Specification of non-functional Requirements

for

Gaia-X Federation Services

Security and Privacy by Design NF.SPBD

Published by

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

Copyright

Table of Contents

List of Figures

List of Tables

1. Introduction

This document covers the following topics:

- Protection Profile
  Starting from the asset analysis for each Federation Services and their need of protection, Assurance Level will be derived which has to be fulfilled by each of the four services. The Assurance Level built the basis for the requirements defined during the Security and Privacy by Design life cycle.
- Security and Privacy by Design (SPBD)
  To ensure security and privacy as an integral part, each Federation Service must ensure security and privacy by design. This chapter explains the overall life cycle and how security and privacy need to be integrated into each life cycle step of a Federation Service.

1.1 Document Purpose

Aim of this document is to specify the security and privacy requirements to deliver and operate Gaia-X Federation Services [1].

Audience of this documentation are supplier and provider of Gaia-X Federation Services.

1.2 Product Scope

This document specifies the non-functional requirements each Gaia-X Federation Services must fulfill.

1.3 Definitions, Acronyms and Abbreviations

Federation Services
Federation Services are grouped into the four domains “Identity and Trust” (WP 1), “Federated Catalogue (Interoperability)” (WP 2), “Sovereign Data Exchange” (WP 3) and “Compliance” (WP 4). Further Details are described in [1].

Abbreviation	Term
AISBL	Association internationale sans but lucratif
BSI	Bundesamt für Sicherheit in der Informationstechnik
C5	Cloud Computing Compliance Control Catalogue
CIS	Center for Internet Security
DAST	Dynamic Application Security Testing
EUCS	European Cybersecurity Certification Scheme for Cloud Services
GDPR	General Data Protection Regulation
NIST	National Institute of Standards and Technology

PII	Personal Identifiable Information
SAST	Static Application Security Testing
SDLC	Software Development Life Cycle
SPBD	Security and Privacy by Design

***Table 1**: Definitions, Acronyms and Abbreviations*

1.4 References

[1] Gaia-X Architecture Document, Release 21.03;
Please refer to annex "Gaia-X_Architecture_Document_2103"

[2] Gaia-X: Policy Rules Document (PRD 21.04);
Please refer to annex "Gaia-X Policy & Rules Document 21.04"

[3] ENISA – Baseline Security Recommendations for IoT
https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

[4] ENISA - GOOD PRACTICES FOR SECURITY OF IOT; https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1

[5] Gaia-X Software Requirements Specification - Continuous Automated Monitoring
Please refer to annex "SRS_GXFS_CP_CAM"

[6] Gaia-X Software Requirements Specification – Compliance Documentation Service
Please refer to "SRS_GXFS_IP_CDS"

[7] ENISA EUCS Scheme; https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme

[8] BSI Federal Office for Information Security - BSI TR-02102 Cryptographic Mechanisms:
https://www.bsi.bund.de/EN/Service-Navi/Publications/TechnicalGuidelines/tr02102/BSITR02102.html

[9] CIS® – Center for Internet Security; https://www.cisecurity.org/ (different standards)

[10] NIST – Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
https://csrc.nist.gov/publications/detail/sp/800-175b/rev-1/final

[11] TeleTrust – Handreichung "Security by Design";
https://www.teletrust.de/fileadmin/user_upload/2020-TeleTrusT-Handreichung_Security_by_Design.pdf

[12] OWASP® – Open Web Application Security Project; https://owasp.org/

1.5 Document Overview

This document describes Security and Privacy by design requirements for Gaia-X Federation Services. It contains two chapters:

- Chapter 2 derives the protection level for each Federation Service by performing a protection analysis.
- Chapter 3 describes the Security and Privacy by design life cycle and defines general security and privacy requirements which are relevant for all Gaia-X Federation Services. As a result, all Federation Services specifications refer to this document. In case there are further Federation Service specific requirements, they will be documented in the corresponding specification.

1.6 Interaction with other Federation Services

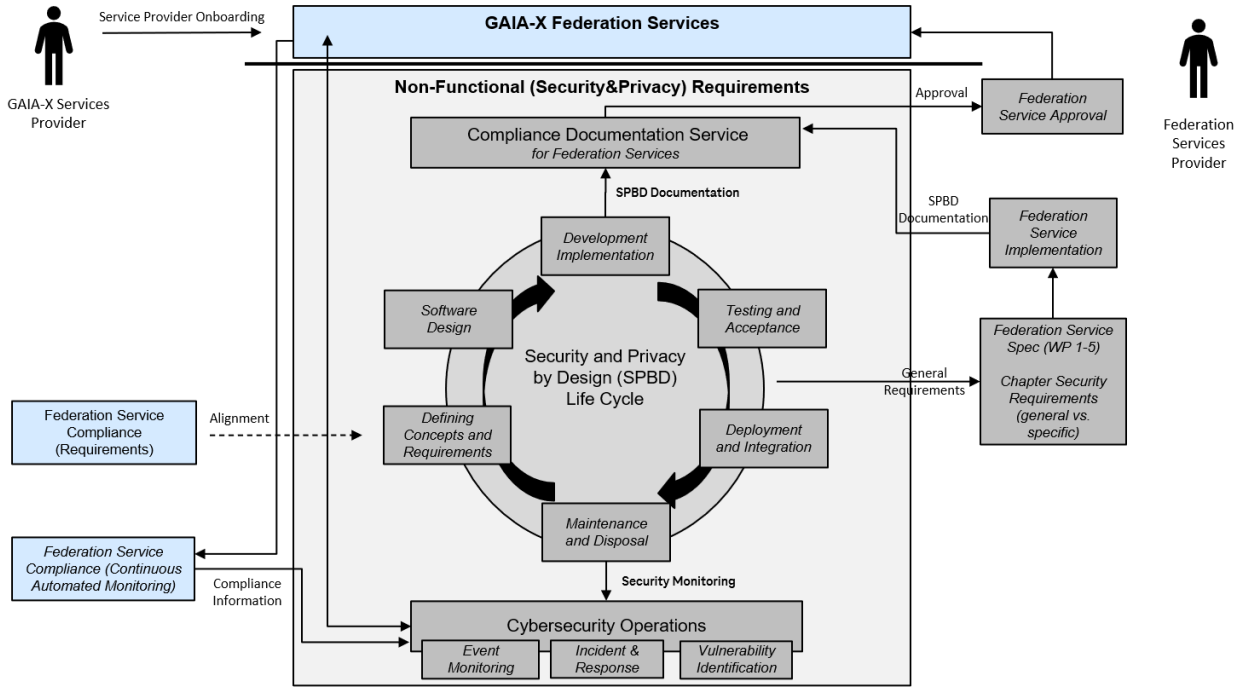

***Figure 1**: Interaction of Security and Privacy by design with other services*

Figure 1 describes the relation to other Federation Services and the interaction with the *Compliance Documentation Service* specified in [6].

