Software Requirements Specification

for

Gaia-X Federation Services

Compliance
Onboarding & Accreditation
Workflows
CP.OAW

Published by

eco – Association of the Internet Industry (eco – Verband der Internetwirtschaft e.V.)
Lichtstrasse 43h
50825 Cologne
Germany

Table of Contents

List of Figures

List of Tables

1. Introduction

To get general information regarding Gaia-X and the Gaia-X Federation Services please refer to [Gaia-X AD].

1.1 Purpose

This document specifies Onboarding and Accreditation Workflows (OAW) for the Gaia-X ecosystem. It introduces concepts, mechanisms, and descriptions on how to foster secure and reliable participation in the Gaia-X ecosystem and to achieve transparency for both Consumers and Providers.

On the one hand, this document describes onboarding processes for Providers to register themselves and their respective Gaia-X Assets (particularly Software Assets and Nodes). On the other hand, this document clarifies how Providers and, more importantly, Assets have to undergo thorough accreditation to ensure that the Gaia-X principles of transparency, security, data protection, and interoperability are fulfilled.

Further on, supporting management workflows are specified, such as offboarding Providers, managing compliance-relevant events, or assessing conformity assessment bodies.

These workflows will be implemented in a workflow engine that helps relevant stakeholders to perform each activity of the workflow. This work therefore aligns with the efforts of WP5[1] in defining a general workflow engine but differs by describing specifics for the OAWs and the resulting specification for the OAW engine.

1.2 Document Conventions – Glossary of Terms

1.2.1 Document Peculiarities

The document describes the product perspective, functions, and constraints. It furthermore lists the functional and non-functional requirements and defines the OAW engine's features in detail. The listed requirements are binding. Requirements as an expression of normative specifications are identified by a unique ID (e.g. [GX.OAW.ID.Number]) and the keywords MUST, MUST NOT, SHOULD, SHOULD NOT, MAY, corresponding to [RFC 2119], are written in capital letters.

This document was written in collaboration with the Gaia-X community in quite a short time and therefore it has reached a certain level of abstraction but may lack certain details. Only the main aspects and essential concepts were considered and can be extended in detail in an agile development process.

1.2.2 Glossary of Terms

Please note that this document uses specific terms, which may be used differently depending on the business language or context, among others. Please carefully read the following **glossary of terms** to ensure that you understand the meaning of the text paragraphs correctly.

[1] Please refer to appendix B for an overview and explanation of the Work Packages (WP).

This glossary of terms was adapted to fit the Gaia-X Conceptual Model (refer to [Gaia-X AD]).

1.2.2.1 Gaia-X Basic Terms

Everything that is referred to by a Gaia-X identifier is an object. Two most important objects are Gaia-X Assets and Gaia-X Participants that will be defined in the following. Figure 1 summarizes major relations between both objects. In addition, Gaia-X will set up further Gaia-X Entities that are required for the management and operation of the ecosystem.

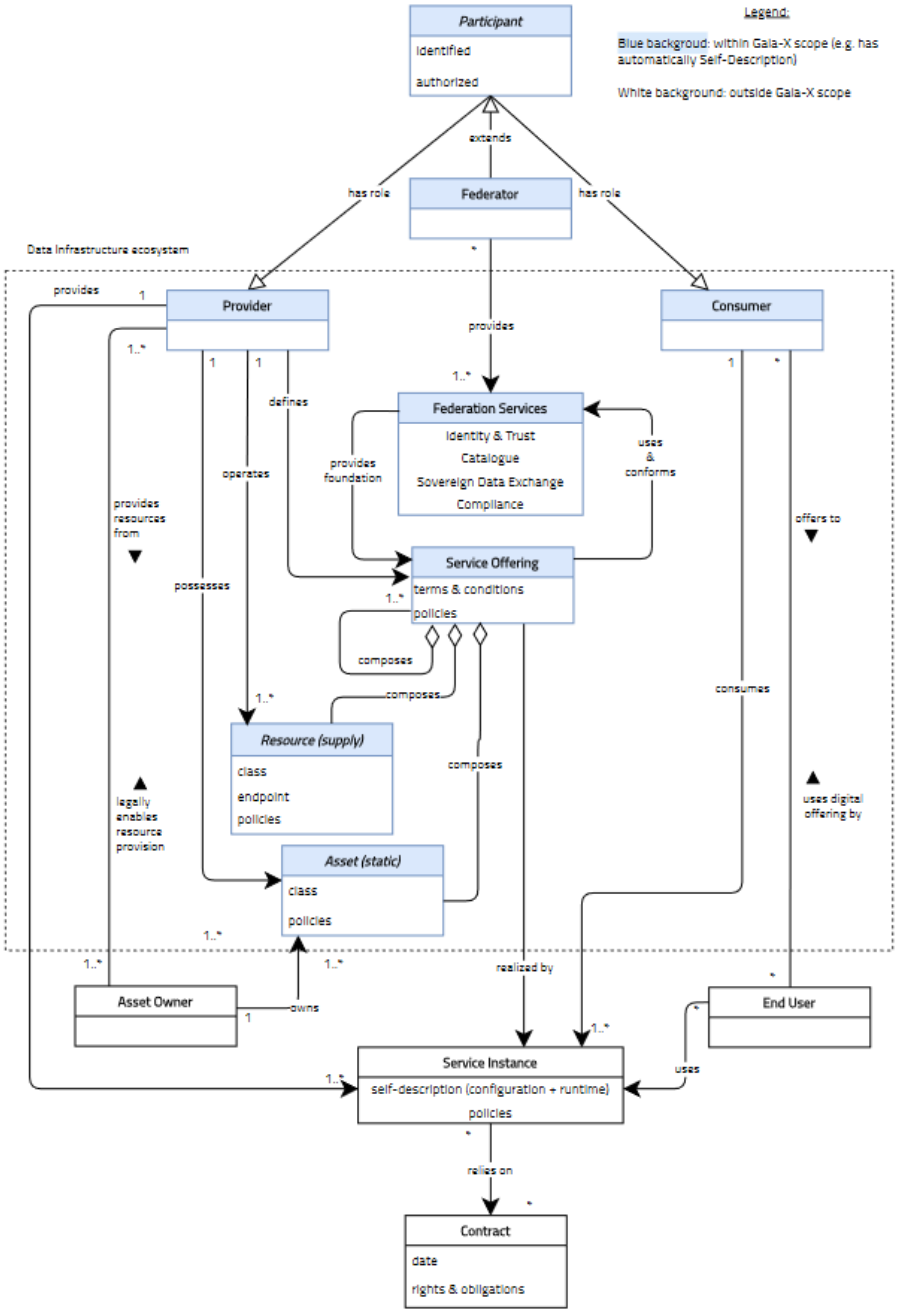


***Figure 1**. Gaia-X conceptual model (refer to [Gaia-X AD])*

Gaia-X Participants (refer to [Gaia-X AD])

A Participant is an entity, as defined in ISO/ IEC 24760-1 as "item relevant for the purpose of operation of a domain (3.2.3) that has recognizably distinct existence"[2], which is onboarded and has a Gaia-X Self-Description. A Participant can take on one or multiple of the following roles: Provider, Consumer, Federator. Provider and Consumer present the core roles that are in a business-to-business relationship while the Federator enables their interaction.

For each participant a technical account is derived, referred to as **Gaia-X User**. As an example, if a company becomes a Gaia-X Participant, there can be many employees of that company with individual accounts. Actions performed by a User are made on behalf of the Participant from which the User is derived.

A **Principal** is an individual (i.e., an employee) that is responsible or authorized to act on behalf of the organization (e.g., CIO, CEO, or authorized managers to act on behalf of the organization).

Gaia-X Provider (refer to [Gaia-X AD])

A Provider is a Participant who provides Assets and Resources in the Gaia-X Ecosystem. It defines the Service Offering including terms and conditions as well as technical Policies. Further, it provides the Service Instance that includes a Self-Description and technical Policies. Therefore, the Provider operates different Resources and possesses different Assets.

Gaia-X Consumer (refer to [Gaia-X AD])

A Consumer is a Participant who searches Service Offerings and consumes Service Instances in the Gaia-X Ecosystem to enable digital offerings for End-Users.

Gaia-X Federator (refer to [Gaia-X AD])

Federators are in charge of the Federation Services and the Federation which are autonomous of each other. Federators are Gaia-X Participants. There can be one or more Federators per type of Federation Service.

A Federation refers to a loose set of interacting actors that directly or indirectly consume, produce, or provide Assets and related Resources.

Gaia-X Assets (refer to [Gaia-X AD])

An Asset is an element which does not expose an Endpoint and is used to compose the Service Offering. An Endpoint is defined according to ISO ISO/TR 24097-3:2019(en) as a combination of a binding a network

[2] ISO / IEC. IT Security and Privacy – A framework for identity management: Part 1: Terminology and concepts (24760-1:2019(en)). ISO / IEC. https://www.iso.org/obp/ui/#iso:std:iso-iec:24760:-1:ed-2:v1:en

address.[3] An Asset can be a Data Asset, a Software Asset, a Node, or an Interconnection Asset. A set of Policies is tied to each Asset.

Gaia-X Node

A Node is an Asset and represents a computational or physical entity that hosts, manipulates, or interacts with other computational or physical entities (refer to [Gaia-X AD]).

A Node is one the fundamental concept of connecting real-world things to the Gaia-X world: A Node is enabled by one or more Gaia-X Providers to interact with other Gaia-X Software Assets and Nodes. The generic term *'Node'* emphasizes the open and broad nature of Gaia-X. The scope of what a Node can represent can range from datacenters, edge computing, basic hardware, network, and infrastructure operation services to more sophisticated, but still generic infrastructure building blocks like virtual machines or containers. Nodes are generic in the sense that different Software Assets can be deployed on them. Nodes expose functional and non-functional attributes via their Self-Description, allowing Node Consumers to select them based on their requirements. One prominent attribute is the Node's geolocation. Hierarchies of Nodes are supported by Gaia-X, so Nodes can contain further Nodes as children. An example for this is a Node representing a pan-European Node Provider that is structured into country regions, which are themselves structured into data center locations, racks, and individual servers, which themselves are exposed as Gaia-X Nodes.

Gaia-X Software Asset

A Software Asset is a form of Assets that consist of non-physical functions (refer to [Gaia-X AD]).

A Gaia-X Software Asset is a Gaia-X platform offering. Software Assets can be standalone or built in relation to other Gaia-X Software Assets by turning them into more complex service networks. The term Software Asset does not favor any of the common as-a-Service concepts like Infrastructure-as-a-Service, Platform-as-a-Service and so on. Software Assets are is offered by Gaia-X Providers and consumed by Gaia-X Consumer. It is the central way of interaction between Gaia-X platform actors. The Gaia-X platform facilitates establishing Provider-Consumer service relationships.

Every Software Asset has a Self-Description. This description enables the discovery of the Software Asset. It makes the Software Asset comparable to other (similar) Software Assets. A Consumer uses the Self-Description to match the offering to his requirements. A Gaia-X Software Asset can be built on other Gaia-X Software Assets.

[3] ISO/IEC. Intelligent transport systems – Using web services (machine-machine delivery) for ITS service delivery (ISO/TR 24097-3:2019(en)). https://www.iso.org/obp/ui/fr/#iso:std:iso:tr:24097:-3:ed-1:v1:en

Gaia-X Data Asset

A Data Asset is an Asset that consist of data in any form and necessary information for data sharing (refer to [Gaia-X AD]).

A Gaia-X Data Asset is a data set that is made available to Consumers via a Software Asset that exposes the Data Asset. Consumers and Providers can also host private data within Gaia-X that is not made available (and hence not a consumable Data Asset). Data Assets are exposed and provided by Gaia-X Software Assets, where they can be searched and consumed by another Gaia-X Software Asset or a Gaia-X Participant. From this, it follows that data being provided or consumed by a Gaia-X Software Asset is hosted on a Gaia-X Node.

As the capability of Self-Description is a major aspect of the Gaia-X Architecture, Data Assets provide a Self-Description as well. This mechanism enables exchange, sharing and brokerage of data between Gaia-X Software Assets, and between Gaia-X Software Assets and non-Gaia-X Software Assets.

Gaia-X Interconnection Asset

An Interconnection is an Asset that presents the connection between two or multiple Nodes [refer to annex Gaia-X AD]. Interconnections Assets are not part of this Specification.

1.2.2.2 Gaia-X Entities

AISBL

AISBL: Association international sans but lucratif. The AISBL is the central management entity of Gaia-X. The association's purpose and objective will be to consolidate and facilitate work and collaboration within the Gaia-X community. Gaia-X AISBL will be representing its members and promoting international cooperation. To this end, the association will develop regulatory frameworks, and ensure that necessary services are made available.

Gaia-X Onboarding Authority

An authority where the onboarding and administration of Gaia-X Providers and Assets is handled. In the first version of the Gaia-X ecosystem, the AISBL will act as the onboarding authority. The AISBL can decide to outsource onboarding activities to one or many third parties, referred to as conformity assessment bodies.

