An Introduction to the **Gaia-X Trust Framework**

Pierre Gronlier (Pierre.Gronlier@gaia-x.eu)
Gaia-X European Association for Data and Cloud

7 March 2024 v1.6

Gaia-X 2024

Contents

Executive Summary

The Gaia-X Trust Framework is a comprehensive system designed with three primary goals in mind: empowering users to make informed decisions across various jurisdictions and domains, accommodating specific needs of different regions and industries, and laying the groundwork for automated compliance processes.

Trust is a fundamental aspect of this framework, defined as the favourable response of a decision-making party assessing the risk regarding another party’s ability to fulfil a promise. Trust decisions are nuanced and influenced by various factors, and the Gaia-X Framework provides a methodology and technical specifications for risk assessment.

Interoperability is another key aspect, with a focus on organisational and semantic layers. The framework provides ontology and logic rules to translate the European values of transparency, openness, self-determination, privacy, and interoperability into machine actionable information. While initially targeting ICT services and data products, the technical protocols and data formats can be adapted for other use cases, such as the EU Digital Product Passport for various industries.

Guidelines are provided for both policy-rules makers and users. Policy-rules makers define assessment schemes and criteria, ensuring compliance with European values and legislation. Users can apply for assessments and procure services/products based on various levels of compliance, ranging from basic conformity to higher levels of cybersecurity and data processing restrictions.

Additional scoring tools, known as Trust Indexes, are introduced to enhance the framework’s effectiveness and adaptability. These indexes enable more granular rankings and facilitate comparisons between offerings, promoting interoperability and trust within the Gaia-X ecosystem.

In conclusion, the Gaia-X Trust Framework represents a collaborative effort across disciplines to promote organisational and semantic interoperability while adhering to European values and regulations. Its comprehensive approach and adaptable nature make it a valuable asset for fostering trust and compliance in digital ecosystems.

Abstract

Gaia-X’s mission is to:

> ”Enable trusted decentralised digital ecosystems creating the de facto standard aligned with European values by developing a set of policies, rules, specifications and a verification framework.”

To achieve the above mission a unique and new framework was developed by associating state-of-the-art and cutting-edge market standards: the Gaia-X Trust Framework.

1. Introduction

The Gaia-X Trust Framework is designed with three objectives in mind:

- help the users of the framework make educated decisions independently of the jurisdictions and domains in which they operate.
- be extendable for specific jurisdictions (Japan, . . .) and domains needs (finance, health, . . .)
- be the starting point for the elaboration of automated compliance.

To be noted that this document does assume knowledge of concepts like vocabularies, cryptographic certificates and data structures that are common to most ICT1[1] engineering fields and is referring to external resources the reader should be familiar with.

The first important element of that framework is Trust. In accordance with the commonly accepted English definitions[2] for trust, trust is defined in this document as "*the favourable response of a decision-making party who assesses the risk concerning the target party's ability to fulfil a promise*".

This definition implies the following:

- Trust involves at minima two parties: the decision- making party p1 and the target party p2.
- Trust is not automatically reciprocal or mutual: the fact that the decision-making party trusts the targeted party doesn't imply that the reverse is true p1 trusts p2 ≠⇒ p2 trusts p1.
- Trusted (1) or untrusted (0) is the result of the decision-making process Tχ(p1, p2) performed by the decision-making party p1 on a promise χ and using a risk threshold τχ as a decision criterion.

It's important to note that the risk assessment is rarely an abrupt binary decision; risk is usually expressed by a combination of heuristic[3] $r_n \circ \cdot \cdot \cdot \circ r1$ in terms of risk sources[4], potential events[5], their consequences[6] and their likelihood[7].

$$T\chi(p_1, p_2) = \begin{cases} 1 & \text{if } r_n \circ \cdots \circ r_1(p_1, p_2, \chi) > T\chi \\ 0 & \text{else} \end{cases}$$

This also means that the same decision-making party p1, having access to the same available information about target party's p2 capabilities, might make different final trust decisions, depending on the promises $\chi_1, \chi_2, \ldots$.

The Gaia-X Trust Framework provides a methodology and technical specifications for collecting and organising the information needed to perform this risk assessment.

Later in this document, a party p ∈ P [8], which can be either a P = {legal entity, natural person, process[9]}, is always uniquely identifiable, ∀p1, p2 ∈ P, if p1 ≠ p2 then Id(p1) ≠ Id(p2).

To conclude this introduction, the Gaia-X Trust framework helps to objectivise and rationalise the risk assessment and decision-making process and can be used to implement automated compliance.