This specification with the Security and Privacy by design life cycle defines the requirements for all Federation Services. The implementation of the life cycle will be documented in the *Compliance Documentation Service*.

2. Protection Profiles

Within the five domains of Federation Services, a set of technical components will be developed. Work package 1 addresses (1) a *Self Sovereign Identity* (SSI) *Service* to provide authentication and authorization facilities, (2) *Credential Management Services* which issues, manages and verifies credentials for Gaia-X participants (Natural persons as well as organizations), (3) a *Decentralized Identity and Trust Management Service* for identity handling as well as trust policy enforcement and management.
The F*ederated Catalogue* will be the result of work package 2. It has three main services, (1) a Catalogue *Query* to search for marketed assets, (2) a *Catalogue Management* for onboarding new providers and managing self-descriptions, and (3) a *Catalogue Synchronization* to synchronize between catalogues that might be eco-system specific.
Work package 3 focuses on creating an infrastructure for sovereign data exchanges and will build (1) a Data Contract Service that enables data transactions in a secure, trusted and auditable way and (2) a Data Exchange Logging Service.
Work package 4 will develop (1) a *Onboarding and Accreditation Workflow* to onboard new Gaia-X participants and accreditation of asset's compliance with Gaia-X principals, such as data protection and transparency, and (2) a *Continuous Automated Monitoring*, which automatically gathers and assess information about the compliance of Gaia-X services, with regards to the Gaia-X Policy of Rules and Architecture of Standards, and (3) a *Notarization Service* that has the task to verify "analogue" credentials and to map them to digital ones.

Finally, user a friendly *Portal*, a *Life Cycle Manager,* a *Workflow Engine* and an *API Framework* will be provided by work package 5 to tie all Federation Services together and support providers as well as consumers by offering and consuming services with Gaia-X.

Each technical component will store, process or publish one or more assets implying requirements on the security aspects integrity, confidentiality and non-repudiation. These assets as well as their protection profile will be explained in more details in the following sections.

2.1 Assets

2.1.1 Identity & Trust-Related Assets

Identities
Identities are the basis for verifying the authenticity of Gaia-X entities. Identities may contain high-sensitive data, e.g. in case of natural or legal persons, personal data such as addresses or birthdates. According to GDPR, this information is confidential, and the Federation Services have to ensure, that they are not modified in an unauthorized and inexplicable way.

Verified (Digital) and Analogues Credentials
Gaia-X entities use credentials for authentication and authorization purposes. Similar to identities, credentials regardless of their nature (digital or analogues) may contain sensitive data, too. For example,

both a digital diploma issued by a university as well as a printed copy of a driving licence contain information about birthdate and age, which must not be publicly readable. Hence, Federation Services have to accomplish confidentiality, integrity and non-repudiation with respect to analogue and digital credentials.

Access Policies

Each technical component will provide an API to communicate with. Whereas some API functions are available to all Gaia-X entities, there will be functions which are limited to a restricted set of roles. E.g. a service's self description must only be published, modified and deleted by the owner of the appropriate service. Access policies define which role is allowed to perform which operation on a Federation Service. And each Federation Service has to have access policies.

Access policies have to ensure integrity as well as non-repudiation as they are an important part of access control mechanisms. However, there is no need for confidentiality as long as they do not link any identity information, but e.g. just roles.

2.1.2 Service-Related Assets

Service Self -Descriptions and their Schema

Within Gaia-X, service self-descriptions detail any information a potential consumer may need to know about a service's usage, such as service's provider, input and output data or billing information. The structure of this information is described by a well-defined schema. Both service self-descriptions and its schema are publicly visible and can be read. Thus, there is no need for confidentiality, but for integrity and non-repudiation. Only the provider of a service is entitled to create, modify or delete a service's self-description.

Service Access Policies

Service access policies describe the term of use of a service. Basic parts answer the questions who is allowed to use the service, which restrictions have to be considered by both consumer and provider and when does the service usage ends. Terms of use should be free of sensitive data and visible for everyone. Service access policies may be part of services' self-descriptions. Thus, integrity and non-repudiation are relevant in this case.

Service

A service is a software or hardware artefact, that is provided, selected and consumed with the help of Gaia-X Federation Services. It is hard to define requirements on the protection profile of services in general, as such requirements depend highly on the kind of service that is provided. But at least for software services, Federation Services have to ensure, that the software provider and consumer had entered a contract for, is the same as the software, which was deployed. Hence integrity checks are mandatory.

2.1.3 Data-Related Assets

Data Self-Descriptions and their Schema

Data self-descriptions and their schema are equivalent to service self-descriptions and their schema. Instead of defining the terms of use of a service, data self-descriptions detail meta information about the data, that is published, shared, processed and consumed within the international data space. Hence, data self-

descriptions and their schema pose the same requirements on protection profile, namely integrity and non-repudiation.

Data Access Policies
Data access policies are the counterpart to service access policies. They detail the terms of use for data, such as who is authorized to access specific data or within which time frame data has to be deleted by the consumer. Consequently, security goals of service access policies can be assigned to data access policies, too. Similar to service access policies, data access policies may be a part data self-descriptions.

Data
Data are core assets in Gaia-X. Every service is doing one or more of the following data operations: consuming, processing or publishing. With data access policies, a data owner describes the security requirements for his data. And, whereas confidentiality and non-reputation is up to the definition of the data owner, integrity fits to all kinds of data.

2.1.4 Compliance-Related Assets

Compliance Policies
Work package 4 focusses on compliance of Gaia-X participants and services. Therefore, a set of compliance rules must be defined. With regards to transparency, these rules should be public readable and ideally signed by an authorized entity.

Onboarding Data
Onboarding of new Gaia-X participants is the task of the Onboarding and Accreditation Workflow. This task ends in some files, which document the process. Onboarding files may contain sensitive data, that organisations do not want to be public readable. Hence, this asset puts requirements on confidentiality, integrity and non-reputation.

Monitoring Data
Compliance monitoring will output Gaia-X participant's and service's compliance level within a specific time period. These monitoring data may be high-sensitive and have to be considered as confidential. And, as participants may take legal steps if the contractually agreed compliance level is not given, monitoring data must also be of integrity and non-repudiation.

2.1.5 Summary

Table 2 summarizes the protection profile of each asset that is created, stored and processed by Gaia-X Federation Services. A closer look into table 2, integrity and non-reputation are important for each asset. In addition to it, there are assets that have to be confidential.

