Overview Security Tasks

# Software Requirements Specification for Gaia-X Federation Services Authentication/Authorization IDM.AA

(SRS\_GXFS\_IDM\_AA.pdf)

## IDM.AA.00005 Participant Documentation

The documentation MUST contain:

* Short Software Description (why and for what, when to use, how use, where to use)
* Usage guide
* **GDPR design decisions**
* **Security concept**
* Operations concept
* FAQ
* Keyword Directory

**🡺 Create Security Concept**

**🡺 Create GDPR design decisions documentation**

## IDM.AA.00019 OAuth 2.0 Security Best Current Practice

SSI OIDC Provider SHOULD employ all relevant measures for security of OAuth2.0 framework

Acceptance Criteria:

* Documentation of applied measures as per
* <https://datatracker.ietf.org/doc/html/draft-ietf-oauth-security-topics-16>

**🡺 Review Spring Auth Server to ensure all relevant security measures are employed**

**🡺 Document in Security Concept**

## IDM.AA.00028 Security Hardening

The whole adoption shell is security relevant, and it has to be defined in the security concept how these components can be more secured and what kind of steps to do.

🡺 **By doing a threat model and identifying additional security measures**

## IDM.AA.00053 Quality Aspects

The software MUST meet the following requirements:

* …
* Security
* …

Major security concerns regarding design and implementation MUST be documented and highlighted to the steering board*.* Minor security concerns SHALL be documented and mitigated.

**🡺 Create Threat Model**

**🡺 After all security Measures are applied check for remaining risks**

**Proceed with required process for remaining security risks**

## IDM.AA.00062 Interoperability of IT security features and algorithms

The following interoperability requirements of the respective IT security features and algorithms MUST be ensured across the system components:

* Interoperability of crypto algorithms and protocols (including the novel peer-reviewed ones through the established bodies and communities)
* Interoperability of secure secret transfer protocols (such as the holistic usage of PKCS#11 for HSM communication, etc.)
* Format interoperability of crypto material (such as the holistic usage of PKCS#12 for relevant cases)

🡺 **use of standardized crypto only**

## IDM.AA.00065 Automated Test Environment

All functionalities MUST be demonstrated in a complex test environment within a sandbox, with the following infrastructure components:

* Load Balancer, e.g., HAProxy
* API Gateway, e.g., Kong
* Service Mesh, e.g., Linkerd/Istio
* DNS
* Multiple Servers
* Firewalls

All security tests **MUST** be passed in this test environment automatically.

**🡺 Document Security Tests and Setup in the Security Concept (or reference respective documentation in the security concept)**

## 3.3.7. Security Requirements

### 3.3.7.1. General Security Requirements

Each Gaia-X Federation Service SHALL meet the requirements stated in the document “Specification of non-functional Requirements Security and Privacy by Design” [NF.SPBD]. Federation Services specific requirements will be documented in the next chapter.

## IDM.AA.00041 Cryptographic Algorithms and Cipher Suites

Cryptographic algorithms and TLS cipher suites SHALL be chosen based on the recommendation from the German Federal Office for Information Security (BSI) or SOG-IS.

* TR 02102-1
* TR 02102-2

**🡺 Create list of all used cryptographic algorithms**

**🡺 Cross reference list with applicable TRs**

**🡺 Document result in the security Concept**

## IDM.AA.00042 Digital Certificates

For digital certificates and cryptographic signatures in the context, the major requirements on cryptographic algorithms and key length MUST meet the definitions in the following table (as of 2020):

|  |  |  |
| --- | --- | --- |
| **Signature Algorithm** | **Key size** | **Hash function** |
| EC-DSA | Min. 250 Bit | SHA-2 with an output length ≥ 256 Bit or better |
| RSA-PSS (recommended)  RSA-PKCS#1 v1.5 (legacy) | Min. 3000 Bit RSA Modulus (n) with a public exponent e > 2^16 | SHA-2 with an output length ≥ 256 Bit or better |
| DSA | Min. 3000 Bit prime p  250 Bit key q | SHA-2 with an output length ≥ 256 Bit or better |

Named curves SHALL be used for EC-DSA (e.g., NIST-p-256).