The second important element of that framework is Interoperability. The European Interoperability Frame- work[10] lists four different interoperability layers: Legal, Organisational, Semantic, and Technical.

[1] ICT: Information and Communication Technology

[2] trust: Collins, Cambridge, Oxford

[3] heuristic: https://en.wikipedia.org/wiki/Heuristic

[4] risk source: https://www.iso.org/obp/ui/en/#iso:std:iso:31000:ed-2:v1:en:term:3.4

[5] potential event: https://www.iso.org/obp/ui/en/#iso:std:iso:31000:ed-2:v1:en:term:3.5

[6] consequence: https://www.iso.org/obp/ui/en/#iso:std:iso:31000:ed-2:v1:en:term:3.6

[7] likelihood: https://www.iso.org/obp/ui/en/#iso:std:iso:31000:ed-2:v1:en:term:3.7

[8] W3C Open Digital Rights Language party: https://www.w3.org/TR/odrl-model/#party

[9] process: https://en.wikipedia.org/wiki/Process_(computing)

[10] European Interoperability Framework: https://ec.europa.eu/isa2/eif_en/

The Gaia-X Trust Framework targets the Organisational and Semantic layers by providing an ontology[11] and a set of second order logic[12] rules to translate the European values of transparency, openness, self-determination, privacy and interoperability into machine actionable information.

While the Gaia-X Trust Framework primarily targets ICT services and data products, the technical protocols and data formats used by the Gaia-X framework can easily be reused and adapted for other use cases such as the EU Digital Product Passport[Gal22] for batteries, cosmetics, clothes, . . .

2. Fundamentals

For the decision-making party to perform a risk assessment, information, referred later as claims, about the target party, its capabilities, and the promise, referred later as the objects of the assessments, must be collected.

To organise the collected claims, the Gaia-X Trust Framework relies on asymmetric cryptography[13] and linked data[14] to:

- build a machine-readable knowledge graph of claims about the objects of assessment.
- be able to verify at any time the content integrity of the claims.
- keep track from where the claims originated from or to keep track of the parties issuing the claims, referred later as the issuers.

Then, to have organisational and semantic interoperability, the Gaia-X Trust Framework provides:

- generic information models such as the Licensor- Licensee, Producer-Provider or Provider-Consumer relations, the law of obligations[15], the contracting procedures, and rules.
- data exchange specific information models such as data transactions, data intermediaries, consent management for data processing, policy management.
- vocabularies and schemata to describe the characteristics of the objects of the assessments, and enable policy reasoning on those characteristics[FCC19] [De +19], like ICT services, cloud offerings like big data cluster, AI training and inferencing engines, hardware and software infrastructure including edge devices, data product, the licence and terms of uses.

To be noted that the last point introduces the topic of automated or supervised policy reasoning, which is a key element for future smart legal contract[Sch21] [AH22], including legally binding contracts[Smi17].

This framework also enables both parties p1 and p2 to exchange their roles where p2 becomes the decision- making party and p1 the target party. For example, in a context where p2 provides data processing services, p1 might want to ensure that the services provided by p2 meet its needs in terms of legal, operational and technical autonomy and p2 might want to ensure that p1 will use the service and process the data in accordance with the agreed terms of service and data processing purposes.

[11] ontology: https://en.wikipedia.org/wiki/Ontology_(information_science)
[12] 2nd order logic: https://en.wikipedia.org/wiki/Second-order_logic
[13] public-key: https://en.wikipedia.org/wiki/Public-key_cryptography
[14] W3C Linked-Data: https://www.w3.org/DesignIssues/LinkedData.html
[15] law of obligations: https://en.wikipedia.org/wiki/Law_of_obligations

To ease and foster the adoption by the market of the Gaia-X Trust Framework, the Gaia-X Association members decided to reuse as much as possible to existing vocabularies and terms defined in:

- The W3C Verifiable Credentials[16] and Linked-Data[17] standards.
- The vocabulary and general principles from the ISO Committee on Conformity Assessment (ISO/CASCO)[18]

3. Guidelines for the Gaia-X policy-rules makers

To help a decision-making party with its assessment, the Gaia-X policy-rules makers, ie Gaia-X Association members, have predefined four assessments scheme:

- The Gaia-X Conformity which specifies the mandatory requirements[19] for an object to be qualified as Gaia-X compliant.
- The Gaia-X Label level 1, level 2 and level 3 which add extra requirements specifically to EEA[20] legis- lation.

In the context of Gaia-X globalisation and keeping Gaia-X core EU values intact, it's important to note that it's up to the Gaia-X members to be innovative and articulate Gaia-X requirements that capture the intent of the legislation without necessarily referring to it.