2.2 Assurance Level

The last section deduced important assets and their requirements on the security aspects integrity, confidentiality and non-reputation. This is a prerequisite for the definition of the protection profile of the work packages' individual technical components. Therefore, the EUCS candidate scheme (European Cybersecurity Certification Scheme for Cloud Services) [7] will be referenced. The EUCS already defines security objectives of cloud services in a fine granular manner and groups them into three Assurance Levels: basic, substantial and high. All three levels require "to protect stored, transmitted or otherwise processed data against accidental or unauthorised[1]" modification (integrity) and "make it possible to check which data … have been accessed, used or otherwise processed, at what times and by whom[2]" (non-reputation). In contrast to that, the Assurance Levels basic, substantial and high differ in the level of confidentiality. Cloud services with basic level store, process or transmit public data, such as web sites. Cloud services with substantial level come in touch with sensitive data, such as personal data or e-mails, and have to keep them confidential. Cloud services at level high, work with critical data, such as company secrets or digital identities. Cloud services like that must fulfil the highest demand to confidentiality.

Asset	Confidentiality	Integrity	Non-Repudiation
Identities	x	x	x
Verified Credentials	x	x	x
Analogues Credentials	x	x	x
Access Policies		x	x
Service Self-Description Schema		x	x
Service Self-Description		x	x
Service Access Policies		x	x
Data Self-Description Schema		x	x
Service		x	x
Data Self-Descriptions		x	x
Data Access Policies		x	x
Data	(x)	x	x
Compliance Policies		x	x
Onboarding Data	x	x	x
Monitoring Data	x	x	x

***Table 2**: Summary of protection goals of assets of Federation Services*

The following section will analyse each technical component as defined at the beginning of chapter 2. The goal is to figure out which assets of chapter 2.1 are processed, stored or transmitted by each component. Table 3 summarizes this assignment of assets to technical components. Based on this information the

[1] Artikel 51.a EUCS, https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme
[2] Artikel 51.f EUCS, https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme

component will tagged with the EUCS Assurance Level that fits most, with regard to the assets' protection profile. The relationship between technical component and Assurance Level is shown in Table 4.

2.2.1 Work Package 1

The technical components of work package 1, namely Self Sovereign Identity Service (Authentication/Authorization), Credential Management Services (Personal Credential Manager (PCM) and Organization Credential Manager (OCM)), Decentralized Identity and Trust Management Service are key aspects to achieve digital and data sovereignty in Gaia-X. These Federation Services handles the entire life cycle and the verification of identities and credentials of Gaia-X entities. Furthermore, the technical components of work package 1 form the trust anchor, the functionality of security related operations of any other Federation Services or Gaia-X entity is based on. Thus, the technical services of work package 1 should have Assurance Level high.

2.2.2 Work Package 2

Work packages 2 builds components to realize the federated catalogue consisting of a Catalogue Query, a Catalogue Management and a Inter-Catalogue Synchronization. All three services process, store and publish service and data self-descriptions and their schemas. All four assets are publicly available and require integrity and non-reputation, only. In that case, it is sufficient to design and implement work package 2 artefacts with Assurance Level basic.
Table 2 shows three other assets, work package 2 is related to identities, credentials and access policies. Access policies have the same protection profile as self-descriptions and their corresponding schemas. Hence, Assurance Level basic fits. However, identities and credentials must be considered as high confidential. In contrast to artefacts of work packages 1 and according to the concept of Self Sovereign Identity (SSI), work package 2 does not operate on foreign identities and credentials, but just stores its own identities and credentials, used to authenticate and authorise itself at other Gaia-X entities. This is an aspect, all technical components have in common. Instead of assigning Assurance Level high to all Federation Services, making design and implementation more difficult, Assurance Level high is just assigned to a secure sub-component, called wallet. A wallet keeps component's identities and credentials safe and must fulfil security requirements of Assurance Level high.

2.2.3 Work Package 3

The scope of work package 3 is to implement an infrastructure for sovereign data exchange. This infrastructure is grounded on a Data Contract Service and a Data Exchange Logging Service. The Data Contract Service enables data transactions in a secure, trusted and auditable way. It offers interfaces for negotiation of data contracts detailing the agreed terms and usage policies for a planned data exchange. The Data Exchange Logging Service logs those data transactions and is able to provide evidence that data has been submitted and received.

2.2.4 Work Package 4

Work package 4 builds three technical components, namely an Onboarding and Accreditation Workflow, a Continuous Automated Monitoring as well as a Notarization Service. All components work with assets, that are to be considered as confidential. The Onboarding and Accreditation Workflow outputs sensible onboarding data, whereas Continuous Automated Monitoring generates monitoring data. The notarization service is required to enable trusted issuers to issue verifiable credentials.
As monitoring and notarization data are sensible, both are classified with Assurance Level high. Onboarding data are sensible, but not critical. Therefore, the Assurance Level substantial may be sufficient for the technical component.

2.2.5 Work Package 5

The focus of work package 5 is to provide Portal and integration services. The integration services are divided in a Life Cycle Manager, Workflow Engine and API Framework, which do not work with confidential assets and can be designed and implemented at a basic Assurance Level.
The Portal ties all Federation Services together and provides a user-friendly interface to communicate with Gaia-X. It acts as a proxy and may transfer sensible data between Federation Services and Gaia-X participants. Ideally, it just forwards data and does not process it. In that case, the Portal can be evaluated with Assurance Level basic and uses end-to-end encryption to ensure confidentiality of the forwarded messages. If it turns out, that end-to-end-encryption is not feasible in all places, the Portal must be reassigned to Assurance Level high. The Portal will pose a popular target for cyber attacks, otherwise.

WP	Technical Component	Identities	Verified Credentials	Analogues Credentials	Access Polices	Service Description Schema	Service Description	Service Policies	Service	Data Self-Description Schema	Data Self-Description	Data Access Policies	Data	Compliance Policies	Onboarding Data	Monitoring Data
1	Self Sovereign Identity Service (Authentication/Authorization)	X	x		x											
	Credential Management Services (PCM & OCM)	X	x		x											
	Decentralized Identity and Trust Management Service	X	x		x											
2	Catalogue Query	X	x		x	x	x			x	x					
	Catalogue Management	X	x		x	x	x			x	x					
	Inter-Catalogue Synchronization	X	x		x	x	x			x	x					
3	Data Contract Service	X	x		x		x			x	x	x	x			
	Data Logging Service	X	x		x		x				x	x	x			
4	Onboarding and Accreditation Workflow	X	x		x									x	x	
	Continuous Automated Monitoring	X	x		x									x	x	x
	Notarization Service	X	x	x	x											
5	Portal	X	x		x											

	Life Cycle Manager	X	x		x	x	x	x	x							
	Workflow Engine	X	x		x	x	x	x	x							
	API Framework	X	x		x											

***Table 3**: Assignment of assets to technical components of Federation Services*

WP	Technical Component	Assurance Level
1	Self Sovereign Identity Service (Authentication/Authorization)	high
	Credential Management Services (PCM & OCM)	high
	Decentralized Identity and Trust Management Service	high
2	Catalogue Query	basic
	Catalogue Management	basic
	Inter-Catalogue Synchronization	basic
3	Data Contract Service	high
	Data Logging Service	high
4	Onboarding and Accreditation Workflow	substantial
	Continuous Automated Monitoring	high
	Notarization Service	high
5	Portal	basic (high)
	Life Cycle Manager	basic
	Workflow Engine	basic
	API Framework	basic

***Table 4**: Assurance Level of Federation Services*

3. Security and Privacy by Design

This chapter describes how security and privacy by design shall be fulfilled by Federation Services.