Gaia-X Conformity Assessment Body

Conformity assessment bodies (CABs) verify Providers and Assets regarding their fulfilment of Gaia-X controls during accreditation. CABs may refer to existing certification authorities, monitoring bodies, auditors, or novel Gaia-X-specific assessment bodies. To perform assessments, CABs have to fulfill Gaia-X requirements for CABs that will be defined in future Gaia-X versions.

1.2.2.3 Onboarding and Accreditation Terms

Onboarding of Gaia-X Providers and Assets

Onboarding refers to the process of registering Gaia-X Providers and Assets. The Gaia-X ecosystem will introduce an onboarding workflow that Providers can then use to request accreditation for themselves or their assets.

Accreditation of Gaia-X Providers and Assets

Accreditation refers to the process of assessing and verifying Gaia-X Providers and Assets. Each Asset offered by a Provider has to be compliant with the mandatory controls [PRD] as stipulated by the Gaia-X ecosystem.

Self-Description

A Self-Description provides basic information on a Provider or Asset in a transparent manner to communicate a Provider's or Asset's characteristics.

Gaia-X Terms and Conditions

Gaia-X terms and conditions will be specified later in the Gaia-X development process and require, for example, the Provider to sign-up a Software Asset or Node in due time after the Provider onboarding is completed.

Gaia-X Minimal Viable Set of Controls

The policy rules committee (and approved by the Board of Directors of the Gaia-X AISBL) defines a minimal viable set of controls (MVSC) that an Asset (mostly referring to Software Assets and Nodes) has to fulfill to be compliant with the Gaia-X principles.[4] Each Asset needs to adhere to specific controls (i.e., regarding data privacy / data protection or IT-/ cybersecurity).

[4] Please note: the current version of the policy rules document was not published at the time of writing this specification.

Declaration of Adherence

The Declaration of Adherence has to be signed by the Provider during the onboarding process for specific Assets. By signing the Declaration of Adherence, the Providers confirm that the Self-Description is complete and accurate, and that the fulfillment of the MVSC set out by Gaia-X policy rules [PRD] and the Gaia-X principles have been demonstrated at least in internal testing for the Asset in question.

Accreditation Agreement

A legally enforceable agreement between the Provider and the Onboarding Authority (and/ or CABs performing the accreditation) for the provision of accreditation activities. Accreditation agreements comprise the responsibilities of the Onboarding Authority (and/ or CABs performing the accreditation) and the Provider, among others.

Assurance Levels

To ensure that all Nodes and Software Assets participating in the Gaia-X ecosystem exhibit appropriate qualities, for example, regarding IT security, data protection, and performance, Gaia-X introduces three levels of assurance for Software Assets and Nodes: basic, substantial, and high (refer to Section 5.5.1).

Decentralized Identifier (DID)

Decentralized identifiers (DIDs) are a new type of identifier that enables verifiable, decentralized digital identity.[5] A DID identifies any subject (e.g., a person, organization, thing, data model, abstract entity, etc.) that the controller of the DID decides that it identifies. In contrast to typical, federated identifiers, DIDs have been designed so that they may be decoupled from centralized registries, identity providers, and certificate authorities. Specifically, while other parties might be used to help enable the discovery of information related to a DID, the design enables the controller of a DID to prove control over it without requiring permission from any other party. DIDs are URIs that associate a DID subject with a DID document allowing trustable interactions associated with that subject. A DID can be generated by a DID as a service provider.

1.3 Intended Audience and Reading Suggestions

This document is intended for managers, developers, testers, and further stakeholders that should implement the OAW engine to be integrated into the Gaia-X ecosystem. Understanding this document requires a thorough understanding of the Gaia-X ecosystem, its principles and core mechanisms. It does not require specific programming skills or domain knowledge. A basic understanding in conformity assessment methods (e.g., auditing, certification etc.) is recommended.

[5] The description of DIDs are taken from https://www.w3.org/TR/did-core/

Given high interdependencies of the OAW engine with other Gaia-X Federated Services (i.e., Identity Management, Federated Catalogue, Compliance Documentation Service, and Portal), this document is also intended to further developers and project managers, who develop, manage, or operate related Federated Services.

This document is structured as follows. First, an overall outline and description of the OAW engine is provided in Section 2. Second, Section 3 describes interface requirements. Section 4 summarizes the workflow steps to be implemented. Section 5 outlines non-functional requirements. To fully understand the OAW it is important that each reader grasps the whole document.

1.4 Product Scope

This document specifies an OAW engine that MUST be implemented to onboard and accredit Providers and their Assets, particularly Software Assets and Nodes. Onboarding and accrediting Data Assets are out-of-scope for this document and will be handled by Gaia-X Data Contract Service, developed by WP3[6] and their specifications. Please note, the OAW engine does not comprise onboarding or accreditation workflows for Consumers at the moment because no compliance verification is needed for these Participants. Likewise, this document does not specify OAW for Interconnection Assets, which may be added in later versions. Thus, the OAW engine SHOULD NOT be developed for Consumers but SHOULD be extendible to consider Interconnection Assets in the future.

The OAW engine's objective is to foster secure and reliable participation in the Gaia-X ecosystem and to achieve transparency for both Consumers and Providers. While the OAW engine should support the Onboarding Authority and their CABs to perform the accreditation workflows, most work will be manually done by them.

1.5 References

[ENISA 2020]	ENISA (2020): EUCS–Cloud Services Scheme. EUCS, a candidate cybersecurity certification scheme for cloud services. As of December 2020. Retrieved March 2021 from *https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme/*
[Gaia-X AD]	Gaia-X, European Association for Data and Cloud, AISBL (2021): Gaia-X Architecture Document. As of March 2021. Refer to annex "Gaia-X_Architecture_Document_2103"
[NF.SPBD]	Gaia-X Federation Service Non-functional Requirements Security & Privacy by Design. Please refer to annex "GXFS_Nonfunctional_Requirements_SPBD"
[NOTAR]	Specifications for Gaia-X Federation Services Compliance – Notarization API. Please refer to annex "SRS_GXFS_CP_NOTAR"

[6] Please refer to appendix B for an overview and explanation of the Work Packages (WP).

[PRD]	Gaia-X, European Association for Data and Cloud, AISBL (2021): Gaia-X Policy Rules Document. As of March 2021. Please refer to annex "Gaia-X_Policy Rules_Document_2104"
[RFC 2119]	Network Working Group (1997): Key words for use in RFCs to Indicate Requirement Levels. Retrieved March 2021 from https://tools.ietf.org/html/rfc2119
[TDR]	Gaia-X Federation Services Technical Development Requirements. Please refer to annex "GXFS_Technical_Development_Requirements"
[WFE]	Specifications for Gaia-X Federation Service Integration & Portal – Workflow Engine / Business Process Management. Please refer to annex "RFP_GXFS_IP_WFE"

***Table 1**: References*

2. Overall Description

Next to the requirements stated in this document, the requirements regarding the Technical Environment/ Development [TDR] must be also met.

2.1 Product Perspective

The OAW engine is a core service within the Gaia-X Federation Services. Its main goal is to provide transparency to Consumers about the compliance of individual Software Assets and Nodes offered in the Gaia-X Federated Catalogue. The OAW engine offers diverse functions to enable onboarding and accreditation of Providers and Assets. The OAW engine is part of the workflow engine that is specified in WP5[7], and hence, functional and non-functional requirements described in their respective Specification document should be considered when developing the OAW engine [WFE].

The OAW engine is in particular used to perform accreditation of Software Assets and Nodes to prove their compliance by the Onboarding Authority, namely the AISBL, or CABs authorized by the AISBL.[8] The OAW engine uses the Notary Services to generate verifiable credentials once the accreditation process is accomplished [NOTAR].

2.2 Product Functions

The OAW engine MUST offer six major functions, relating to the onboarding and accreditation workflows as well as related management processes. The building blocks of the OAW engine will be briefly outlined in the following.

[7] Please refer to appendix B for an overview and explanation of the Work Packages (WP).

[8] Please note, this document refers mainly to workflow activities performed by the Onboarding Authority. Each of the activity may be outsourced and performed by a CAB. To enhance readability of this document, it is referred to the Onboarding Authority solely.

2.2.1 GX OAW Provider Onboarding Workflow (GX-OAW-PO)

Before offering Assets on Gaia-X, the Provider has to register at Gaia-X. This registration is done through the provider onboarding workflow. During the onboarding, the Provider has to generate relevant onboarding data (e.g., the Provider's Self-Description) and sign the terms and conditions and accreditation agreement. Afterwards, the Provider can submit its onboarding request to the Onboarding Authority, which will then start the accreditation workflow.

2.2.2 GX OAW Provider Accreditation Workflow (GX-OAW-PA)

During the provider accreditation workflow, the Gaia-X Onboarding Authority will, with the support of CABs, verify Provider's onboarding information for completeness, integrity, and honesty. If the Onboarding Authority approves the onboarding, a respective verifiable credential is created using the Notary Service (e.g., Gaia-X membership credentials).

2.2.3 GX OAW Software Asset and Node Onboarding Workflow (GX-OAW-SNO)

Similar to onboarding Providers, each new Software Asset or Node (or each Software Asset and Node family) has to undergo an onboarding process before being listed in the Gaia-X ecosystem. The goal is to design an onboarding approach assuring that each Asset fulfills the Gaia-X principles and MVSC. Therefore, a Provider has to submit a Self-Description for the Asset; sign the Declaration of Adherence to confirm that fulfillment of the MVSC considering the determined Assurance Levels has been demonstrated at least in internal testing for the Asset in question; and, most importantly, submit assurance information that proves adherence (e.g., documentation about self-assessment, existing certifications for the Software Asset like ISO/IEC 27001), which will be assessed during the accreditation performed by the Onboarding Authority.

2.2.4 GX OAW Software Asset and Node Accreditation Workflow (GX-OAW-SNA)

Gaia-X will comprise three different Assurance Levels for Software Assets and Nodes (i.e., basic, substantial, and high) to ensure that Gaia-X controls will be met in regard to the specific characteristics of each Software Asset and Node (e.g., processing personal data necessitates compliance with the GDPR). Depending on the claimed Assurance Level, an accreditation workflow will verify whether a Software Asset or Node is in compliance with the Gaia-X MVSC. At the Basic Assurance Level, the accreditation is greatly simplified, and it relies solely on self-assessment evidence provided by the Provider, if needed upon explicit request from the Onboarding Authority. The verification of Substantial Gaia-X Nodes and Software Assets builds on the Basic verification process but differs in the verification scope and efforts. In particular, self-assessments are not sufficient for the Substantial Assurance Level. Instead, Gaia-X will refer to existing standards, certifications, attestations, code of conduct, audit results, etc. that are appropriate to fulfil the MVSC for the Substantial Assurance Level. The verification of High Gaia-X Nodes and Software Assets builds on the Substantial verification process but differs in the verification scope and efforts. Besides the Substantial Level controls there will be additional controls that a Software Asset / Node has to fulfill, for example, in the case of cybersecurity. In addition, further verification processes and measurements are applied. In particular, Continuous Automated Monitoring may be applied to verify ongoing compliance with selected controls.

2.2.5 GX OAW Management Workflows (GX-OAW-MW)

Besides the core workflows of onboarding and accreditation, the OAW engine must comprise management workflows to enable an efficient and trustworthy operation of the Gaia-X ecosystem, such as surveillance and re-assessment workflows to ensure ongoing compliance of Software Assets and Nodes with the MVSC; management workflows to handle compliance-relevant events (e.g., need for revocation or restriction of Gaia-X compliance attestations); and acknowledgement workflows for existing assurance mechanisms; among others.

2.2.6 GX OAW Offboarding Workflow (GX-OAW-OFF)

In case a Provider, Software Asset or Node should be withdrawn from the Gaia-X ecosystem due to a Provider's request or Asset's violation of the MVSC, the OAW engine must support offboarding workflows.

2.3 User Classes and Characteristics

The following users may rely on or interact with the OAW engine:

1) Gaia-X Providers to submit onboarding information and a corresponding onboarding request for themselves or their Assets.
2) The Onboarding Authority that is in charge of managing the onboarding and accreditation workflows. In the first version of Gaia-X, the AISBL will act as the onboarding authority. The AISBL can decide to outsource onboarding activities to one or many third parties, mainly CABs. The Onboarding Authority may deploy and operate the OAW engine itself or outsource this federated service.
3) CABs that are authorized by the AISBL to perform the accreditation. The CAB may deploy and operate the OAW engine itself or outsource this federated service.
4) System administrators that operate and maintain the OAW engine. System administrators may be employees of the Onboarding Authority, CABs, or any third party that provides the OAW engine as a service.

2.4 Operating Environment

This document does not specify any specific hardware or operating system requirements. Please refer to the Technical Development Requirements in [TDR].

2.5 Design and Implementation Constraints

The OAW engine is part of the WP5[9] workflow engine and therefore MUST consider design and implementation constraints specified for the general workflow engine [WFE].