For example, given the following two requirements with similar objectives:

- *"Regardless of its location and the location of the service users, a service provider must comply with EU GDPR[21]."*
- *"If personal or sensitive data is processed by a service provider, the later must always be able to prove, on request, that the owner of the data has given un- equivocal consent for its processing and for explicit purposes and duration."*

The first one adds little value to EEA providers and EEA residents, because the GDPR is already enforced by law. However, it adds a significant burden on providers not initially subject to EU law and surely slows down the adoption of Gaia-X standards globally, where similar data protection regulations are already in place: Japan[22], Brazil[23], Singapore[24], USA/California[25], USA/Virginia[26], . . .

The second one offers Gaia-X policy-rules makers the opportunity to further detail the semantics and syntax of the claims to be collected to demonstrate compliance with the requirement, such as consent, processing purposes, duration, service provider contact point for information requests, revocation of consent and so on, to reach semantic interoperability across existing data protection regulations.

This extra effort by Gaia-X members to detail as much as possible the semantics and syntax of the information required to provide evidence that a requirement is fulfilled is directly proportional to the future effectiveness of organisational and semantic interoperability.

To help the Gaia-X policy-rules makers, a decision flow chart1, has been developed in accordance with the ISO/CASCO and W3C Verifiable Credentials standards, starting from a high-level criterion down to measurable and comparable requirements.

[16] W3C Verifiable Credential: https://w3c.github.io/vc-data-model/

[17] linked-data: https://www.w3.org/wiki/LinkedData

[18] ISO/CASCO: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:17000:ed-2:v2:en

[19] requirement: https://www.iso.org/obp/ui/#iso:std:iso-iec:17000:ed-2:v2:en:term:5.1

[20] EEA: European Economic Area

[21] General Data Protection Regulation

[22] The Act on the Protection of Personal Information Act No. 57 of 2003

[23] General Personal Data Protection Law

[24] Personal Data Protection Act 2012

[25] California Consumer Privacy Act

[26] Virginia Consumer Data Protection Act

This workflow is summarised as follows:

1. For each requirement, the Gaia-X policy-rules makers must decide if the claims must be validated or verified.
   - For a validation[27], a 1st or 2nd party assessment activity is sufficient.
   - For verification[28], a 3rd party assessment activity is required.
2. For each claim, the Gaia-X policy-rules makers must specify one or more of the following lists:
   - The accepted claim's issuers.
   - The characteristics qualifying an accepted issuer.
   - The characteristics qualifying an accepted public-key to digitaly sign the claim.

Those lists or the results of the evaluation of the char- acteristics from those lists are referred in the Gaia-X Trust Framework as Trust Anchors and are published via the Gaia-X Registry service.

The careful selection of the Trust Anchors is critical for the result of the assessment to be legally relevant or legally binding.

Finally, a special attention from the Gaia-X policy-rules makers must be given to the scope[29] of the collected claims.

For each requirement r, the union of the scopes s(ci) of the collected claims ci must cover the entire scope s(r) of the requirement r, such as

$$s(r) = s(r) \cap \left(\bigcup_{i}^{n} s(ci)\right)$$

4. Guidelines for the Gaia-X policy-rules users

As described in the previous section, Gaia-X policy-rules makers have defined four assessment scheme:

- Gaia-X Conformity: the provider and consumer can make informed and educated decisions based on information gathered to demonstrate European values.
- Gaia-X Label level 1: on top of the Gaia-X Conformity, the provider and consumer can rely on their mutual declaration of adherence to the European data protection rules.
- Gaia-X Label level 2: on top of the Gaia-X Label level 1, cybersecurity criteria have been verified by impartial third parties and data can be processed exclusively in the European Economic Area.
- Gaia-X Label level 3: on top of the Gaia-X Label level 2, the data is processed exclusively in the European Economic Area and cannot be accessed by parties from outside the EEA.

This categorisation gives the users of the framework a mean to apply for an assessment and/or order services and data products with a rank r on a scale from 0 to 4 – non-compliant to compliant with Gaia-X Label level 3 - by increment of 1. $r \in \{0, 1, 2, 3, 4\}$.

However, this ranking:

- Doesn't automatically adapt to the market which always evolves faster than the rules.
- Doesn't capture the subtleties of organisational and semantic interoperability complexity, de facto lowering the interoperability to the basic commonly conceded denominators.