3.1 Overview

To ensure security and privacy as an integral part, each Federation Service must ensure security and privacy by design. This chapter explains the overall life cycle and how security and privacy need to be integrated into each life cycle step of a Federation Service.

3.2 Definition SPBD

Security and privacy by design (SPBD) means that security and privacy is ensured through the whole life cycle of the product, service or solution [1].

As stated by ENISA [3] it is important to mention, when referring to security and privacy by design, the security measures should reflect the particularities and the context in which the product, service or solution will be deployed. The security and privacy measures mentioned in this document reflect the security and privacy by design principals for Gaia-X Federation Services. It can be adopted by Gaia-X services as well – nevertheless this is not the scope of this document.

3.3 Integration of SPBD into the development life cycle

The aim of this chapter is to define a Secure Service Development Life Cycle (SSDLC) and incorporate relevant processes in their operations.

Making use of SSDLC principles is an effective and proactive means to avoid vulnerabilities in cloud services and thus assist in developing software applications and services in a secure manner [4].

Based on the outcome of [4] a Software Development Life Cycle (SDLC) comprises up to six phases, as shown in Figure 2.
With respect to modern development cycles like the DevSecOps for cloud-native environments (see *Figure 4*), it should be taken into account that activities of the phases *Development & Implementation*, *Testing and Acceptance* and *Deployment and Integration* take place in every (development) cycle in a repeating sequence and not only as one separated, completed phase (see *Figure 3*).
Independent on which development and operation model is used by a Federation Service provider, the following described life cycle requirements must be applied accordingly.

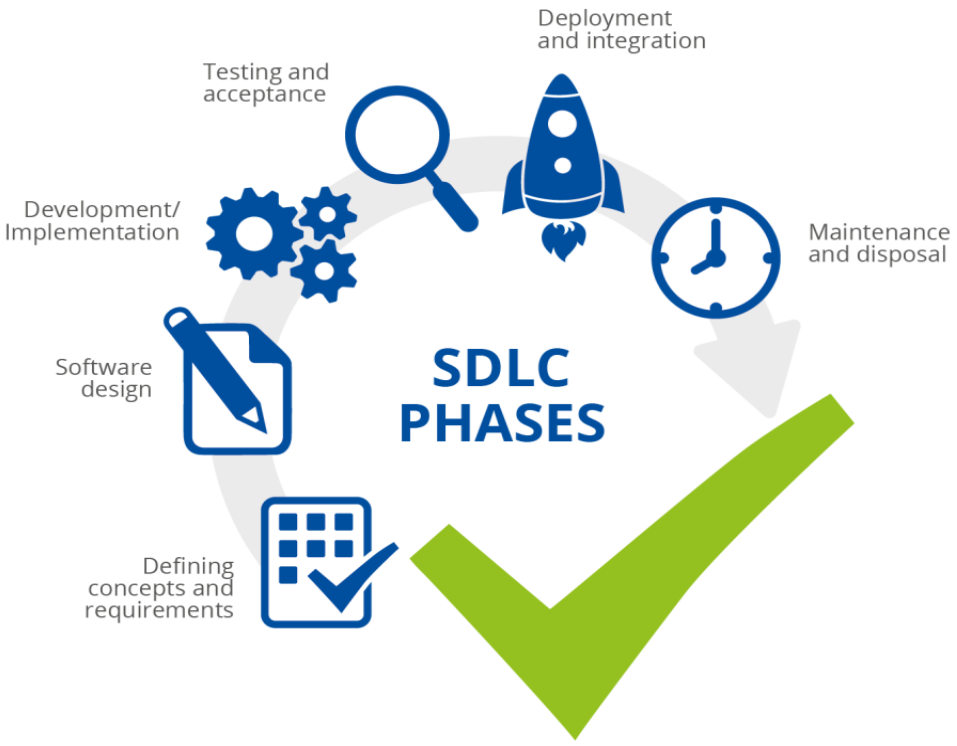

***Figure 2**: Software Development Life Cycle (SDLC) phases (from [3])*

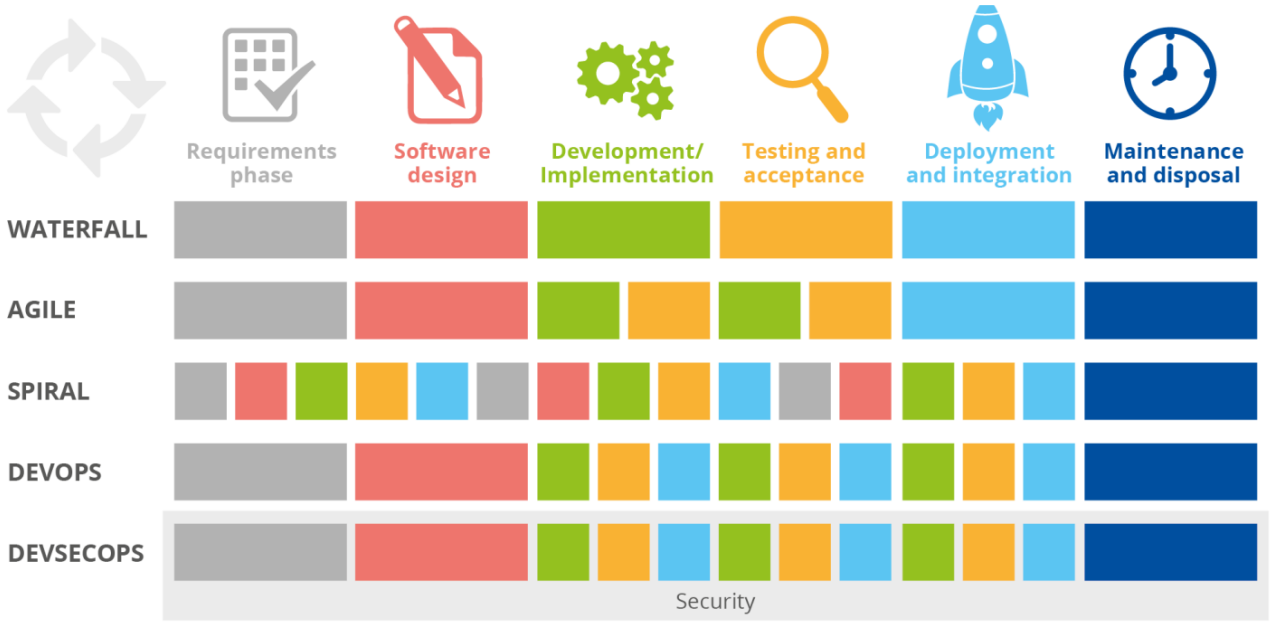

***Figure 3**: Overview of Software Development Life Cycle (SDLC) models from [3]*

3.4 SDLC of Gaia-X Federation Services to ensure SPBD

The ENISA documentation [4] has already described a Software Development Life Cycle for IoT products. Based on this description, the following chapters are structured and extended by cloud-related and Gaia-X Federation Services specific extensions.