**🡺 Check that the used cryptographic signatures we use adhere to the minimum key length requirement**

**🡺 document in security concept**

## IDM.AA.00043 TLS Certificate Validity Periods

In general, the recommended validity period for a certificate used in the system should be one year or less. Under some circumstances (for example RootCA) the certificate validity can be extended. Certificate owners MUST ensure that valid certificates are renewed and replaced before their expiration to prevent service outages

* Only for operations

## IDM.AA.00044 Security by Design

The software security MUST be from the beginning a design principle. Means separation of concerns, different administrative roles, especially for private key material and separate access to the data MUST be covered from the first second. It MUST be described in the security concept, what are the different security risks of the product and how they are mitigated (e.g., by Threat Modeling Protocols)

**🡺 Create Threat Model**

**🡺 Derive security measures to mitigate or remove risk**

**🡺 Documentation in Security Concept**

## IDM.AA.00045 Installation of Critical Security Updates

Node operators SHALL deploy security critical updates without undue delay.

* Only for operations

## IDM.AA.00046 Avoid HTTP Request Smuggling

To avoid Request Smuggling attacks, the product MUST implement a standard which handles this kind of attack by design, because the attack vector results in an insufficient implementation of the header handling. The chosen way to handle it MUST be shared to the other implementers of all other subcomponents within IDM & Trust and MUST be described in the security concept

🡺 **use HTTP/2 end-to-end to mitigate this problem**

**🡺 It is important to ensure that downgrading to HTTP/1 is not possible**

**🡺 Document solution in the security concept**

## IDM.AA.00047 HTTP Pentesting

All HTTP parts of the product has to be pen tested, for the following criteria:

1. Unauthorized Access to the System MUST be tested
2. Unauthorized Actions MUST be triggered without a user action
3. Endpoints MUST be tested for HTTP smuggling attack vectors
4. If a datastore is present over HTTP, illegal data access MUST be tested

It’s RECOMMENDED to test more attack vectors and document it for the purpose to mitigate it in later versions.

**🡺 Organize PenTest (with internal or external resources)**

**🡺 Reference PenTest results in the Security Concept**

## IDM.AA.00048 Storage of Secrets

The storage of secret information such as private keys MUST take place in state-of-the-art secure environments to protect secret data confidentiality and integrity. Examples of this are Secure Enclaves, TPMs, HSM or Secure Vaults. In case (Personal) Agents are not equipped with a secure storage it MAY also be possible to store the secrets in a third party (e.g., Cloud) provider (e.g., Secure Wallet) that MUST provide overall the same level of security as the aforementioned methods.

🡺 **Create list of all used cryptographic key material**

🡺 **needs to be discussed with eco**

## IDM.AA.00049 Secret Distribution and Usage

The product MUST ensure interoperability of cryptographic primitives and components by public standards and MUST use secure state of the art methods to create and import secrets into the secure storage, as well as performing cryptographic operations (e.g., encryption or digital signatures). For Key distribution, state of the art DKMS methods MUST be implemented.

🡺 **needs to be discussed with eco**

## IDM.AA.00050 Support for Potential Requirements for Secret Storages

Devices that hold cryptographic information and perform cryptographic functions MUST be compliant with the standard PKCS #11. Moreover, the products MUST be potentially eligible for a [FIPS-140-2] or ETSI/Common Criteria certification with the minimum-security level necessary to operate securely in the Gaia-X ecosystem. Security Levels in FIPS-140-2 range from 1 to 4. Current HSM Cloud Service offerings (AWS, Azure, GCP) are Level 3.

🡺 **needs to be discussed with eco**

## IDM.AA.00052 Special Availability and Scalability Requirements for Secret Storage Components

Secret Storage components play a central role in storage, encryption, and digital signing in the Gaia-X ecosystem, thus they can become a single point of failure for a Gaia-X participant, for example an organization. Therefore, methods and procedures to ensure the availability and scalability of the Secret Storage functionality MUST be implemented.