[9] Please refer to appendix B for an overview and explanation of the Work Packages (WP).

2.6 User Documentation

The following documentation MUST be provided:

- User manual about onboarding workflows for Providers, the Onboarding Authority, and CABs
- User manual about accreditation workflows for Providers, the Onboarding Authority, and CABs
- User manual about management workflows for the Onboarding Authority, and CABs
- User manual about offboarding workflows for Providers, the Onboarding Authority, and CABs
- Tutorials for onboarding of Providers and Assets
- Training materials to use the OAW engine for the Onboarding Authority and CABs
- Brochures about the general functionality of the OAW engine for the general public

The documentation MUST follow best practices in the software engineering field, such as keeping language simple, using plain English, explaining technical terms and jargon if they must be used, and making sure that individual needs are catered.

Further requirements regarding the documentation can be found in [TDR].

3. External Interface Requirements

3.1 User Interfaces

The OAW engine SHOULD offer a GUI for its users. Basically, three different GUIs are recommended: onboarding GUI, accreditation GUI, and management GUI.

3.1.1 Onboarding GUI

The onboarding GUI should offer functionalities to foster the onboarding of Providers and their Assets.

ID	Description	Acceptance Criteria	Priority
OGUI-F-01	The onboarding GUI SHOULD present users with information about the workflow activities (e.g., what kind of activities are needed, what type of data is required as input for each activity, who is responsible for each activity, etc.).	documentation; test cases	SHOULD
OGUI-F-02	The onboarding GUI SHOULD offer users means to enter and/or upload onboarding information, including the self-description, assurance information for Assets, and signed terms and conditions, declaration of adherence, and agreement of accreditation.	documentation; test cases	SHOULD
OGUI-F-03	The onboarding GUI SHOULD offer users functions to contact the Onboarding Authority and /	documentation; test cases	SHOULD

	or CABs in charge of performing the accreditation.		
OGUI-F-04	The onboarding GUI SHOULD present users with information about open, pending, or approved / rejected onboarding requests, such as status of each onboarding request, submitted information, users who process the onboarding request.	documentation; test cases	SHOULD
OGUI-F-05	The onboarding GUI SHOULD offer user functions to alter or withdraw an onboarding request.	documentation; test cases	SHOULD

***Table 2**: Functional Requirements of the onboarding GUI*

3.1.2 Accreditation GUI

The accreditation GUI should offer functionalities to foster the accreditation of Providers and their Assets.

ID	Description	Acceptance Criteria	Priority
AGUI-F-01	The accreditation GUI SHOULD present users with information about the accreditation activities (e.g., what kind of activities are needed, what type of data is required as input for each activity, who is responsible for each activity, etc.).	documentation; test cases	SHOULD
AGUI-F-02	The accreditation GUI SHOULD offer users means to view pending, under review, approved / rejected onboarding requests, and available information about each onboarding request.	documentation; test cases	SHOULD
AGUI-F-03	The accreditation GUI SHOULD offer users functions to contact the Provider who has submitted an onboarding request.	documentation; test cases	SHOULD
AGUI-F-04	The accreditation GUI SHOULD enable users to inspect, download, export, or directly alter onboarding information that was submitted by a Provider.	documentation; test cases	SHOULD
AGUI-F-05	The accreditation GUI SHOULD offer users functions to document (intermediate) verification results for each accreditation activity (e.g., self-description verified, assurance information verified with result X).	documentation; test cases	SHOULD

AGUI-F-06	The accreditation GUI SHOULD offer user functions to use the Notary Service to generate verifiable credentials.	documentation; test cases	SHOULD

***Table 3**: Functional Requirements of the accreditation GUI*

3.1.3 Management GUI

The management GUI should offer functionalities to foster the management of onboarding and accreditation.

ID	Description	Acceptance Criteria	Priority
MGUI-F-01	The management GUI SHOULD offer functionalities to support the management workflows described below.	documentation; test cases	SHOULD
MGUI-F-02	The management GUI SHOULD enable the communication between Providers and the Onboarding Authority or CABs that perform the accreditation (e.g., implementing a GUI for a messaging system).	documentation; test cases	SHOULD
MGUI-F-03	The management GUI SHOULD enable functionalities to support the Onboarding Authority in acknowledging further assurance mechanisms for the Substantial and High Assurance Levels, such as a form to enter data about assurance mechanisms, submit these data, and an overview for the Onboarding Authority to view all requests.	documentation; test cases	SHOULD

***Table 4**: Functional Requirements of the management GUI*

3.2 Hardware Interfaces

Not applicable.

3.3 – 3.4 Software and Communication Interfaces

Data Items

Provider Onboarding Data

To perform the onboarding, data is required about the Provider. **Table 5**5 summarizes minimum data about Providers that MUST be collected and / or generated to perform the onboarding workflows. Further data may become necessary to collect or generate during the development phase. The OAW engine MUST be capable to process and store the data.

Property	Type	Special Remarks
Onboarding Request ID	Int	Unique ID to identify each request
Organization Identifier (e.g., DID)	Various	
Approval about Principal's authorization to act on behalf of the organization	Verifiable Credential, Document (e.g., pdf), other	
Provider Self-Description	JSON-LD	Please note, WP2[10] defines the format and content of self-descriptions.
Optional Assurance Information	Documents (e.g., pdf)	Any further assurance information that may be appended to the onboarding request.
Signed terms and conditions	Document (e.g., pdf), eventually with digital signature	
Signed accreditation agreement	Document (e.g., pdf), eventually with digital signature	
Request Status	Collection {submitted, under review, clarification needed, approved, rejected}	"Clarification needed" refers to a status, where the accreditation process is paused because the Onboarding Authority requires further information from the Provider and has contacted her.
Date of Submission	Timestamp & Date	Information about when the onboarding information was submitted.
Accountable user	User account ID	Information about who submitted the information.

***Table 5**: Minimum data about Providers required for onboarding workflows*

Software Asset and Node Onboarding Data

To perform the onboarding, data is required about the Software Asset or Node. **Table 6**6 summarizes minimum data about Software Assets and Nodes that MUST be collected and / or generated to perform the

[10] Please refer to appendix B for an overview and explanation of the Work Packages (WP).

onboarding workflows. Further data may become necessary to collect or generate during the development phase. The OAW engine MUST be capable to process and store the data.

Property	Type	Special Remarks
Onboarding Request ID	Int	Unique ID to identify each request
Organization Identifier (e.g., DID)	Various	
Approval about Principal's authorization to act on behalf of the organization	Verifiable Credential, Document (e.g., pdf), various	
Asset Self-Description	JSON-LD	Please note, WP2[11] defines the format and content of self-descriptions.
Asset Documentation	Documents, various	If needed, additional asset documentation, including asset boundaries, scope, sub services etc.
Assurance Level for each MVSC category	List of Pairs {Collection {Basic, Substantial, High}; MVSC category}	The Assurance Level that a Provider claims for its Asset in question for each MVSC category (i.e., cybersecurity, data protection, transparency, etc.). Refer to Section 5.5.1.
Flag referring to 'meta-asset'	Asset ID	A pointer to another Asset ID to which this asset belongs to.
Signed declaration of adherence	Document (e.g., pdf), eventually with digital signature	
Signed accreditation agreement	Document (e.g., pdf), eventually with digital signature	
Statement about how the Asset fulfills the MVSC	Documents (e.g., pdf), various	
Assurance Information	Documents (e.g., pdf), various	Any assurance information that may be appended to the onboarding request to prove

[11] Please refer to appendix B for an overview and explanation of the Work Packages (WP).

		compliance with the MVSC (e.g., self-assessment results, existing certifications).
Optional Information	Documents (e.g., pdf), various	Any further information that may be appended to the onboarding request, such as standardized SLAs.
Request Status	Collection {submitted, under review, clarification needed, approved, rejected}	"Clarification needed" refers to a status, where the onboarding process is paused because the Onboarding Authority requires further information from the Provider and has contacted her.
Date of Submission	Timestamp & Date	Information about when the onboarding information was submitted.
Accountable user	User account ID	Information about who submitted the information.

***Table 6**: Minimum data about Software Assets and Nodes required for onboarding workflows*

Accreditation Data

During accreditation, further data may be generated and stored by the Onboarding Authority or CABs. **Table 7**7 summarizes minimum data related to the accreditation workflow that MUST be collected and / or generated to perform the accreditation workflows. Further data may become necessary to collect or generate during the development phase. The OAW engine MUST be capable to process and store the data.

Property	**Type**	**Special Remarks**
Accountable users	User IDs	Assigning users who are accountable for performing the accreditation.
Accreditation Status	Collection {received, under review, clarification needed, approved, rejected}	"Clarification needed" refers to a status, where the accreditation process is on hold because the Onboarding Authority requires further information from the Provider and has contacted her.
Signed accreditation agreement	Document (e.g., pdf), eventually with digital signature	The Onboarding Authority and/or CAB performing the accreditation has to sign the accreditation agreement as well.

Accreditation plan	Various	The Onboarding Authority and/or CAB may store its accreditation plan.
Accreditation report	Document (e.g., pdf), eventually with digital signature	
Accreditation decision	Collection {approved, rejected}	
OAW engine interaction log	Function identifier, timestamp, date	Information about when an OWA engine function was used, what function was used, and by whom the function was used.

***Table 7**: Minimum data relevant for accreditation workflows*

Verifiable Credentials

If the onboarding of a Provider or an Asset is successful, the Onboarding Authority generates a verifiable credential by using the Notary Service that proves Gaia-X compliance. The verifiable credentials should comprise at least the information summarized in **Table 8**8 for Providers and **Table 9**9 for Software Assets and Nodes.

Property	**Type**	**Special Remarks**
Unique ID	Integer, various	Unique ID for the credential.
Organization Identifier (e.g., DID)	Various	
Provider name	String	
Date of issuance	Date	Date when the accreditation was approved.
Validity period	Date	A date until which the accreditation is valid, as specified by the Onboarding Authority.
Status	Collection {valid; suspended; revoked}	The status of the approval
Accountable Onboarding Authority and / or CAB	Name, or pointer to ID	Reference to the stakeholder that performed the accreditation and decided about the approval.
Optional information	String	Any optional comments, information etc. that should be published along the credential.

***Table 8**: Content of the verifiable credential for Providers*

Property	Type	Special Remarks
Unique ID	Integer, various	Unique ID for the credential.
Organization Identifier (e.g., DID)	Various	
Asset description (e.g., name)	String	In line with the self-description.
Fulfilled Assurance Level for each category of the MVSC	List of Pairs {Collection {Basic, Substantial, High}; MVSC category}	The Software Asset or Node fulfills an Assurance Level for each category of controls listed in the MVSC (e.g., data protection, cybersecurity, transparency, interoperability).
Recognized Certificates	List of certifications	A list of Software Asset or Node certification that were recognized during the accreditation (e.g., C5 attestation, CSA STAR etc.).
Date of issuance	Date	Date when the accreditation was approved.
Validity period	Date	A date until which the accreditation is valid, as specified by the Onboarding Authority.
Status	Collection {valid; suspended; revoked}	The status of the approval
Accountable Onboarding Authority and / or CAB	Name, or pointer to ID	Reference to the stakeholder that performed the accreditation and decided about the approval.
Surveillance information	String	Information when and how often compliance surveillance is performed.
Optional information	String	Any optional comments, information etc. that should be published along the credential.

***Table 9**: Content of the verifiable credential for Software Assets and Nodes*

In the upcoming releases of Gaia-X, the Onboarding Authority may decide to outsource certain accreditation activities to CABs after they have been formally approved. As a result of the CAP approval workflow, a verifiable credential for CAB should be issued, with the data summarized in **Table 10**10.

Property	Type	Special Remarks
Unique ID	Integer, various	Unique ID for the credential.
Organization Identifier (e.g., DID) of the CAB	Various	
CAB name	String	
Date of issuance	Date	Date when the CAB was approved.
Validity period	Date	A date until which the approval of CABs is valid, as specified by the Onboarding Authority.
Status	Collection {valid; suspended; revoked}	The status of the approval
Accountable Onboarding Authority	Name, or pointer to ID	Reference to the stakeholder that performed the assessment and decided about the approval.
Surveillance information	String	Information when and how often surveillance of the CAB is performed.
Optional information	String	Any optional comments, information etc. that should be published along the credential.

***Table 10**: Content of the verifiable credential for CABs*

Communication & Interfaces

The OAW engine MUST implement an interface to receive or export the data outlined above.

Since the OAW engine may be hosted internally or as an external Federated Service, each of the functions described for the modules:

- GX OAW Provider Onboarding Workflow
- GX OAW Provider Accreditation Workflow
- GX OAW Software Asset and Node Onboarding Workflow
- GX OAW Software Asset and Node Accreditation Workflow
- GX OAW Management Workflows
- GX OAW Offboarding Workflow

SHOULD be accessible via a secure and protected communication interface.

The OAW engine MUST communicate with the Notary Service to generate verifiable credentials.