Although the following chapters describe the Service (or Software) Development Life Cycle (SDLC), security and privacy are fundamental principles across all six phases of the life cycle.
To ensure, that these principals are covered appropriately, security gates shall be defined as described in chapter 3.5.

3.4.1 Defining Concepts and Requirements

As already describe by ENISA [3], requirements are the foundation for all that is to follow in the development cycle. During this phase all types of requirements, i.e. business, functional and non-functional requirements of the development objects are being defined. These requirements reflect the intended use of the object and will be translated to specifications that will guide design, development and maintenance/deployment decisions at a later stage. Therefore, it is essential to embed security and privacy from this first phase onward to ensure security by design principles as well as privacy by design principals.

Types of requirements and their coverage by Gaia-X

- Business / functional requirements / Use Cases:
  These requirements are defined individually by the specification of each Federation Service and therefore out of scope of this specification. The Federation Services are
  - Identity and Trust
  - Federated Catalogue
  - Sovereign Data Exchange
  - Compliance
  - Federation Service Portal
- Legal and governmental, e.g. General Data Protection Regulation (GDPR), etc. (partially in scope):
  This specification only considers the GDPR as overall legal data protection and privacy requirement for the whole EU. Other legal or governmental requirements are out of scope.
- Regulatory, e.g. processing Payment Card Industry (PCI) data, etc. (out of scope):
  No regulatory requirements are considered in this specification. Therefore, the Gaia-X Federation Services does not fulfill regulatory requirements by default.
- Non-functional requirements, i.e. security and privacy requirements (in scope):
  Scope of this specification are the requirements related to security and privacy. An overview of standards is given by *Table 7*. The applicability of the resulting requirements to Gaia-X Federation Services are described in the following.

Derivation, structuring and justification of Gaia-X security and privacy requirements.
The requirements in this specification are derived from and structured by the "European Union Agency for Cybersecurity (EUCS) – Cloud Services Scheme" [7]. Where necessary, further details from other security standards or the GDPR will be added.

As justification for adequacy and completeness a protection profile described in chapter 2 was done.

Cybersecurity Requirements
The EUCS [7] defines 20 control categories. The list below gives an overview of these controls, shows the applicability to Gaia-X Federation Services and lists additional standards if required for further detailing.

Beside EUCS [7] the Federation Services and their operation must be in compliance with the policies and rules defined by Gaia-X in [2].

The Federation Services will be listed in the following abbreviated way:

- Identity and Trust: Identity
- Federated Catalogue: Catalogue
- Sovereign Data Exchange: Data Exchange
- Compliance: Compliance
- Federation Service Portal: Portal

Services are operated by so called "Operating Entities" (like infrastructure or platform provider) which develop and/or operate related services.

	EUCS controls	Control Description	Relevance for Gaia-X Federation Services	Affected Gaia-X Federation Service	Reference to further details
A.1	Organization of Information Security	Plan, implement, maintain and continuously improve the information security framework within the organization.	Relevance for the organization of the Federation Service Provider *(Information Security Management topics)*	-	ISO 27001
A.2	Information Security Policies	Provide a global information security policy, derived into policies and procedures regarding security	Relevance for the organization of the Federation Service Provider	-	ISO 27001

		requirements and to support business requirements.	*(Information Security Management topics)*		
A.3	Risk Management	Ensure that risks related to information security are properly identified, assessed, and treated, and that the residual risk is acceptable to the CSP	Relevance for the organization of the Federation Service Provider *(Information Security Management topics)*	-	ISO 27001 ISO 27005
A.4	Human Resources	Ensure that employees understand their responsibilities, are aware of their responsibilities with regard to information security, and that the organisation's assets are protected in the event of changes in responsibilities or termination.	Relevance for the organization of the Federation Service Provider *(Information Security Management topics)*	-	ISO 27001
A.5	Asset Management	Identify the organization's own assets and ensure an appropriate level of protection throughout their life cycle.	Relevance for the operation of the Federation Service *(IT Operation topics – basis for cybersecurity operation)*	• *Identity* • *Catalogue* • *Data Exchange* • *Compliance* • *Portal*	ISO 27001
A.6	Physical Security	Prevent unauthorized physical access and protect against theft, damage, loss and outage of operations.	Relevance for the Infrastructure Provider only, not for the Federation Service Provider *(Infrastructure topics)*	-	ISO 27001 SOC (Service Organization Controls)

A.7	Operational Security	Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.	Relevance for the operation of the Federation Services	• *Identity* • *Catalogue* • *Data Exchange* • *Compliance* • *Portal*	ISO 27001 + complementary standards (see Table 7)
A.8	Identity, Authentication, and Access Control Management	Limit access to information and information processing facilities	Relevance for the operation of the Federation Services	• *Identity* • *Catalogue* • *Data Exchange* • *Compliance* • *Portal*	ISO 27001 + complementary standards (see Table 7)
A.9	Cryptography and Key Management	Ensure appropriate and effective use of cryptography to protect the confidentiality, authenticity or integrity of information.	Relevance for the operation and data exchange of the Federation Services	• *Identity*[3] • *Catalogue*[4] • *Data Exchange*[5] • *Compliance* • *Portal*	See Table 7
A.10	Communication Security	Ensure the protection of information in networks and the corresponding information processing systems.	Relevance for the data exchange of the Federation Services	• *Identity* • *Catalogue* • *Data Exchange* • *Compliance* • *Portal*	See Table 7
A.11	Portability and Interoperability	Enable the ability to access the cloud service via other cloud services or IT systems of the cloud customers, to obtain the stored data at the end of the contractual relationship and to securely delete it from the Cloud Service Provider	Relevance for all Federation Services	• *Identity* • *Catalogue* • *Data Exchange* • *Compliance* • *Portal*	C5

[3] Management of user and service credentials
[4] The Federation Service Catalogue includes only public data
[5] Credentials / Token for secure data exchange