🡺 **needs to be discussed with eco**

# Specification of non-functional Requirements for Gaia-X Federation Services Security and Privacy by Design NF.SPBD

(GXFS\_Nonfunctional\_Requirements\_SPBD.pdf)

## 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.

## 2.2 Assurance Level

### Protection Profile

|  |  |  |  |
| --- | --- | --- | --- |
| Asset | Confidentiality | Integrity | Non-Repudiation |
| Identities | x | x | x |
| Verified Credentials | x | x | x |
| Access Policies |  | x | x |

1Summary of protection goals of assets of Federation Services

### Assignment of Assets to Technical Components

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| WP | Technical Component | Identities | Verified Credentials | Access  Polices |
| 1 | Self Sovereign Identity Service (Authentication/Authorization) | x | x | x |

2Assignment of assets to technical components of Federation Services

### 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.

|  |  |  |
| --- | --- | --- |
| WP | Technical Component | Assurance Level |
| 1 | Self Sovereign Identity Service (Authentication/Authorization) | high |

Assurance Level of Federation Services

The Assurance Level is based on the European Cybersecurity Certification Scheme for Cloud Services.

## 3.4 SDLC of Gaia-X Federation Services to ensure SPBD

### 3.4.1 Defining Concepts and Requirements

#### Cybersecurity Requirements

(see: <https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme>)

|  |  |  |
| --- | --- | --- |
| Applicable | Unsure | Not applicable |

Excerpt of the Table in the original document, everything not scoped to WP 1 was left out.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **EUCS controls** | **Control Description** | **Relevance for Gaia-X Federation Services** | **Affected Gaia-X Federation Service** | **Reference to further details** |
| 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. 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  🡪 Only for operations | ISO 27001 + complementary standards |
| 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 |
| 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 ²  • Catalogue  • Data Exchange  • Compliance  • Portal  ² Management of user and service credentials | complementary standards |
| 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 | complementary standards |
| 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 |
| 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. | Ensure information security in the development cycle of information systems. | • Identity  • Catalogue  • Data Exchange  • Compliance  • Portal | See description of SDLC |
| A.14 | Procurement Management | Ensure the protection of information that suppliers of the CSP can access and monitor the agreed services and security requirements. |  | • Identity  • Catalogue  • Data Exchange  • Compliance  • Portal  🡪 Only for operations |  |
| 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 |
|  | 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 |
|  | 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 |
|  | 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 |

#### 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.

#### Deliverables

The following deliverables must be provided as proof of compliance with the security and privacy by design requirements:

**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

#### 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
  + 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
  + 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

#### Deliverables

**Federation Services documentation as defined above.**

### 3.4.3 Development and Implementation

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 (EUCS - DEV-01). The policy shall cover the following aspects (EUCS - DEV-01 - DEV-07):

* + availability of secure development environments with separation from test and production environments (EUCS - DEV-02 - DEV-04)
  + appropriate documentation and testing of security features (EUCS - DEV-05)
  + identification of vulnerabilities introduced during the development process (EUCS - DEV-06).
  + aspects of outsourcing of development activities (EUCS - DEV-07)
  + security related trainings required for developers (EUCS - HR-04)
* Performing of security tests and analyzing of security information

Different security tests must be carried out during the development and implementation phase.

#### Deliverables:

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

### 3.4.4 Testing and Acceptance

With regard to the Continuous Integration / Continuous Delivery (CI/CD) process model, 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.

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

Required tests grouped by development phases:

**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).
    - **TruffleHog** (Suggestion by Wolfgang)
  + 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.
    - **Dependency Check** (already used and recommended by Wolfgang)
  + 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).
    - **SonarQube** (Suggestion by Wolfgang)
  + 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.
    - Should most likely be run as part of the PenTest (Suggestion by Wolfgang)
* 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.
    - **Checkov** (Suggestion by Wolfgang)
* 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)
  + 🡪 not applicable

#### Deliverables:

* **Test results from security tests.**

**🡺 see Test\_Plan documentation for the documentation of 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.

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.**
* **🡪 after discussion with eco this is not needed anymore**

### 3.4.6 Maintenance and Disposal

🡪 not applicable

## 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 below.

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.

|  |  |  |
| --- | --- | --- |
| **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 |