To address this challenge, additional scoring tools named Trust Indexes are developed as Veracity TV , Transparency TT , Composability TC and Semantic-Match TSM indexes. Those indexes enable the users of the Gaia- X Trust Framework:

- As a consumer to compare objects or offerings with a more granular ranking that wouldn't necessarily fit into one of the predefined conformity schemes. Eg: A service offering compliant with Label level 1 but not Label level 2 will be assessed with a

[27] validation: https://www.iso.org/obp/ui/#iso:std:iso-iec:17000:ed-2:v2:en:term:6.5

[28] verification: https://www.iso.org/obp/ui/#iso:std:iso-iec:17000:ed-2:v2:en:term:6.6

[29] scope: https://www.iso.org/obp/ui/#iso:std:iso-iec:17000:ed-2:v2:en:term:7.4

score rSO in the range 2.0 to 3.0 excluded, as in $r_{SO} \in [2.0, 3.0[$

- The providers to compare their offering with existing ones and help them to improve their interoperability; *"As a provider, is my service interoperable and composable with 10% or 90% of the other offerings in the Gaia-X Catalogues? "*

The proposed Trust Indexes T_V , T_T , T_C, T_{SM} are meant to be used by all parties - licensor, licensee, producer, provider, consumer, . . . - as a measure of distance for interoperability and trust with regards to the other offerings in the Gaia-X Catalogues; the intent being that Gaia-X helps the market by providing measurement tools and let the market actors themselves to converge to an optimum solution, similar to gradient descent algorithms[30] where an error metric is given and a process iteratively applied converge to an optimum solution.

For example, a provider that declares its services or products by providing only the bare minimum information without machine readable claims nor policies may still meet Gaia-X Compliance criteria but will have a low interoperability score with other offerings from the Gaia- X Catalogues and it would be in the provider's own inter- est to improve the quality and quantity of the provided information.

The Trust Indexes will be described more in detail in a separate document.

[30] Gradient descent: https://en.wikipedia.org/wiki/Gradient_descent

5. Conclusion

The Gaia-X Trust Framework specification is the result of a multi-disciplinary work astride the domains of compliance, maths, ICT and data privacy regulations with the mission to help organisational and semantic interoperability.

Furthermore, this framework describes an intention, a methodology, an architecture, and rules which, combined, are greater than the sum of the elements analysed separately, which gives this framework a sui generis quality.

This framework will be further developed as an enabler for automated compliance, and a separate document will be published to describe possible deployment models.

References

[Smi17] Jan Smits. Contract Law: A Comparative Introduction. English. 2nd ed. United Kingdom: Edward Elgar Publishing, 2017.

[De +19] Marina De Vos et al. “ODRL Policy Modelling and Compliance Checking”. In: Rules and Reasoning. Ed. by Paul Fodor et al. Cham: Springer International Publishing, 2019, pp. 36–51. ISBN: 978-3-030-31095-0.

[FCC19] Nicoletta Fornara, Alessia Chiappa, and Marco Colombetti. “Using Semantic Web Technologies and Production Rules for Reasoning on Obligations and Permissions”. In: Agreement Technologies. Ed. by Marin Lujak. Cham: Springer International Publishing, 2019, pp. 49–63. ISBN: 978-3-030-17294-7.

[Sch21] Thibault Schrepel. Smart contracts and the digital single market through the lens of a “law plus technology” approach. Tech. rep. 2021. URL: https://digital-strategy.ec.europa.eu/en/library/smart-contracts-and-digital-single-market-through-lens-law-plus-technology-approach.

[AH22] Jason Allen and Peter Hunn. Smart Legal Contracts: Computable Law in Theory and Practice. Oxford University Press, Apr. 2022. ISBN: 9780192858467. DOI: 10.1093/oso/9780192858467.001.0001. URL: https://doi.org/10.1093/oso/9780192858467.001.0001.

[Gal22] Michele Galatola. “Digital Product Passport”. In: European Commision, 2022. URL: https://circulareconomy.europa.eu/platform/sites/default/files/michele-galatola-european-commission.pdf.