The OAW engine is part of the workflow engine of WP5[12] and therefore MUST offer communication interfaces specified in its specification document [WFE].

4. System Features

4.1 GX OAW Provider Onboarding Workflow (GX-OAW-PO)

4.1.1 Description and Priority

The OAW Provider Onboarding Workflow manages the gathering of relevant information needed for the accreditation, such as the Self-Description, signed Terms and Conditions, and further relevant assurance information. The Provider Onboarding Workflow is of high relevance and MUST be implemented.

4.1.2 Stimulus/Response Sequences

Preconditions (out of scope for OAW engine):

1. **Provider Identification.** Providers have to successfully identify themselves, such as providing the organization's DID first. If the organization has no DID, it may get one from a DID service provider that is acknowledged by Gaia-X (e.g., German Bundesdruckerei). Supposedly, the Gaia-X Portal will list acknowledged DID service providers. Gaia-X identity management may verify that the DID exist. Alternative mechanisms of proving Provider's identity are possible.
2. **Principal Selection.** Providers have to define Principals (i.e., representatives that are authorized to act on behalf of the organization) that will be able to perform the onboarding process (e.g., fill in the self-description, provide required onboarding information, and sign terms and conditions). Each Provider has to define by herself, which Principal(s) will be capable of performing the onboarding process (e.g., the CEO, secretary, product owners etc.). During the accreditation workflow it must be verified by Gaia-X that the Principal is in a role acting on behalf of the organization (refer to *PA-F-01*). In the future, Gaia-X will request verifiable credentials about the Principal from the organization. Such verifiable credentials have to be issued by a trusted issuer (e.g., GLEIF, GS1, local commercial registries, certifying notaries) that performs appropriate verification processes of the Principal (e.g., verify ID card and related documents). Gaia-X may determine a set of trustworthy issuers based on a selection process, which will be defined in the future.

Workflow Interaction Sequence:

- The Provider provides required data to the OAW engine.
- The Provider changes or deletes submitted data.
- The Provider completes the onboarding workflow by submitting an onboarding request.

[12] Please refer to appendix B for an overview and explanation of the Work Packages (WP).

- Once completed, the OAW engine submits all information for accreditation to the Onboarding Authority.

4.1.3 Functional Requirements

The OAW engine comprises the following workflow features to enable the Provider onboarding:

ID	Description	Acceptance Criteria	Priority
PO-F-01	The OAW engine MUST be able to receive a Provider's Self-Description.	documentation; test cases	MUST
	Explanation An important basis for the onboarding process is the Provider Self-Description to communicate Provider's characteristics in a transparent manner. This Self-Description must be filled by the Provider according to Gaia-X guidelines, defined by WP2[13]. The Gaia-X Portal or onboarding GUI may also provide a tool to enter and upload the Self-Description as well as functionalities to ensure syntactical correctness as well as the possibility to perform automated checks on the information entered in the Self-Description.		
PO-F-02	The OAW engine MUST be able to receive information about a Principal's authorization to act on behalf of the organization.	documentation; test cases	MUST
	Explanation In line with the precondition *'Principal Selection'*, the OAW engine must receive any kind of information to enable verification during the accreditation that the Principal is authorized. This information may be in the form of verifiable credentials or an official approval document that contains the Principal's digital signature, a statement that he/she is authorized to perform the onboarding on behalf of the organization, an identification of the organization (e.g., organization's DID), and, most importantly, a digital signature of the organization's leader (e.g., members of the board), among others.		
PO-F-03	The OAW engine MUST be able to receive the signed terms and conditions.	documentation; test cases	MUST
	Explanation The Provider must sign the Gaia-X terms and conditions. These will be specified later in the Gaia-X development process and require, for example, the Provider to sign-up an Asset in due time after the Provider onboarding is completed.		

[13] Please refer to appendix B for an overview and explanation of the Work Packages (WP).

PO-F-04	The OAW engine MUST be able to receive the signed accreditation agreement.	documentation; test cases	MUST
	Explanation The Provider must sign the accreditation agreement. The accreditation agreement is a legally enforceable agreement between the Provider and the Onboarding Authority (and/ or CABs performing the accreditation) for the provision of accreditation activities. Accreditation agreements comprise the responsibilities of the Onboarding Authority (and/ or CABs performing the accreditation) and the Provider, among others. The content of the agreement will be specified later in the Gaia-X development process.		
PO-F-05	The OAW engine SHOULD be able to receive further information (e.g., documents).	documentation; test cases	SHOULD
	Explanation Supposedly, the Provider may submit further assurance information that relates to the Provider organization and is independent of specific Assets (e.g., ISO 9001 QMS certification for the provider organization). The upcoming Gaia-X onboarding workflows should consider the additional upload for assurance information in case the AISBL decides that certain assurance evidence is mandatory.		
PO-F-06	The OAW engine MUST be able to submit all gathered onboarding information as request for onboarding to the Onboarding Authority.	documentation; test cases	MUST
	Explanation Finally, the Provider submits all information as onboarding request to the Gaia-X Onboarding Authority, which will then initiate accreditation workflows.		
PO-F-07	The OAW engine MUST log each workflow activity (i.e., generate an audit trail) to enable third party auditing, including input data, data about processing activities, output data (e.g., results), corresponding timestamps and accountable users.	documentation; test cases	MUST
	Explanation To support the documentation activities of the Onboarding Authority and ensure an audit trail, the OAW engine should log workflow activities in an immutable and confidential manner to ensure its auditability.		
PO-F-08	The OAW engine MUST provide the means to change, export, and delete onboarding data.	documentation; test cases	MUST
	Explanation		

	It must be possible to change or delete the data gathered through onboarding by the Provider and CAB/Onboarding Authority.

***Table 11**: Functional Requirements of the Provider Onboarding Workflow (GX-OAW-PO)*

4.2 GX OAW Provider Accreditation Workflow (GX-OAW-PA)

4.2.1 Description and Priority

The Gaia-X Onboarding Authority will, with the support of CABs, verify onboarding information for completeness, integrity, and honesty. The Provider Accreditation Workflow is of high relevance and MUST be implemented.

4.2.2 Stimulus/Response Sequences

Precondition:

1. **Request received.** Onboarding Authority received the onboarding request from a Provider.

Workflow Interaction Sequence:

- The Onboarding authority and / or CAB accesses onboarding data.
- The Onboarding authority and / or CAB stores (intermediate) accreditation data.
- The Onboarding authority and / or CAB accesses, changes, or deletes (intermediate) accreditation data.
- The Provider provides additional data that is then stored and accessible for the Onboarding Authority.
- The Onboarding authority and / or CAB completes the accreditation workflow by specifying the final decision (i.e., approved or rejected).
- Once completed, the OAW engine submits all information to the Notary Service to generate a verifiable credential.

4.2.3 Functional Requirements

The OAW engine comprises the following workflow features to enable accreditation activities:

ID	Description	Acceptance Criteria	Priority
PA-F-01	The OAW engine MUST provide the information on Principal's authorization. It SHOULD automatically validate verifiable credentials of a Principal if available. It MAY accept eIDAS service as an acceptable source of provider's identity with verifiable credentials.	documentation; test cases	MUST
	Explanation First, the Onboarding Authority will verify whether a Principal is authorized to perform the onboarding process on behalf of the organization. In the future, Gaia-X will request verifiable		

	credentials about the Principal from the organization. Such verifiable credentials have to be issued by a trusted issuer (e.g., GLEIF, GS1, local commercial registries, certifying notaries) that performs appropriate verification processes of the Principal (e.g., verify ID card and related documents). However, currently there are no trustworthy issuer nor related mechanisms that enable automatic validation whether a Principal is authorized to perform the Gaia-X onboarding. As interim solution, Gaia-X therefore requires the Principals to submit an official approval document that contains his/her digital signature, a statement that he/she is authorized to perform the onboarding on behalf of the organization, the identification of the organization (e.g., organization's DID), and, most importantly, a digital signature of the organization's leader (e.g., members of the board), among others. This document will be verified by the Onboarding Authority to ensure that the Principal was authorized to perform the onboarding. If the Onboarding Authority has any doubts regarding the approval's integrity and/or honesty, the Onboarding Authority will inform the Provider, and request evidence that the information is truthful or corrections of the information in question.		
PA-F-02	The OAW engine MUST provide the signed terms and conditions. The OAW engine SHOULD automatically validate the signatures' authenticity.	documentation; test cases	MUST
	Explanation Second, the Onboarding Authority verifies that the Provider has signed the Gaia-X terms and conditions during onboarding.		
PA-F-03	The OAW engine MUST be able to receive the signed accreditation agreement. The OAW engine MUST be able to store the accreditation agreements once signed by the Onboarding Authority (and/or CABs) as well.	documentation; test cases	MUST
	Explanation The Provider and the Onboarding Authority (and/or CABs) MUST sign the accreditation agreement. The accreditation agreement is a legally enforceable agreement between the Provider and the Onboarding Authority (and/ or CABs performing the accreditation) for the provision of accreditation activities. Accreditation agreements comprise the responsibilities of the Onboarding Authority (and/ or CABs performing the accreditation) and the Provider, among others. The content of the agreement will be specified later in the Gaia-X development process.		
PA-F-04	The OAW engine MUST provide the Self-Description. The OAW engine SHOULD incorporate features to support the Onboarding Authority performing verification of the Self-Description. For example, the OAW engine SHOULD automatically	documentation; test cases	MUST

	verify attributes of the Self-Description (e.g., whether an attribute is given, adheres to a given policy etc.).		
	Explanation The Onboarding Authority will review the Self-Description. During this review, the Onboarding Authority will verify that all mandatory fields of the Self-Descriptions are completed (i.e., ensuring completeness). The Onboarding Authority will then check whether the information entered in the Self-Description is truthful by performing spot checks on random or conspicuous information (i.e., ensuring integrity and honesty). For example, the Onboarding Authority may match information from the Self-Description with public available information (e.g., on the website of the Provider). If the Onboarding Authority has any doubts regarding the information's integrity and/or honesty, the Authority will inform the Participant, and request evidence that the information is truthful or corrections of the information in question. The review of the Self-Description should be automated to the highest extent possible. For example, scripts may be implemented that check whether the provided commercial registry number is authentic by automatically querying public databases.		
PA-F-05	The OAW engine MUST provide additional assurance information that may be contained in the onboarding request.	documentation; test cases	MUST
	Explanation Supposedly, the Provider may submit further assurance information that relates to the Provider's organization and is independent of specific Assets (e.g., ISO 9001 QMS certification for the Provider organization). The upcoming Gaia-X OAW engine should consider the additional upload for assurance information in case the AISBL decides that certain assurance evidence is mandatory. Depending on the type of assurance information required, verification processes need to be specified in the future.		
PA-F-06	The OAW engine MUST be able to receive and store the final decision of the Onboarding Authority.	documentation; test cases	MUST
	Explanation After verification, the Gaia-X Onboarding Authority approves or rejects the Provider onboarding. In case of rejection, the Gaia-X Provider will be informed about the reasons for rejection and allowed to adjust the registration and related information.		
PA-F-07	The OAW engine MUST create a verifiable credential using the Notary Service if onboarding is approved.	documentation; test cases	MUST
	Explanation		

	If the Onboarding Authority approves the onboarding, a respective verifiable credential is created using the Notary Service (e.g., Gaia-X Membership credentials). The verifiable credential is then sent to the Provider.		
PA-F-08	The OAW engine MUST be able to send data to other stakeholders and services.	documentation; test cases	MUST
	Explanation Eventually, the Participant's Self-Description will be added to the Gaia-X Federated Catalogue. The OAW engine therefore must be able to send the verified Self-Description to a Catalogue. Similar, the OAW engine must send the verifiable credential to the Provider.		
PA-F-09	The OAW engine MUST be able to send data and requests to the Provider.	documentation; test cases	MUST
	Explanation During accreditation, the Onboarding Authority may need to contact the Provider, for example, to request further information or clarifications, or to inform her about the reasons for rejecting the onboarding request. The OAW engine should provide respective means to enable efficient and fast communication between the Onboarding Authority and the Provider.		
PA-F-10	The OAW engine MUST provide means to store accreditation documentation. Documentation MUST be stored in an immutable and confidential manner to ensure its auditability. The OAW engine MUST store these data at least two times the validity periods of the Gaia-X compliance attestation (i.e., six years). All documentation SHOULD be stored in the Compliance Documentation Service.	documentation; test cases	MUST
	Explanation The Onboarding Authority has to document the verification results for each workflow activity and the final decision (e.g., rejection or approval).		
PA-F-11	The OAW engine MUST log each workflow activity (i.e., generate an audit trail) to enable third party auditing, including input data, data about processing activities, output data (e.g., results), corresponding timestamps and accountable users. The OAW engine MUST store these logs at least two times the validity periods of the Gaia-X compliance attestation (i.e., six years).	documentation; test cases	MUST
	Explanation		

	To support the documentation activities of the Onboarding Authority and ensure an audit trail, the OAW engine should log workflow activities in an immutable and confidential manner to ensure its auditability.		
PA-F-12	The OAW engine MUST provide the means to change, export, and delete accreditation data.	documentation; test cases	MUST
	Explanation It must be possible to change or delete the data gathered through accreditation by CAB and Onboarding Authority.		