A.12	Change and Configuration Management	Ensure that changes and configuration actions to information systems guarantee the security of the delivered cloud service.	Relevance for the operation of the Federation Services	• *Identity* • *Catalogue* • *Data Exchange* • *Compliance* • *Portal*	ISO 27001
A.13	Development of Information Systems	Ensure information security in the development cycle of information systems.	Relevance for the operation of the Federation Services	• *Identity* • *Catalogue* • *Data Exchange* • *Compliance* • *Portal*	see chapter 3.4.2 ff.
A.14	Procurement Management	Ensure the protection of information that suppliers of the CSP can access and monitor the agreed services and security requirements.	Relevance for the operation of the Federation Services	• *Identity* • *Catalogue* • *Data Exchange* • *Compliance* • *Portal*	ISO 27001
A.15	Incident Management	Ensure a consistent and comprehensive approach to the capture, assessment, communication and escalation of security incidents.	Relevance for the operation of the Federation Services	• *Identity* • *Catalogue* • *Data Exchange* • *Compliance* • *Portal*	ISO 27001
A.16	Business Continuity	Plan, implement, maintain and test procedures and measures for business continuity and emergency management.	Relevance for the operation of the Federation Services	• *Identity* • *Catalogue* • *Data Exchange* • *Compliance* • *Portal*	ISO 22301
A.17	Compliance	Avoid non-compliance with legal, regulatory, self-imposed or contractual information security and compliance requirements.	Relevance for the operation of the Federation Services	• *Identity* • *Catalogue* • *Data Exchange* • *Compliance* • *Portal*	Gaia-X Continuous Automated Monitoring [5]
A.18	User Documentation	Provides up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers.	Relevance for the documentation of the Federation Services	• *Identity* • *Catalogue* • *Data Exchange* • *Compliance* • *Portal*	Gaia-X Compliance Documentation Service [6]
A.19	Dealing with Investigation	Ensure appropriate handling of government investigation	Relevance for the organization of the		ISO 27001

	Requests from Government Agencies	requests for legal review, information to cloud customers, and limitation of access to or disclosure of data.	Federation Service Provider *(Information Security Management topics)*		
A.20	Product Safety and Security	Provide appropriate mechanisms for cloud customers.	Relevance for the Infrastructure Provider only.		

***Table 5**: Overview of EUCS Control and their assignment to Federation Services*

A further outcome of the protection profile in chapter 2 is the assignment of an Assurance Level to each of the Gaia-X Federation Services. Assurance Levels are defined in [1]. Table 6 assigns each Federation Service the required Assurance Level.

Federation Service	Assurance Level
Identity and Trust	High
Federated Catalogue	Basic
Sovereign Data Exchange	High
Compliance	Substantial/High
Federation Service Portal	Basic

***Table 6**: Assignment of Assurance Level to Federation Services*

Although the EUCS controls considering all security aspects, the requirements are not always described in sufficient detail. Therefore, the following description gives an overview of standards or guidelines which shall be used for detailing.

Organization	Standards / Guidelines	Topics related to EUCS Control
BSI [8]	BSI Technical Guidelines series[6]: technical recommendations	A.7 – Operational Security (System Hardening)
	TR-02102 Cryptographic Mechanisms (2020)	A.9 – Cryptography and Key Management
OWASP [12]	OWASP Top 10 2017: awareness about the most critical risks to web applications	
	OWASP Cheat Sheet series good practice guides for application developers, e.g. XSS Prevention, Injection Prevention, etc.	A.7 – Operational Security (System Hardening)
CIS [9]	CIS Benchmark series guidelines to safeguard operating systems, software and networks.	A.7 – Operational Security (System Hardening)
TeleTrusT [11]	Guideline “State of the art” in IT security[11] (2021)	A.7 – Operational Security A.8 – Identity, Authentication, and Access Control Management A.9 – Cryptography and Key Management
NIST [10]	SP 800-175B Rev. 1 (2020) Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms	A.9 – Cryptography and Key Management

[6] https://www.bsi.bund.de/EN/Service-Navi/Publications/TechnicalGuidelines/techniguidelines.html

Product Vendors	Vendor's Security Best Practices	A.7 – Operational Security (System Hardening)

***Table 7**: Overview Security Standards for detailling EUCS*

Privacy Requirements

In case of processing of personal identifiable information (PII) all Federation Services must be operated according to the EU GDPR by fulfilling the relevant acknowledged criteria. For further details see [2].

Deliverables[7]

Attestation of fulfilment of the security (EUCS) and privacy (GDPR) requirement according to the assigned Assurance Level of the Federation Service.

3.4.2 Software Design

During the software design phase, the service architecture and the design of the service solution are created. This phase involves the creation of a set of documents that describe how the business, functional and non-functional requirements will be translated to system specifications and essentially how the Gaia-X Federation Services will work.
It is crucial to have a good documentation and a documentation management system that supports the SDLC process to make it understandable, traceable, and subject to monitoring and auditing [4].

Gaia-X Federation Services documentation

For the Federation Services the following documents are defined as mandatory:

- Service Description / Specification
  - understand the service functionality, architecture, implementation, and interoperation/communication inside a Federation Service, with other Federation Services as well as outside Gaia-X.
- Cybersecurity Documentation
  - Description of implementation of the relevant security requirements, i.e. security measures[8]
  - Description of fulfillment level (basic, substantial, high)
  - Documentation of remaining risks (e.g. in case when a Federation Services specification provides for the use of a framework, which however contradicts the requirements of the EUCS)
- Data Privacy Documentation
  - Documentation of used personally identifiable information (PII) by using Data Field Catalogs and the purpose of processing,
  - Description of implementation of the relevant privacy requirements, i.e. privacy measures
- Authorization Concept

[7] The following deliverables must be provided as proof of compliance with the security and privacy by design requirements.
[8] Security and privacy measures can be documented in one central documentation.

    - Description of roles, rights and the process how these roles and rights will be assigned to and revoked from user.
- Source Code
    - Reference to the repository with the code (Gaia-X repository)
        - Repository must be accessible for auditors.
        - Builds must be reproducible.
- Business/Service Continuation Plan / Emergency Plan / Disaster Recovery Plan
    - Description how the Federation Service will come back to operation in case of emergency.
- Certification / Attestation
    - Attestation that the Federation Service fulfills all necessary requirements.
- Threat Modeling: verify / update the existing threat model given by Gaia-X in chapter 2.

It is important, that the specification meet all the requirements - according to the Assurance Level - as defined in the previous phase.

Gaia-X documentation management system
The above defined documents must be available for Gaia-X AISBL at any time. Therefore, a documentation management system for Federation Services will be established by or under the responsibility of Gaia-X AISBL. The documentation management system is described in [6].

Deliverables
- Federation Services documentation as defined above.

3.4.3 Development and Implementation

In the development and implementation phase, specifications and service design diagrams written in an appropriate notation are transposed into code. Therefore, what is defined in the two previous phases plays a crucial role in the successful execution of the development process. The foundation of Gaia-X secure Federation Services development relies on secure code. Code should be built, tested, integrated, maintained, and updated with security aspects in mind [4].

