraint Language) for checking and enforcing compliance with common data schemas and ontologies
- **linked data** (JSON-LD) for creating instances of credentials

Additionally, it relies and uses the following standards for certain tasks:

- **LinkML** (Linked Data Modeling Language)
- **OID4VC** (Open ID for VC) for secure credential issuance and presentation
- **Eclipse CAP** (Conformity Assessment Policy and Credential Profile) ontology allowing so-called Notaries to turn arbitrary (paper or PDF) attestations of conformity assessment bodies (CAB) into machine-readable (verifiable) credentials.

It integrates very well with

- **ODRL** (Open Data Rights Language) for expressing access and usage policies
- **DCAT** (data asset catalog) for defining interoperable data catalogs.

The **Gaia-X Meta-Registry** (new in Gaia-X "Danube") extends the basic VC data model to so-called Ecosystem Trust Profiles allowing ecosystems to mutually trust credentials issued by "foreign" trust service providers, i.e., belonging to other ecosystems

Gaia-X 3.0 "Danube" Release

The Gaia-X Danube release of the Gaia-X open-source software (OSS) constitutes the software implementation of the Architecture Document 25.11 and a large subset of the ICAM Document 25.07. It is based on a completely re-factored architecture clearly separating the rules layer from the technical compatibility layer. This, by design, allows the quick and smooth integration of external trust services, domain-specific rule engines, and multi-ecosystem credential validation while remaining 100% compatible with the Gaia-X Loire release and the Gaia-X Digital Clearing Houses (GXDCHs).

Gaia-X

European Association
for Data and Cloud AISBL

Avenue des Arts 6-9

Bruxelles, Belgium

P.C. 1210

info@gaia-x.eu