***Table 12**: Functional Requirements of the Provider Accreditation Workflow (GX-OAW-PA)*

4.3 GX OAW Software Asset and Node Onboarding Workflow (GX-OAW-SNO)

4.3.1 Description and Priority

The OAW Software Asset and Node Onboarding Workflow manages the gathering of relevant information needed for the accreditation, such as the Self-Description, signed Declaration of Adherence, and further relevant assurance information. The Software Asset and Node Onboarding Workflow is of high relevance and MUST be implemented.

4.3.2 Stimulus/Response Sequences

Preconditions (out of scope for OAW engine):

1. **Provider Identification.** Providers have to successfully identify themselves, such as providing the organization's DID first.
2. **Principal Selection.** Providers have to define Principals (i.e., representatives that are authorized to act on behalf of the organization) that will be able to perform the onboarding process (e.g., fill in the self-description, provide required onboarding information, and sign terms and conditions).
3. **Asset Selection.** The Provider selected the Assets (i.e., Software Asset(s) and Node(s)) that apply for enlisting to Gaia-X. Each Provider has to enlist at least one but can also offer multiple Assets.
4. **Assurance Level Determination.** The Provider has to determine the intended Assurance Levels, namely Basic, Substantial, or High, for each Asset and for each control category individually (refer to Section 5.5.1). Thereby, the Provider has also to clarify whether personal data is processed by the Asset.

Workflow Interaction Sequence:

- The Provider provides required data to the OAW engine.
- The Provider changes or deletes submitted data.
- The Provider completes the onboarding workflow by submitting an onboarding request.
- Once completed, the OAW engine submits all information for accreditation to the Onboarding Authority.

4.3.3 Functional Requirements

The OAW engine comprises the following workflow features to enable accreditation activities:

ID	Description	Acceptance Criteria	Priority
SNO-F-01	The OAW engine MUST be able to receive a Software Asset and Node's Self-Description.	documentation; test cases	MUST
	Explanation The Provider has to provide the Self-Description in the defined format about the Assets (e.g., Node(s) or Software Asset(s)) on all items of the defined set of attributes. This Self-Description should be completed by the Provider according to Gaia-X guidelines. A tool to help with the onboarding of the Self-Descriptions may be made available through the Gaia-X Portal or onboarding GUI. The extent of the data to be provided by the Provider will depend on the kind and number of Assets applied for. Since one Provider can provide a multitude of Assets with varying scope and functionalities, mechanisms should be provided enabling Providers to be register and maintain Self-Description information as *'meta asset data'* during the Asset onboarding process. This will help ensuring consistency and minimize the effort of updating Asset information. To the extent (novel) Assets will not be consistent with this meta asset data, the Provider will be required to adequately communicate such differences. To the extent no differences apply, Provider may – efficiently – refer to *"meta asset data"* during the onboarding of Asset (variations).		
SNO-F-02	The OAW engine MUST be able to receive information about a Principal's authorization to act on behalf of the organization. It MAY accept eIDAS service as an acceptable source of provider's identity with verifiable credentials.	documentation; test cases	MUST
	Explanation In line with the precondition *'Principal Selection'*, the OAW engine MUST receive any kind of information to enable verification during the accreditation that the Principal is authorized. This information may be in the form of verifiable credentials or an official approval document that contains the Principal's digital signature, a statement that he/she is authorized to perform the onboarding on behalf of the organization, an identification of the organization (e.g., organization's DID), and, most importantly, a digital signature of the organization's leader (e.g., members of the board), among others.		
SNO-F-03	The OAW engine MUST be able to receive the signed accreditation agreement.	documentation; test cases	MUST
	Explanation The Provider and the Onboarding Authority / CABs must sign the accreditation agreement. The accreditation agreement is a legally enforceable agreement between the Provider and the Onboarding Authority (and/ or CABs performing the accreditation) for the provision of accreditation activities. Accreditation agreements comprise the responsibilities of the		

	Onboarding Authority (and/ or CABs performing the accreditation) and the Provider, among others. The content of the agreement will be specified later in the Gaia-X development process.		
SNO-F-04	The OAW engine MUST be able to receive the claimed Assurance Level of each MVSC control category.	documentation; test cases	MUST
	Explanation The Provider has to determine the intended Assurance Levels (i.e., Basic, Substantial, or High), for each Asset and for each control category individually.		
SNO-F-05	The OAW engine MUST be able to receive the signed Declaration of Adherence.	documentation; test cases	MUST
	Explanation The Provider has to sign a declaration of adherence. Thereby, the Provider confirms that the Self-Description is complete and accurate, and that the fulfillment of the MVSC considering the determined Assurance Levels have been demonstrated at least in internal testing for the Asset in question.		
SNO-F-06	The OAW engine MUST be able to receive the statement about how the Asset fulfills the MVSC.	documentation; test cases	MUST
	Explanation The Provider must provide a rich description that explains how the Asset fulfills each control of the MVSC in accordance with the selected Assurance Levels.		
SNO-F-07	The OAW engine MUST be able to receive the assurance information that proves that the Asset fulfills the MVSC.	documentation; test cases	MUST
	Explanation The Provider has to submit assurance information that proves adherence (e.g., documentation about self-assessment, existing certifications for the Software Asset like ISO/IEC 27001), which will be assessed during the verification performed by the Onboarding Authority. Other documentation to be provided by the Provider for the Assets, including copies of standard service agreements, documentation on IT security management, or any other documents of adherence to existing standards applicable to the Nodes/Software Assets. Information provided by the applying Provider is legally binding and should be signed off by the management.		
SNO-F-08	The OAW engine SHOULD be able to receive further information (e.g., asset documentation).	documentation; test cases	SHOULD
	Explanation		

	Supposedly, the Provider may submit further documentation about the asset or related assurance information.		
SNO-F-9	The OAW engine MUST be able to submit all gathered onboarding information as request for onboarding to the Onboarding Authority.	documentation; test cases	MUST
	Explanation Finally, the Provider submits all information as onboarding request to the Gaia-X Onboarding Authority, which will then initiate accreditation workflows.		
SNO-F-10	The OAW engine MUST log each workflow activity (i.e., generate an audit trail) to enable third party auditing, including input data, data about processing activities, output data (e.g., results), corresponding timestamps and accountable users.	documentation; test cases	MUST
	Explanation To support the documentation activities of the Onboarding Authority and ensure an audit trail, the OAW engine should log workflow activities in an immutable and confidential manner to ensure its auditability.		
SNO-F-11	The OAW engine MUST provide the means to change, export, and delete onboarding data.	documentation; test cases	MUST
	Explanation It must be possible to change or delete the data gathered through onboarding by the Provider and CAB/Onboarding Authority.		

***Table 13**: Functional Requirements of the Software Asset and Node Onboarding Workflow (GX-OAW-SNO)*

4.4 GX OAW Software Asset and Node Accreditation Workflow (GX-OAW-SNA)

4.4.1 Description and Priority

The Gaia-X Onboarding Authority will, with the support of CABs, verify onboarding information for completeness, integrity, and honesty. Most importantly, they will verify whether the Asset complies with the MVSC in accordance with the relevant Assurance Levels.

The Software Asset and Node Accreditation Workflow is of high relevance and MUST be implemented.

4.4.2 Stimulus/Response Sequences

Precondition:

1. **Request received.** Onboarding Authority received the onboarding request from a Provider.

Workflow Interaction Sequence:

- The Onboarding authority and / or CAB accesses onboarding data.
- The Onboarding authority and / or CAB stores (intermediate) accreditation data.
- The Onboarding authority and / or CAB accesses, changes, or deletes (intermediate) accreditation data.
- The Provider provides additional data that is then stored and accessible for the Onboarding Authority.
- The Onboarding authority and / or CAB completes the accreditation workflow by specifying the final decision (i.e., approved or rejected).
- Once completed, the OAW engine submits all information to the Notary Service to generate a verifiable credential.

4.4.3 Functional Requirements

The OAW engine comprises the following workflow features to enable accreditation activities:

ID	Description	Acceptance Criteria	Priority
SNA-F-01	The OAW engine MUST provide the information on Principal's authorization. It SHOULD automatically validate verifiable credentials of a Principal if available.	documentation; test cases	MUST
	Explanation The Onboarding Authority will verify whether a Principal is authorized to perform the onboarding process on behalf of the organization.		
SNA-F-02	The OAW engine MUST be able to receive the signed accreditation agreement. The OAW engine MUST be able to store the accreditation agreements once signed by the Onboarding Authority (and/or CABs) as well.	documentation; test cases	MUST
	Explanation The Provider and the Onboarding Authority (and/or CABs) must sign the accreditation agreement. The accreditation agreement is a legally enforceable agreement between the Provider and the Onboarding Authority (and/ or CABs performing the accreditation) for the provision of accreditation activities. Accreditation agreements comprise the responsibilities of the Onboarding Authority (and/ or CABs performing the accreditation) and the Provider, among others. The content of the agreement will be specified later in the Gaia-X development process.		
SNA-F-03	The OAW engine MUST be able to provide all data submitted via the onboarding request.	documentation; test cases	MUST
	Explanation		

	The Onboarding Authority will verify onboarding information for completeness, integrity, and honesty. Particularly, it has to verified whether: • the onboarding request contains all the mandatory information; • the scope of the accreditation is clearly defined (i.e., all parts of the Software Asset / Node are identified); • the information about the Software Asset / Node is sufficient for conducting the accreditation.		
SNA-F-04	The OAW engine MUST be able to adjust the workflow based on the selected Assurance Level to ease accreditation.	documentation; test cases	MUST
	Explanation The accreditation efforts differ for each Assurance Level. Higher Assurance Level require additional verification activities, among others.		
SNA-F-05	The OAW engine MUST offer functionalities to support the Onboarding Authority to familiarize herself with the Asset in question. Potential functionalities include, generating summaries and overviews of the onboarding information; providing all required information submitted by the Provider; allowing the Onboarding Authority to take notes and store them; searching, filtering, and highlighting information functions.	documentation; test cases	MUST
	Explanation The Onboarding Authority has to familiarize itself with the specific Asset. This process includes a review of the Self-Description, the identification the boundaries of that Asset, and how it interfaces with other systems (e.g., Assets provided by sub providers). In addition, the Onboarding Authority determines to what extent and for which processes the Provider uses sub providers and how the Provider controls and monitors the Assets provided by these sub providers.		
SNA-F-06	The OAW engine MUST offer functionalities to support the Onboarding Authority to create an audit plan for the accreditation. Potential functionalities include, audit plan templates, plan management and storage capabilities, accreditation workflow overviews, dashboards, and summaries.	documentation; test cases	MUST
	Explanation		

	The accreditation shall be driven by a predefined audit plan, which has to be developed by Onboarding Authority, including setting the scope, timing and direction of the verification to be carried out in order to achieve the objective of the accreditation.		
SNA-F-07	The OAW engine MUST be able to support the accreditation activities for the Basic Assurance Level.	documentation; test cases	MUST
	Explanation The accreditation of Assurance Level Basic aligns with the basic assessment specified in EUCS and is adjusted to consider Gaia-X specifics (refer to [ENISA 2020]).[14] At the Basic Assurance Level, the verification is greatly simplified, and it relies solely on evidence provided by the Provider, if needed upon explicit request from the Onboarding Authority. Such a lightweight approach is facilitating a controlled environment for providing limited assurance while keeping the associated cost for accreditation affordable for small and medium-sized Providers, through limited verification of documentation by an independent reviewer that the Software Asset or Node is built and operated with procedures and mechanisms to meet the corresponding Gaia-X MVSC. The verification starts when the Provider provides the results of their self-assessment, together with all required supporting documentation during the onboarding of Assets.		
SNA-F-08	The OAW engine MUST be able to support the accreditation activities for the Substantial and High Assurance Level.	documentation; test cases	MUST
	Explanation The verification of Substantial and High Gaia-X Nodes and Software Assets builds on the Basic verification process but differs in the verification scope and efforts (refer to [ENISA 2020] for more information). In particular, self-assessments are not sufficient for the Substantial and High Assurance Levels. Instead, Gaia-X will refer to existing standards, certifications, attestations, code of conducts, audit results, etc. that are appropriate to fulfil the MVSC for the Substantial and High Assurance Levels. In the following, these are referred to as “assurance mechanisms”. In case no assurance mechanism exists to provide required evidence, Gaia-X Onboarding Authority will perform additional verification.		
SNA-F-09	The OAW engine SHOULD store a list of assurance mechanisms that are sufficient to prove	documentation; test cases	SHOULD

[14] Refer to EUCS Annex D [ENISA 2020]. Please note, following functions descriptions may be adapted from the paragraphs of this annex. GAIA-X highly acknowledges the efforts of ENISA and their proposal for an EU cybersecurity scheme.