To ensure information security in the development cycle of each service the following requirements must be fulfilled:

- **Development and Implementation Policy**
  A policy must be available defining technical and organizational measures for the secure development of a Federation Service throughout its life cycle ([7] - DEV-01).
  The policy shall cover the following aspects ([7] - DEV-01 - DEV-07):
    - availability of secure development environments with separation from test and production environments ([7] - DEV-02 - DEV-04)
    - appropriate documentation and testing of security features ([7] - DEV-05)
    - identification of vulnerabilities introduced during the development process ([7] - DEV-06).

- aspects of outsourcing of development activities ([7] - DEV-07)
- security related trainings required for developers ([7] - HR-04)

- **Performing of security tests and analyzing of security information**
  Different security tests must be carried out during the development and implementation phase. Chapter 3.4.4. gives an overview of which tests are required in SDLC phases.

Deliverables:

- Policies of how security is ensured during development process.
- Test results of security testing

3.4.4 Testing and Acceptance

The testing and acceptance phase involves all necessary steps to verify that the developed software actually meets the identified requirements and design principles of the previous phases. For this reason, a variety of tests (each serving a different purpose) are performed on the software. These tests may be automated or manual, and both the source code (static analysis) and the running software (dynamic analysis) need to be checked [4].

With respect to modern development methods like the DevSecOps model, and to ensure that security and privacy is an integral part of the development process, testing take place in different phases of the SDLC or at different steps of the DevSecOps model.
Therefore, the testing activities shall take place during *Development & Implementation*, *Deployment & Integration* as well as during the *Operations* phase. With regard to the Continuous Integration / Continuous Delivery (CI/CD) process model (Figure 4), testing shall take place during the integration as well as the deployment pipeline.

Wherever possible, perform automated testing to ensure consistency and efficiency.

Planning security tests

Policies and procedures are required to ensure the timely identification and addressing of vulnerabilities[9]. The following aspects must be covered:

- frequency of tests (regular, continuous, event driven)
- scope of tests
    - Code Testing
    - Vulnerability Scanning
    - Penetration Testing
    - Compliance Testing
- test types, test environments and test tools (e.g. on- vs. offsite tests, tests in test vs. production environments, integration of security tools into build processes)
- documentation of test results (e.g. automated generation and delivery of test reports as required documents for the *Compliance Documentation Service* [6]
- remediation of test findings

[9] See [7] OPS-17 MANAGING VULNERABILITIES, MALFUNCTIONS AND ERRORS – POLICIES

Performing security tests

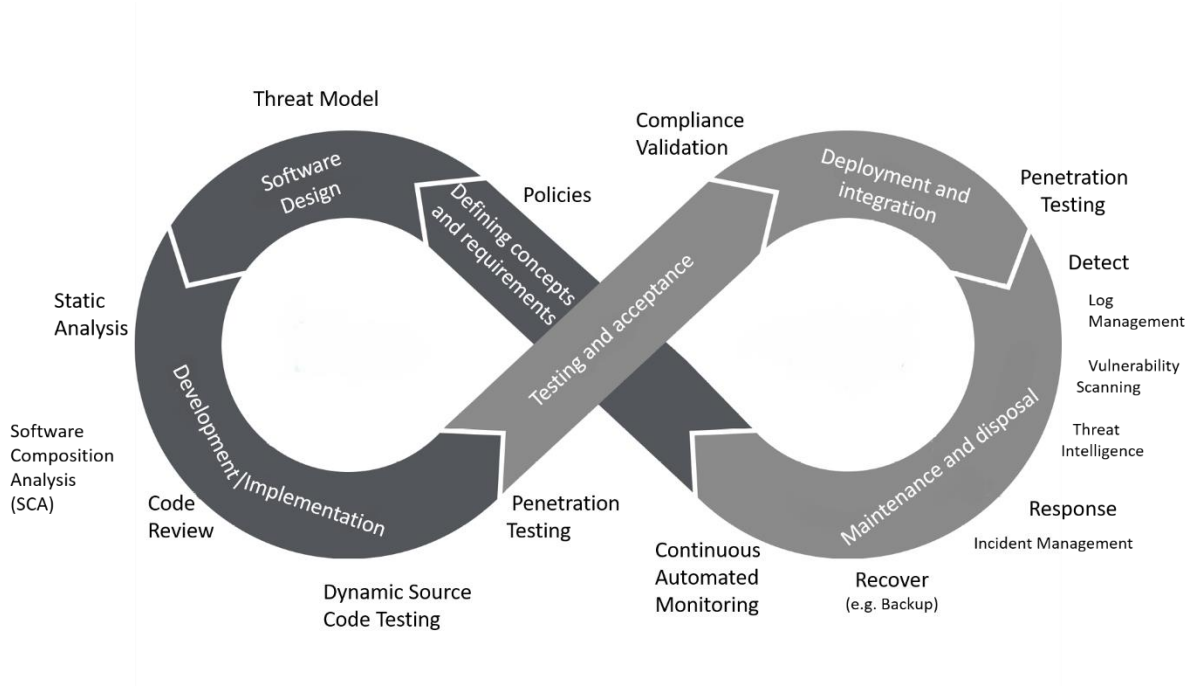

***Figure 4**: DevSecOps life cycle for Federation Services*

Figure 4 integrates the phases of the Software Development Life Cycle (SDLC) from chapter 3.3 into the DevOps cycle to give a better understanding of the required types of testing in the different phases.
Depending on the life cycle phase and the situation, appropriate tests must be performed for identifying vulnerabilities[10].

- Development/build phase
  - Human-based code review
    - Peer review of code through different developers and code signoff shall be performed.
  - Tool based source code review.
    - Automatic tests must be performed to detect secrets such as API keys, private crypto keys etc. in the source code or packaged applications (e.g. container).
    - Software composition analysis (SCA) must be performed to ensure that libraries, dependencies, and other 3rd party artifacts, is used to properly identify, document and check (security & software license compliance) the code base.
    - Static source code testing (SAST) must be integrated into the development cycle (ideally in the CI/CD pipeline) and code is mark non-compliant if it fails automatic checks (build fail in case of non-compliance).