Annexe 1

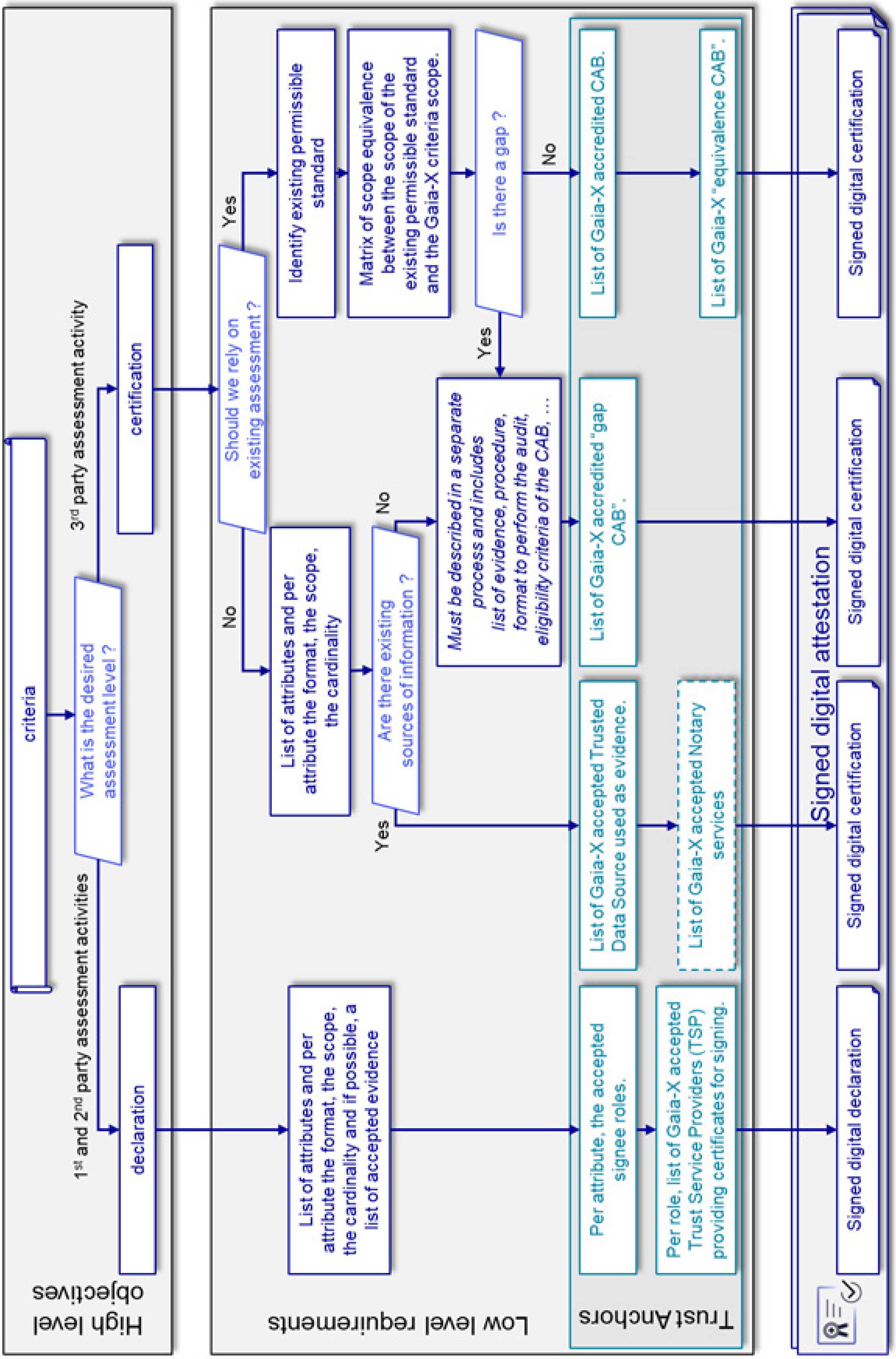
High level objectives
criteria
What is the desired assessment level ?
1st and 2nd party assessment activities
declaration
3rd party assessment activity
certification
Low level requirements
List of attributes and per attribute the format, the scope, the cardinality and if possible, a list of accepted evidence
Should we rely on existing assessment ?
Yes
No
Identify existing permissible standard
Matrix of scope equivalence between the scope of the existing permissible standard and the Gaia-X criteria scope.
Is there a gap ?
No
Yes
List of attributes and per attribute the format, the scope, the cardinality
Are there existing sources of information ?
Yes
No
Must be described in a separate process and includes list of evidence, procedure, format to perform the audit, eligibility criteria of the CAB, …
Trust Anchors
Per attribute, the accepted signee roles.
Per role, list of Gaia-X accepted Trust Service Providers (TSP) providing certificates for signing.
List of Gaia-X accepted Trusted Data Source used as evidence.
List of Gaia-X accepted Notary services
List of Gaia-X accredited "gap CAB".
List of Gaia-X accredited CAB.
List of Gaia-X "equivalence CAB".
Signed digital attestation
Signed digital declaration
Signed digital certification
Signed digital certification
Signed digital certification

Figure 1: Workflow for building a criteria

Gaia-X

European Association
for Data and Cloud AISBL

Avenue des Arts 6-9
Bruxelles, Belgium
P.C. 1210
info@gaia-x.eu