	compliance for each MVSC for the Substantial and High Assurance Levels.		
	Explanation Gaia-X will list assurance mechanisms that are sufficient to prove compliance for each MVSC category. Participants and external stakeholders may propose further assurance mechanisms to be acknowledged by Gaia-X.		
SNA-F-10	The OAW engine MUST provide the Self-Description. The OAW engine SHOULD incorporate features to support the Onboarding Authority performing verification of the Self-Description. For example, the OAW engine SHOULD automatically verify attributes of the Self-Description (e.g., whether an attribute is given, adheres to a given policy etc.).	documentation; test cases	MUST
	Explanation The Onboarding Authority will review the Self-Description. During this review, the Onboarding Authority will verify that all mandatory fields of the Self-Descriptions are completed (i.e., ensuring completeness). The Onboarding Authority will then check whether the information entered in the Self-Description is truthful by performing spot checks on random or conspicuous information (i.e., ensuring integrity and honesty). For example, the Onboarding Authority may match information from the Self-Description with public available information (e.g., on the website of the Provider). If the Onboarding Authority has any doubts regarding the information's integrity and/or honesty, the Authority will inform the Provider, and request evidence that the information is truthful or corrections of the information in question. The review of the self-description should be automated to the highest extent possible. For example, scripts may be implemented that check whether the provided commercial registry number is authentic by automatically querying public databases.		
SNA-F-11	The OAW engine MUST provide assurance information that is contained in the onboarding request.	documentation; test cases	MUST
	Explanation The Provider has to submit assurance information to prove compliance with the MVSC. For the Basic Assurance Level, the Provider provides the results of their self-assessment, together with all required supporting documentation during the onboarding of Assets. For the Substantial and High Assurance Levels, the Provider provides evidence of their accomplished assurance mechanisms.		
SNA-F-12	The OAW engine SHOULD provide functionalities to support the Onboarding Authority in assessing	documentation; test cases	SHOULD

	completeness, coherence and plausability of the provided documentation.		
	Explanation The Onboarding Authority assesses completeness, coherence and plausability of the provided documentation: 1. the evidence addresses the MVSC in a sufficiently comprehensive manner; 2. the evidence is sufficiently clear and unambiguous in how the MVSC are met and implemented by the Provider; 3. the evidence is prima facie plausible (i.e., it appears in the professional opinion of the reviewer that there are no elements in the evidence that are manifestly inaccurate, incomplete, or false) and verifiable (can in principle be verified by an on-site audit).		
SNA-F-13	The OAW engine MUST provide functionalities to support the Onboarding Authority in assessing assurance information for Assets with the Basic Assurance Level.	documentation; test cases	MUST
	Explanation For the Basic Assurance Level, the Onboarding Authority inspects the provided documents in detail (refer to [ENISA 2020] for more information). The Onboarding Authority shall obtain sufficient and appropriate objective evidence by evaluating the provided documentary evidence by the Provider regarding: • the suitability of the design of controls to meet the MVSC. A control is suitably designed when actions or events that comprise a risk (e.g., for information security) are prevented or detected and corrected. Obtaining evidence regarding the suitability of the design of controls requires the Onboarding Authority to determine whether the risks that threaten the achievement of the Gaia-X principles and therefore the MVSC have been identified by management; and the controls are, if operating effectively, able to prevent or detect if the MVSC are not met. • the actual existence and implementation of controls to be in accordance with their design as of a point in time (specified date). To be able to conclude on this the reviewer shall obtain evidence related to exemplary actions or events that triggered the occurrence or performance of the controls (e.g., tickets) and to inspect the environment in which it operates (e.g., suitable configuration of the tools or systems used to execute the control in accordance with the design).		
SNA-F-14	The OAW engine MUST provide functionalities to support the Onboarding Authority in assessing assurance information for Assets with the Substantial Assurance Level.	documentation; test cases	MUST
	Explanation		

	Besides performing verification activities outlined in the Basic Assurance level (i.e., verify onboarding information for completeness, integrity, and honesty; familiarize with the specific Asset; and develop an audit plan), the Onboarding Authority verifies provided assurance mechanisms in detail (refer to [ENISA 2020] for more information), particularly, it verifies that • the assurance mechanism is issued by a trustworthy party (e.g., by an accredited certification body in case of data protection certifications proving GDPR compliance); • the assurance mechanism addresses the MVSC in a sufficiently comprehensive manner, that is, the scope of the assurance mechanism fits the Gaia-X Asset and the MVSC; • the assurance mechanism is sufficiently clear and unambiguous in how the MVSC are met and implemented by the Provider, that is, the Provider transmit the complete audit report and not only a simple certificate, for example; • the assurance mechanism has a sufficient level of formality and rigor, and is based on a thorough assessment and standard and repeatable processes, including on-site audits comprising interviews and inspecting samples, plus a verification that the implementation follows the specified processes and design; • the assurance mechanism is still valid and not outdated, that is, the assurance mechanism is not expired and not older than 3 years; • the assurance mechanism is subject to frequent re-assessment, for example, on a yearly basis to ensure ongoing compliance and validity.		
SNA-F-15	The OAW engine MUST provide functionalities to support the Onboarding Authority in assessing assurance information for Assets with the High Assurance Level.	documentation; test cases	MUST
	Explanation The verification of High Gaia-X Nodes and Software Assets builds on the Substantial verification process but differs in the verification scope and efforts (refer to [ENISA 2020] for more information). Besides the Substantial Level controls there will be additional controls that a Software Asset / Node has to fulfill, for example, in the case of cybersecurity. In addition, further verification processes and measurements are applied. In particular, Continuous Automated Monitoring may be applied to verify ongoing compliance with selected controls. Such activities shall be planned over multiple years, and they shall be performed by personnel with appropriate competences, in particular when penetration testing or in-depth technical reviews are required.		
SNA-F-16	The OAW engine MUST be able to receive and store the final decision of the Onboarding Authority.	documentation; test cases	MUST
	Explanation		

	Based on the verification and provided evidence, the Onboarding Authority shall assess if it can be concluded that nothing has come to its attention that causes the reviewer to believe that the technical and organizational manners warranted by the Provider are not meeting in all material aspects the MVSC of the Assurance Levels and that the evidence presented is at least sufficient for the Onboarding Authority to obtain a level of assurance. The Onboarding Authority approves or rejects the Asset onboarding. In case of rejection, the Gaia-X Provider will be informed about the reasons for rejection and allowed to adjust the registration and related information.		
SNA-F-17	The OAW engine MUST offer functionalities to support the Onboarding Authority in generating, transmitting, and storing a final accreditation report.	documentation; test cases	MUST
	Explanation The Onboarding Authority shall issue the accreditation report to the Provider.		
SNA-F-18	The OAW engine MUST offer functionalities to support the Onboarding Authority in contacting the Provider before final decision.	documentation; test cases	MUST
	Explanation Depending on the outcomes of the accreditation workflow, the Onboarding Authority may need to get in touch with the Provider. For example, if the Asset does not fulfill the MVSC for the Substantial but Basic Assurance Level, the Onboarding Authority may ask the Provider whether listing the Asset with the Basic Assurance Level is sufficient.		
SNA-F-19	The OAW engine MUST offer functionalities to support the Onboarding Authority in determining the validity period of the Gaia-X compliance attestation.	documentation; test cases	MUST
	Explanation If the onboarding is approved, the Onboarding Authority needs to determine the validity period of the Gaia-X compliance attestation. In general, the validity period is 3 years, with annual re-assessments. If existing assurance mechanisms (i.e., certifications) are acknowledged, the shortest validity period of the assurance mechanisms is taken (particularly relevant for Assurance Levels Substantial and High). For example, if an Asset has an ISO/IEC 27001 certificate which is valid for 2 years, the validity period of the Gaia-X compliance attestation is set to 2 years. If the Provider renews the ISO/IEC 27001 certificate, the validity period of the Gaia-X compliance attestation can be extended, but not more than 3 years after making the approval.		

SNA-F-20	The OAW engine MUST create a verifiable credential using the Notary Service if onboarding is approved.	documentation; test cases	MUST
	Explanation If the Onboarding Authority approves the onboarding, a respective verifiable credential is created using the Notary Service (i.e., Gaia-X compliance attestation). The verifiable credential is then sent to the Provider.		
SNA-F-21	The OAW engine MUST be able to send data to other stakeholders and services.	documentation; test cases	MUST
	Explanation Eventually, the Asset's Self-Description will be added to the Gaia-X Federated Catalogue. The OAW engine therefore must be able to send the verified Self-Description to the Catalogue.		
SNA-F-22	The OAW engine MUST be able to send data and requests to the Provider.	documentation; test cases	MUST
	Explanation During accreditation, the Onboarding Authority may need to contact the Provider, for example, to request further information or clarifications, or to inform her about the reasons for rejecting the onboarding request. The OAW engine should provide respective means to enable efficient and fast communication between the Onboarding Authority and the Provider.		
SNA-F-23	The OAW engine MUST provide means to store accreditation documentation. Documentation MUST be stored in an immutable and confidential manner to ensure its auditability. The OAW engine MUST store these data at least two times the validity periods of the Gaia-X compliance attestation (i.e., six years). All documentation SHOULD be stored in the Compliance Documentation Service.	documentation; test cases	MUST
	Explanation The Onboarding Authority has to document the verification results for each workflow activity and the final decision (e.g., rejection or approval).		
SNA-F-24	The OAW engine MUST log each workflow activity (i.e., generate an audit trail) to enable third party auditing, including input data, data about processing activities, output data (e.g., results), corresponding timestamps and accountable users. The OAW engine MUST store these data at	documentation; test cases	MUST

	least two times the validity periods of the Gaia-X compliance attestation (i.e., six years).		
	Explanation To support the documentation activities of the Onboarding Authority and ensure an audit trail, the OAW engine must log workflow activities in an immutable and confidential manner to ensure its auditability.		
SNA-F-25	The OAW engine MUST provide the means to change, export, and delete accreditation data.	documentation; test cases	MUST
	Explanation It must be possible to change or delete the data gathered through accreditation by CAB and Onboarding Authority.		

***Table 14**: Functional Requirements of the Software Asset and Node Accreditation Workflow (GX-OAW-SNA)*

4.5 GX OAW Management Workflows (GX-OAW-MW)

4.5.1 Description and Priority

Besides the main OAW, further management workflows are required to ensure continuously compliant Providers and Assets. Management workflows are of medium relevance and MUST be implemented.

4.5.2 Stimulus/Response Sequences

Workflow Interaction Sequence:

- The Onboarding authority and / or CAB accesses the OAW engine to use management workflows at a specific point in time / during a specific workflow activity / as response to a certain event.

4.5.3 Functional Requirements

The OAW engine comprises the following workflow features to enable management activities:

ID	Description	Acceptance Criteria	Priority
MW-F-01	The OAW engine MUST enable the communication between Providers and the Onboarding Authority or CABs that perform the accreditation.	documentation; test cases	MUST

<table>
<tr><td></td><td colspan="3">Explanation

In general, there might be a need for a Provider, the Onboarding Authority, or a CAB to communicate with the stakeholders participating in the OAW. For example, the Onboarding Authority may request further information from the Provider, or the Provider may ask questions regarding the accreditation process. The OAW engine must therefore implement appropriate communication technologies, such as an internal messaging system, contact forms, email forwarding etc.</td></tr>
<tr><td>MW-F-02</td><td>The OAW engine MUST implement functionalities to support the Onboarding Authority in performing Software Asset and Node surveillance activities.</td><td>documentation; test cases</td><td>MUST</td></tr>
<tr><td></td><td colspan="3">Explanation

At a given interval, a re-evaluation about a Provider’s and their Assets’ compliance with the Gaia-X principles has to be performed. If the Gaia-X principles and particularly the MVSC are not met anymore, the listing in the Gaia-X repository can be suspended. Ideally this surveillance activities can be performed, at least in part, automated.

For the Basic Assurance Level, the Provider has to send once a year a documentation update for review of the continued development and operation of the Software Asset or Node (refer to [ENISA 2020] for more information). Self-gathered evidence shall be regularly submitted by the Provider to the Onboarding Authority to justify the continued development and operation of the Software Asset or Node.

For the Substantial and High Assurance Level, the Onboarding Authority verifies whether recognized assurance evidence (e.g., certifications) are still valid. Self-gathered evidence shall be regularly submitted by the Provider to the Onboarding Authority to justify the continued development and operation of the Software Asset or Node. The Onboarding Authority may decide to perform spot-check verifications to validate Asset’s compliance with the MVSC.