[10] See [7] DEV-06 IDENTIFICATION OF VULNERABILITIES OF THE CLOUD SERVICE

        - Dynamic source code testing (DAST) tools shall be included into the development process (or CI/CD pipeline) or may be executed as part of the penetration test.
    - Tool based vulnerability analysis
        - Any software dependency that are necessary to run the code must be check for vulnerabilities. This includes executables, library, container base images and overlay files as well as other dependencies or artifacts.
    - Configuration Compliance
        - Configuration of software used must be hardened based on best practice requirements (such as CIS). The correct implementation of these hardening requirements needs to be (automatically) checked.
    - Security (Unit) Tests
        - Security function/controls used in the code (e.g. authentication) must be verified with test cases. Tests should be integrated into automatic testing wherever possible. New test cases are developed if new security controls are integrated.
    - Reporting
        - The execution and results of all security tests must be documented and/or logged. In case of follow up activities (e.g. in case of a failed security check), these activities as well as the outcome is also documented. It is ensured, that all security deviations are properly and timely addressed, this also includes documentation of false positives or "won't fix" items (incl. their justification). Reports, test concepts and individual test descriptions are available to Gaia-X on request (incl. auditing purposes to ensure good security practices).

- Test phase
    - Penetration tests must be performed as followed (see also [7] OPS-19.2 - 6)
      In contrast to vulnerability scans, penetration tests are deeper and more specific. Beside generic automated tests (used by vulnerability scanners) the penetration tester must also take into consideration Federation Service specific test use cases. Where vulnerability scans for e.g. missing patches, a penetration test tries to exploit known vulnerabilities to start a deeper investigation with the aim to identify further weaknesses of the service.
        - Testing:
            - A penetration test must be performed before the initial go live of the Federation Service. This test is mandatory to get the service approval.
            - In case of major service updates further penetration tests shall be performed.
            - The penetration tests should focus on aspects not covered by (automatic) testing during development, such as business logic flaws.
        - Report:
            - The penetration test report must be delivered to the responsible entity.

The Software Maintenance phase as well as the operations phase run in parallel during the operational lifetime of a Gaia-X application component. However, since they are often with different entities, the both phases are listed separately.

- Software Maintenance phase (Software Developer)
    - Vulnerability analysis must be performed (see description above).

- Operations phase (Application Operation)
    - Vulnerability scanning
        - Vulnerability scans are automated tests scanning for e.g. missing patches or unsecure configuration settings like week encryption protocols or missing 2-Factor Authentication.
        - Scanning:
            - Infrastructure components and software (container) must be scanned during runtime – after the build phase – for known vulnerabilities.
            - Scanning must be performed continuously to identify vulnerabilities immediately after their occurrence or publication (e.g. announcement by a vender and integration into the vulnerability database of a vulnerability scan tool). Continuously means that these scans must be performed at least daily.
    - Configuration Compliance
        - During the operations phase configuration compliance must be continuously verified. As an alternatively checks can be performed directly if a change is detected (event-driven checks). The Federation Service “Continuous Automated Monitoring” [5] will be used for these automated compliance checks during operations phase.

Deliverables:

- Test results from security tests.

3.4.5 Deployment and Integration

The deployment and integration phase follows the acceptance of the service subject to successful testing in the previous phase, i.e. after it has been approved for release.
It involves integrating all necessary elements of the service in the production environment and its deployment [4].

This means, if the service in scope relates to or requires other services or infrastructure components, these services has to be tested as well – either already done by availability of an attestation/certification or by integration these services/components in the approval process of the service in scope.

The approval is performed by signing the artifact and only signed artifacts are allowed to run in production.
The tested and signed software will be provided via Gaia-X repository.
Approval and signing will be done by the entity which is nominated by GAIX-A AISBL.

Deliverables:

- Accreditation / Certification report.

3.4.6 Maintenance and Disposal

The maintenance and disposal phase is the last phase of the SDLC. It is important, that software deployed in production needs to be constantly maintained to ensure continuous security of the provided functionality.

In general, this phase covers two aspects and will be simply referred to as *Production* phase:

- Maintenance and Disposal of the Federation Services software and
- Operation of the Federation Service

The maintenance of the software and operation of the service can be done by different provider.
The following description gives an overview of topics covering security related aspects during the production phase. The list is by no means exhaustive. A complete list of requirements is given by EUCS [7].

It is the responsibility of the Federation Service provider to ensure security during the production phase.

The verification of the safe operation of the Federation Services is planned to be done by an authorized entity, i.e. the AISBL or a service provider instructed by the AISBL.

Asset Management
The basis for a secure operation is to have an overview of all assets building the service. These assets will be either the Federation Service assets as well as the assets required to operate the Federation Service.
The service provider must have an appropriate asset management system to support the secure operation of the Federation Service.
For details see [7] - A.5 Asset Management.

Change and Patch Management
Ensure that changes and configuration actions to information systems guarantee the security of the delivered cloud service. This addresses changes and patches for the Federation Service software as well as for the operation of the service and infrastructure components.
For details see [7] - A.12 Change and Configuration Management.

Incident Management
All components and functions of the Federation Service as well as the infrastructure the service is operated on must be monitored to identify threats and vulnerabilities causing harm to the service. A central monitoring solution done by a Cybersecurity Operations Service is planned to correlate the security information (security events) from all Federation Services. Although a central service for monitoring is planned, each Federation Service provider is responsible for managing resulting Incident notification on its own. Therefore, it is mandatory that each Federation Service provider has a solution in place to manage security incidents.
For details see [7] - A.15 Incident Management.

Vulnerability Management
Vulnerability Management and testing is described in chapter 3.4.4. Each provider (either Federation Service provider as well as infrastructure provider) must ensure appropriate measures to identify and manage vulnerabilities.
For details see [7] - 14 Vulnerability Management.

Disposal
At the end of use - the "Disposal" phase - comprises all the steps that go with the discontinuation of support, decommissioning and disposal of the Federation Services as well as the components operated by the infrastructure provider [11].

A disposal policy must be available documenting at least the

- Offboarding of services and components
- Deletion of security and privacy related date like user data (e.g. data offer), access credentials, PII related data and system data (e.g. log data for security monitoring)

Deliverables:

- Evidence (Attestation or certification) of fulfillment of the relevant EUCS controls.

3.5 Usage of Quality Gates

Quality gates are used to attest that Federation Services fulfil security and privacy by design.
These quality gates must be passed at the end of each phase of the Federation Service delivery. Passing a quality gate requires the proof of deliverables as listed in Table 8.

Two main attestations are required:

- service attestation before initial Go-Live (Pre Go-Live) → Accreditation and Certification
- regularly service attestation after Go-Live (Post Go-Live) → Continuous Monitoring and recertification.

The table below lists the deliverables per phase.

Phase		**Deliverable**
Defining Concepts and Requirements	Pre Go-Live	List with fulfilment of requirements (Statement of Compliance (SOC) or Statement of Applicability (SOA))
Software Design		Documentation required for Compliance Documentation Service
Development and Implementation		• Policies of how security is ensured during development process • Test results of security testing (code scans)
Testing and Acceptance		Test Reports
Deployment and Integration		Accreditation / Certification report
Maintenance and Disposal	Post Go-Live	Evidence (Attestation or certification) of fulfillment of the relevant EUCS controls

***Table 8**: Overview of quality gates and deliverables*