In particular, this surveillance shall allow where possible to avoid and where needed to detect the following general cases of non-compliance (refer to [ENISA 2020]):
- a non-compliance of the rules and obligations related to a Gaia-X compliance attestation issued on their Assets;
- a non-compliance in the conditions under which the accreditation takes place and that are not related to the individual Asset;
- a nonconformity of an accredited Asset with the MVSC, which includes and is not limited to:
  ○ a change in the Asset itself leading to a change of the Asset’s security posture;</td></tr>
</table>

	○ a significant security incident that has affected the accredited Asset or has resulted in a data breach or loss of sensitive information; ○ a change in the threat environment after the issuance of the Gaia-X compliance attestation, which has an adverse impact on the security of the accredited Asset; - a vulnerability identified and related to the accredited Asset, that has an adverse impact on the security of the accredited Asset. The general surveillance of the accredited Asset shall be based on sampling.		
MW-F-03	The OAW engine MUST implement functionalities to react to changes in the Self-Description of a Provider or an Asset.	documentation; test cases	MUST
	Explanation The Self-Description may be changed or updated by a Provider. Upon receiving an updated Self-Description, the OAW engine should perform (an automated) check if the changes are relevant for the compliance assessments. If changes are relevant, the Onboarding Authority should be informed to verify these changes before the Self-Description is added to the Federated Catalogue. The Onboarding Authority must develop a policy that can be used to perform these automated checks.		
MW-F-04	The OAW engine SHOULD implement functionalities to support the Onboarding Authority in assessing and approving CABs.	documentation; test cases	SHOULD
	Explanation The Onboarding Authority may decide to outsource accreditation activities to third parties, such as certification authorities, auditing companies etc. Before CABs can act on behalf of the Onboarding Authority, they have to be assessed and approved by the Onboarding Authority. In the future releases of Gaia-X, a list of requirements that a CAB needs to fulfill will be developed (e.g., in regard to employees' competencies, structural capabilities, assessment methods, reporting etc.). Once the Onboarding Authority approves the CAB, a verifiable credential will be created that proves this approval, supposedly by using the Notary Service. The OAW engine should consider this upcoming feature extensions.		
MW-F-05	The OAW engine MUST implement functionalities to support the Onboarding Authority in acknowledging further assurance mechanisms for the Substantial and High Assurance Levels.	documentation; test cases	MUST
	Explanation The Substantial and High Level of Assurance require Providers to prove compliance of their Assets with the MVSC by providing existing assurance mechanisms (e.g., certifications, audits, code of conducts etc.). The Onboarding Authority has to develop an acknowledgement process that decides whether an existing assurance mechanism is appropriate to prove		

	compliance with a certain MVSC category (e.g., data protection, cybersecurity). The OAW engine must offer functionalities to support this acknowledgement workflow, such as an interface that offers Gaia-X Participants the possibility to submit an assurance mechanism as potential candidate, and a management dashboard to inspect, accept, and decline proposed assurance mechanisms. In particular, to ensure a Substantial and High Level of Assurance, the assurance mechanisms should 1) guarantee a sufficient level of formality and rigor, 2) are based on a thorough assessment and standard and repeatable processes, 3) offer accurate reporting standard, and 4) there exist clear and well-defined auditor competences requirements. In line with EUCS verification scope (refer to [ENISA 2020]), assurance mechanisms for the Assurance Level Substantial and High shall include on-site audit including interviews and inspecting samples, plus a verification that the implementation follows the specified processes and design, including the validation of the functional tests performed on that implementation.		
MW-F-06	The OAW engine MUST implement functionalities to receive, store, and process OAW events.	documentation; test cases	MUST
	Explanation During the OAW, diverse events may appear, including complaints of Participants, information about Providers' or their Assets' non-compliance (e.g., from the Continuous Automated Monitoring Service), misbehavior by CABs, or issues with the approval of CABs. The OAW engine must implement an event-management system that is able to receive external and internal events, store these events, and enable processing by the CAB and/or the Onboarding Authority.		
MW-F-06	The OAW engine SHOULD offer management workflow templates and the flexibility to implement these into the OAW.	documentation; test cases	SHOULD
	Explanation While this document specifies already a variety of workflows and their activities, the Onboarding Authority or CAB may require further workflow activities. The OAW engine should be flexible and adaptable and offer workflow templates to achieve easy extension of the OAW engine.		

***Table 15**: Functional Requirements of the Management Workflow (GX-OAW-MW)*

4.6 GX OAW Offboarding Workflow (GX-OAW-OFF)

4.6.1 Description and Priority

The OAW engine finally should support the offboarding of Providers, Software Assets and Nodes.

The offboarding workflow is of high relevance and MUST be implemented.

4.6.2 Stimulus/Response Sequences

Workflow Interaction Sequence:

- The Onboarding authority and / or CAB initiates the offboarding workflow (e.g., due to violations of the MVSC).
- The Provider requests to be offboarded.
- Any internal or external stakeholder may want to send the Onboarding Authority about compliance-relevant information.

4.6.3 Functional Requirements

The OAW engine comprises the following workflow features to enable offboarding activities:

ID	Description	Acceptance Criteria	Priority
OFF-F-01	The OAW engine MUST enable the communication between Providers, the Onboarding Authority, CABs that perform the accreditation, further Gaia-X Participants, or external Stakeholders.	documentation; test cases	MUST
	Explanation The OAW engine should offer an interface to receive any notifications regarding the compliance status of a Provider or Asset. Gaia-X Participants or external stakeholders may have information on compliance issues, misbehavior, or violations of the MVSC that should be handed over to the Onboarding Authority to take actions (e.g., suspension, restriction, or revocation of the Gaia-X compliance attestation). For example, an external certification authority may want to inform the Onboarding Authority that a certain certificate has become invalid for a specific Asset.		
OFF-F-02	The OAW engine MUST implement functionalities to suspend Gaia-X compliance attestations for a Provider or an Asset.	documentation; test cases	MUST
	Explanation A suspension refers to temporary withdrawal of the attestation of conformity by the Onboarding Authority. The Onboarding Authority decides why and how long the suspension takes place (e.g., due to minor violations with the MVSC that can be fixed easily by a Provider). If the Gaia-X compliance attestation is suspended, the Onboarding Authority shall take measures to make any necessary changes to formal accreditation documents, public information, permits to use marks, etc. to ensure that it does not give any indication that the Provider, Software Asset and Nodes are still accredited. This includes in particular the temporary withdrawal of the verifiable credential, any mark of conformity and the removal of the Provider, Software Asset and Node from any lists of accredited Gaia-X objects. The Onboarding Authority needs to inform the Provider about the decision.		

OFF-F-03	The OAW engine MUST implement functionalities to restrict or extend Gaia-X compliance attestations for a Provider or an Asset.	documentation; test cases	MUST
	Explanation The Onboarding Authority may restrict the Gaia-X compliance attestation if, although the MVSC for the Assurance Level applied for are not met, the MVSC for a lesser Assurance Level are met. In such cases, the Gaia-X compliance attestation may be granted for a lower Assurance Level. Restriction of attestations are performed by the Onboarding Authority during the surveillance of compliance or if any compliance-relevant event appeared (e.g., violations of certain controls). Also, the Provider may request the restriction of the Gaia-X compliance attestation at any time. The request shall be complied with unless there are serious reasons to the contrary. Similar, the Onboarding Authority may extent the Gaia-X compliance attestation if the Provider can prove and accreditation workflows verify that the MVSC for a higher Assurance Level are met. If the Gaia-X compliance attestation is restricted, the Onboarding Authority shall take action and make any necessary changes to formal accreditation documents, public information, permission to use marks of conformity, etc. to ensure that the restricted scope of attestation is clearly communicated to the Provider and clearly described in the accreditation documentation and public information. This includes in particular the change of the verifiable credential, mark of conformity as well as the change the any entries in lists of accredited Providers, Software Assets and Nodes. The Onboarding Authority needs to inform the Provider about the decision.		
OFF-F-04	The OAW engine MUST implement functionalities to revoke Gaia-X compliance attestations for a Provider or an Asset.	documentation; test cases	MUST
	Explanation A revocation refers to permanent withdrawal of the statement of conformity by the Onboarding Authority. Revocation may result from violations with the Gaia-X principles or MVSC. In addition, the Provider may apply for revocation at any time. The application shall be complied with unless there are serious reasons to the contrary. The Gaia-X compliance attestation shall be revoked if a. the Onboarding Authority determines that the prerequisites for granting the attestation were not met or are no longer met; b. a surveillance audit is not carried out or not carried out within the specified period. If the Gaia-X compliance attestation is suspended, the Onboarding Authority shall take measures to make any necessary changes to formal accreditation documents, public information, permits to use marks, etc. to ensure that it does not give any indication that the		

	Provider, Software Asset and Node are still accredited. This includes in particular the permanent withdrawal of the verifiable credential, any mark of conformity and the removal of the Provider, Software Asset and Node from any lists of accredited Gaia-X objects. The Onboarding Authority needs to inform the Provider about the decision.		
OFF-F-05	The OAW engine MUST implement functionalities to inform services and stakeholders about changes in status of the compliance attestation.	documentation; test cases	MUST
	Explanation If any change is made to the status of the Gaia-X compliance attestation (e.g., suspended, revoked, restricted), the Onboarding Authority may need to inform other Federated Services (i.e., Federated Catalogue) or Stakeholders.		

***Table 16**: Functional Requirements of the Management Workflow (GX-OAW-MW)*

5. Other Nonfunctional Requirements

5.1 Performance Requirements

ID	Description	Acceptance Criteria	Priority
PE-NF-01	The OAW engine SHOULD automate workflow activities as high as possible to ensure efficient workflow processing. For example, the OAW engine may support automated verification of the Self-Description.	Documentation; test cases	SHOULD
PE-NF-02	The OAW engine's operations SHOULD achieve a low latency, high response time and enable fast processing to reduce any delays in the workflows.	Documentation; test cases	SHOULD

***Table 17**: Nonfunctional Requirements Performance Requirements*

5.2 Safety Requirements

Not applicable.

5.3 Security Requirements

5.3.1 General Security Requirements

Each Gaia-X Federation Service MUST meet the requirements stated in the document "Specification of non-functional Requirements Security and Privacy by Design" [NF.SPBD].

Each Gaia-X Federation Service MUST fulfil the cybersecurity control set of the EUCS Annex A according to its assigned Assurance Level. The EUCS control set includes 20 control groups describing requirements on

different layers (from the physical protection to application security) and from different types (organizational, technical, procedural). Only some of the controls and requirements are in primary scope of the Federation Services. Some of them MUST be fulfilled by the Service Provider Organization (e.g., ISO 27001 Certificate) while others addressing the Infrastructure Provider of a Federation Service.

5.3.2 OAW Specific Security Requirements

Not applicable.

5.4 Software Quality Attributes

ID	Description	Acceptance Criteria	Priority
SQ-NF-01	The OAW engine SHOULD be highly available to allow data provisioning and processing.	Documentation; test cases	SHOULD
SQ-NF-02	The OAW engine SHOULD be highly adaptable to include further workflows, change existing workflows, or remove specified workflows.	Documentation; test cases	SHOULD
SQ-NF-03	The OAW engine SHOULD be robust, particularly, being able to handle faulty input and usage.	Documentation; test cases	SHOULD
SQ-NF-04	The OAW engine SHOULD achieve a high degree of ease of use.	Documentation; test cases	SHOULD
SQ-NF-05	The OAW engine SHOULD achieve a high degree of customizability enabling to edit each workflow activity if needed by the Onboarding Authority or a CAB.	Documentation; test cases	SHOULD
SQ-NF-06	The OAW engine SHOULD achieve a high degree of scalability to handle a high number of incoming requests.	Documentation; test cases	SHOULD
SQ-NF-07	The OAW engine SHOULD allow submitting a batch of Assets to reduce efforts for the Provider and Onboarding Authority. For example, Asset families might be submitted, applying modularization (refer to Section 5.5.3).	Documentation; test cases	SHOULD

***Table 18**: Nonfunctional Requirements Software Quality Attributes*

5.5 Business Rules

5.5.1 Definition of Assurance Levels for Software Assets and Nodes

An Assurance Level is a basis for confidence that an Asset meets the MVSC of Gaia-X and indicates the level at which an Asset has been verified, but as such does not measure the quality of the Asset concerned.[15] An Assurance Level thus reflects the level of scrutiny to which the Asset is submitted. The general scope is the same as for all Assurance Levels, however, the number of controls may vary. Higher Assurance Levels will mostly include more controls and have increased verification requirements.

Gaia-X will comprise three different Assurance Levels for Software Assets and Nodes to ensure that Gaia-X controls will be met in regard to the specific characteristics of each Software Asset and Node (e.g., processing personal data necessitates compliance with the GDPR). In addition, these Assurance Levels also enable organizations with limited resources (e.g., start-ups, small and medium-sized enterprises) to enter the Gaia-X ecosystem.

Please note that Gaia-X currently differentiates between control categories of the MVSC, including (1) transparency, (2) cybersecurity, (3) data protection & privacy, and (4) interoperability.[16] The Assurance Level will be determined for each of the control category individually to enable further differentiation of Providers. For example, a Software Asset may fulfill cybersecurity Assurance Level High, however, only supports the Basic Assurance Level for interoperability, since it is not the focus of the Software Asset.

This implies that in the Gaia-X Federated Catalogue a clear and unambiguous indication of the levels of assurance for each Asset and the corresponding control categories have to be provided to allow for the Consumer to make an informed decision as to which Asset match her individual preferences.

The following Assurance Levels are in line with the analogy of the security levels of the EU Cybersecurity Act (EUCA)[17] and the Concept of Categories of Protection Needs as laid out in the GDPR certifications[18] and codes of conduct as entitled by the European Union and its bodies, e.g., European Data protection Board (EDPB):

- **"Basic Gaia-X Assurance":**
  - Required for Software Assets and Nodes suited for the support of non-critical processes or processing public or non-sensitive data.
  - Providers perform a self-assessment at the Basic Assurance Level and provide related documents as evidence, but they cannot make a self-declaration about conformity with Gaia-X controls. The only way to claim conformity with the Gaia-X Basic Assurance Level is to undergo a verification by a CAB that reviews provided evidence.
  - In line with the EU cloud service cybersecurity certification scheme (EUCS), verification of Assurance Level Basic shall consist solely of inspection activities, based on a check for

[15] Please note, GAIA-X has adapted the definition of ENISA's Assurance Level for cybersecurity. Please refer to [ENISA 2020] for more details.

[16] The policy rules committee will determine the MVCS and respective categories in the future.

[17] See https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme, Please note that the following paragraphs partially rely on the descriptions of EUCA's assurance levels on page 19 and the following. All rights reserve to ENISA.

[18] See for example the AUDITOR certification www.auditor-cert.de / www.auditor-cert.eu

completeness, coherence and plausability of the provided documentation on processes and design intended to confirm the fulfilment of technical and organizational measures.
    - Self-gathered evidence shall be regularly submitted to the CAB to justify the continued development and operation of the Software Asset.
- "**Substantial Gaia-X Assurance**":
    - Required for Software Assets and Nodes suited to support potentially business-critical or safety-critical Services, or processing personal or sensitive data (e.g., data that has a specific informative value about the personality or the life of the data subject).
    - Gaia-X will refer to existing standards, certifications and related assurance mechanisms that are appropriate to fulfil the Substantial Assurance Level. In case no assurance mechanism exist, Gaia-X CABs will perform additional verification.
    - In line with EUCS, the verification aims at providing reasonable assurance that the controls are properly designed and operated effectively. The verification scope for Assurance Level Substantial shall include, in addition to the requirements for Assurance Level Basic, on-site audit including interviews and inspecting samples, plus a verification that the implementation follows the specified processes and design, including the validation of the functional tests performed on that implementation.
- **"High Gaia-X Assurance**":
    - Required for Software Assets and Nodes used to support mission-critical processes or to process highly sensitive and regulated data (e.g., data that has a considerable informative value about the personality or the life of a data subject or is otherwise of considerable significance to the data subject's affairs because the data is, for example, directly dependent on the decision or performance of the data processor in an existential way).
    - Besides the Substantial Level controls there will be additional verification processes and measurements applied. In particular, Continuous Automated Monitoring may be applied to verify ongoing compliance with selected controls. Such activities shall be planned over multiple years, and they shall be performed by personnel with appropriate competences, in particular when penetration testing or in-depth technical reviews are required.

A Provider has at least to apply for the '*Basic Assurance Level'* for each control category (e.g., transparency, cybersecurity, data protection & privacy, interoperability) for a specific Software Asset or Node.

For those Assurance Levels different inspection depth or controls (**Fehler! Verweisquelle konnte nicht gefunden werden.**) are needed, following the elementary principles, as already defined in context of the EUCA:

- The Substantial Assurance Level should comply with the controls used for the Basic Level;
- The High Assurance Level should comply with the controls used for the Substantial and the Basic Level;
- The assurance verification mechanisms should allow for a natural progression, through enhanced control implementation and control validation (which is part of any normal auditing and testing effort) for the Software Asset and Node to progress to the next Assurance Level without restarting fully new testing or auditing processes. For the avoidance of doubt: equally, a degradation may take place

if and to the extent an Asset is not complying with a higher assurance but still with any lower level of assurance.

- The levels of non-atomar constructs of processing (e.g., Service A running on Node 1 incorporating Service B running on Node 2) follow the principle of inheritance of the Assurance Level.

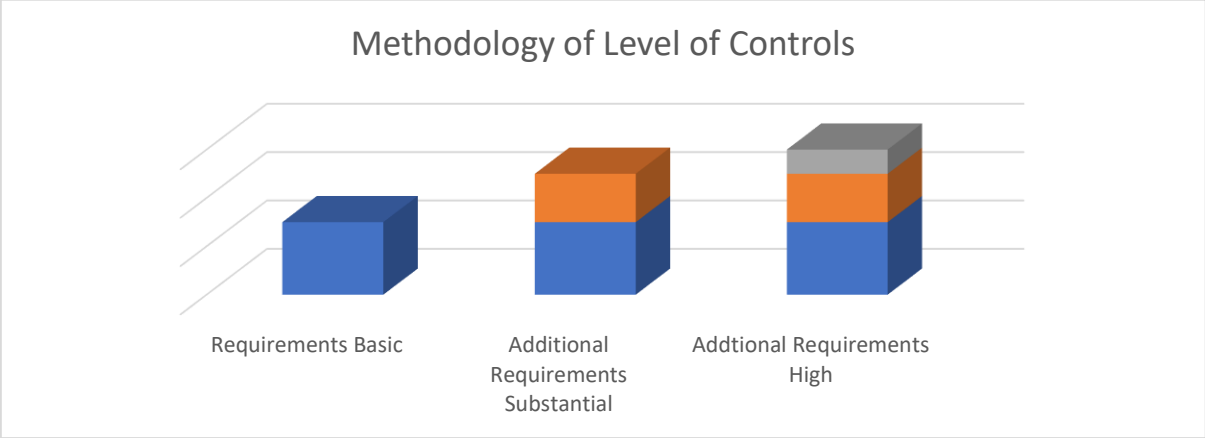


***Figure 2**: Outline for controls based on the Assurance Levels*

5.5.2 Minimal Viable Set of Controls

To ensure that each Nodes and Software Asset fulfills appropriate controls regarding IT security, data protection, and interoperability to foster secure and reliable participation in the Gaia-X ecosystem and to achieve transparency, each Provider has to sign a Declaration of Adherence for each offered Node and Software Asset.

For the first Gaia-X development phase, Gaia-X will only specify MVSC for the Basic Assurance Level. For the Substantial and High Assurance Levels, Gaia-X will list appropriate standards, certifications, code of conducts and related assurance mechanisms that exist in the market. A Participant applying the Substantial or High Assurance Level for Assets has to prove compliance with these assurance mechanisms, which will then be verified by CABs. If no assurance mechanism exist, Gaia-X will define additional controls that will be verified.

Gaia-X has currently major control categories, such as (1) transparency, (2) cybersecurity, (3) data protection & privacy, and (4) interoperability. For each control category an Assurance Level should be specified individually. **Fehler! Verweisquelle konnte nicht gefunden werden.** summarizes the control categories. The policy rules committee will define the MVSC in detail in the future.

Control Category	**Description**
Transparency	Representation of important information of the Provider and Asset (e.g., functional description of the Software Asset).
Cybersecurity	Representation of technical and organizational measures for ensuring cybersecurity

Data Protection & Privacy	Representation of technical and organizational measures for ensuring GDPR compliance and data privacy.
Interoperability	Representation of technical and functional prerequisites for use, portability, migration and change of Assets.

***Table 19**: Summary of MVSC and links to the respective control catalogue*

5.5.3 Accreditation Modularization due to Asset Compositions

Cloud services are layered systems, in which infrastructure and platform capabilities from a Software Asset are often used as a basis for other Software Assets. These Software Assets used by a Provider in the provision of its own Software Asset are referred to as Sub-Services, supplied by Sub-Providers. To ease verification processes, Gaia-X aims to achieve verification modularization, thereby fulfilling two objectives:

- Allowing Assets to be verified along a supply chain.
- Reducing the costs of verifying an Asset that relies on previously verified Asset by allowing the reuse of evidence and of verification results.

The modularization of verification processes is a common way of assessing complex, entangled Assets by leveraging previously verified Assets, such as in the context of the EUCS scheme or the AUDITOR data protection certification.

Modularization refers to a particular case, in which the Sub-Service (then called a base service) is itself a Software Asset that has been verified to be Gaia-X compliant. In such a case the Software Asset (or dependent service) relying on the base service can expect the verification of the controls related to the base service to be greatly simplified because they use the same verification framework and MVSC.

To be eligible for verification modularization, the base service shall satisfy controls for a specific Assurance Level at a level equal or greater than the level targeted by the dependent service. The base service shall provide a description of their contribution to the Gaia-X MVSC fulfilment of their dependent services, properly justified. This information can then be used by the CAB during verification. The CAB only needs to verify that this information has not been modified and if necessary that a subset has been properly selected and will focus on verifying that the remaining MVSC are fulfilled by the dependent service. Finally, note that a dependent service may use modularization with more than one base services.

6. Other Requirements

6.1 Persistence Layer / Data Storage

The OAW engine MUST process and store diverse data (refer to Section 3.3-3.4). In addition, The OAW engine MUST log each workflow activity (i.e., generate an audit trail) to enable third party auditing, including input data, data about processing activities, output data (e.g., results), corresponding timestamps and accountable users. The OAW engine MUST store these logs and all accreditation data (e.g., interim accreditation results, notes, assurance information) at least two times the validity periods of the Gaia-X compliance attestation (i.e., six years). Nevertheless, a persistence layer or data storage should not contradict the idea of Federated

Services. The OAW engine therefore MUST align with the general workflow engine descriptions of WP5 [WFE] and be open to any federated data storage solution.

Appendix A: Glossary

The glossary is part of the Gaia-X Technical Architecture Document [Gaia-X AD].

Appendix B: Overview GXFS Work Packages

The project "Gaia-X Federation Services" (GXFS) is an initiative funded by the German Federal Ministry of Economic Affairs and Energy (BMWi) to develop the first set of Gaia-X Federation Services, which form the technical basis for the operational implementation of Gaia-X.

The project is structured in five Working Groups, focusing on different functional areas as follows:

Work Package 1 (WP1): Identity & Trust

Identity &Trust covers authentication and authorization, credential management, decentral Identity management as well as the verification of analogue credentials.

Work Package 2 (WP2): Federated Catalogue

The Federated Catalogue constitutes the central repository for Gaia-X Self-Descriptions to enable the discovery and selection of Providers and their Service Offerings. The Self-Description as expression of properties and Claims of Participants and Assets represents a key element for transparency and trust in Gaia-X.

Work Package 3 (WP3): Sovereign Data Exchange

Data Sovereignty Services enable the sovereign data exchange of Participants by providing a Data Agreement Service and a Data Logging Service to enable the enforcement of Policies. Further, usage constraints for data exchange can be expressed by Provider Policies as part of the Self-Description

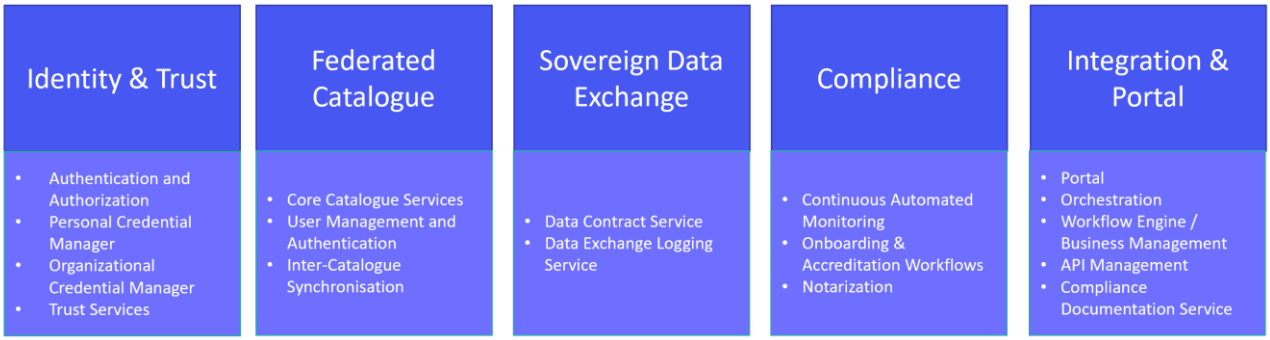
Work Package 4 (WP4): Compliance

Compliance includes mechanisms to ensure a Participant's adherence to the Policy Rules in areas such as security, privacy transparency and interoperability during onboarding and service delivery.

Work Package 5 (WP5): Portal & Integration

Gaia-X Portals and API will support onboarding and Accreditation of Participants, demonstrate service discovery, orchestration and provisioning of sample services.

All together the deliverables of the first GXFS project phase are specifications for 17 lots, that are being awarded in EU-wide tenders:



Further general information on the Federation Services can be found in [Gaia-X AD].