

TEST PLAN

< GAIA-X Authentication & Authorization Service >

Abstract

This document provides an overview of the project and the product test strategy, a list of testing deliverables and plan for development



VERSION HISTORY

Version #	Write by	Revision Date	Approved By	Approval Date	Outline
1.0					Test Plan create
1.1	Wolfgang Studier	26.04.22			Added Security Tests

Table of Contents

INTRODUCTION.....	5
1 TEST STRATEGY.....	5
1.1 Scope of Testing.....	5
1.1.1 Features to be tested - FUNCTIONAL	5
1.1.2 Features to be tested - SECURITY.....	9
1.1.3 Features to be tested – OTHER NON-FUNCTIONAL.....	12
1.1.4 Features not to be tested	15
1.2 Test Type	15
1.3 Risk and Issues	15
1.4 Test Logistics.....	16
1.4.1 Who will test?	16
1.4.2 When will tests occur?	16
2 TEST OBJECTIVE	16
3 TEST TOOLS	16
3.1 OpenID Conformance Suite	16
3.2 Security tools	16
3.3 JIRA – for reporting bugs?	16
4 TEST CRITERIA	16
4.1 Suspension Criteria	16
4.2 Exit Criteria	16
5 RESOURCE PLANNING.....	17
5.1 System Resource	17
5.2 Human Resource	17
6 TEST ENVIRONMENT.....	17
7 SCHEDULE & ESTIMATION.....	17
7.1 All project task and estimation	18
8 TEST DELIVERABLES	18

8.1	Before testing phase	18
8.2	During the testing	18
8.3	After the testing cycles is over	18

INTRODUCTION

The Test Plan is designed to prescribe the scope, approach, resources, and schedule of all testing activities of the project GAIA-X Authentication & Authorization Service.

The plan identifies the items to be tested, the features to be tested, the types of testing to be performed, the personnel responsible for testing, the resources and schedule required to complete testing, and the risks associated with the plan.

1 TEST STRATEGY

1.1 Scope of Testing

1.1.1 Features to be tested - FUNCTIONAL

All the feature of GAIA-X which were defined in software requirements spec need to be tested. (AAS spec: <https://www.gxfs.eu/download/1752/>)

Requirement	Acceptance criteria	Description	Comments
IDM.AA.00014 Credential Based Access Control (CrBac)	1) During a resource access, it must be demonstrated that new credentials can be transmitted to get access. 2) The documentation must describe what to configure in the demonstration IAM	The SSI adoption shell SHOULD be able to dynamically reload credentials for access decisions, for instance the current identity wants a “sales” action and is currently just logged in with a “visitor” permission. The CrBac SHOULD be able to resolve this by requesting new credentials. This might be achieved either by a renewed authentication and authorization flow triggered by the application (via SSI OIDC Provider), or via an asynchronous process, which SHOULD be done over standard IAM outgoing PIP interface towards Trust Services or the It MAY be realized over additional components within the architecture, but the Standard IAM MUST NOT be modified (excepting configuration, plugins or supported extensions).	Manual test in JIRA GAIAXAUTH-82
IDM.AA.00015 External PIP Integration		It MUST be demonstrated how an external PIP with asynchronous behavior can be integrated in the authorization services of a standard IAM system. It MAY be demonstrated with additional components.	Manual test in JIRA GAIAXAUTH-82

GAIA-X Authentication & Authorization Service

IDM.AA.00016 Standard open source IAM Package	<ol style="list-style-type: none"> 1) One working IAM System with the Adoption Shell. 2) Documentation of proper configuration of both Adoption Shell and chosen IAM system. 3) "All in one" package, ready for installation 	Together with the Adoption Shell, the product MUST include a working integration with one basic open source IAM system. The selection has to be compliant with the Gaia-X policy and rules and any choice that supports the OAuth2 [RFC7591] standard functions as Client Registration [RFC7591], Token Issuing (minimum code and client credential flow), authorization and permission handling.	Does not require any special test, the configured IAM will be part of project delivery.
IDM.AA.00017 OpenID Provider Configuration Information	<ol style="list-style-type: none"> 1) Documentation of self-conducted conformance testing of OpenID Provider Publishing Configuration Information profile or an official certification from OpenID Foundation. 2) Documentation how the Well-Known Configuration has to be setup. 3) Demonstrate a working dynamic configuration of a standard IAM OIDC broker with OpenID Provider Configuration Information of SSI OIDC Provider. 4) Explanation in the operations concept how to configure it. 	SSI OIDC Provider MUST offer an OpenID Provider Configuration Information endpoint as specified in [OIDC.Discovery]. All SSI-related scopes and claim types SHOULD be exposed through this endpoint for dynamic discovery and configuration. The SSI OIDC Provider MUST fulfill the requirements of OpenID Provider Publishing Configuration Information profile as in [OIDC.Conformance].	Tests with OIDC oidc-discovery-endpoint-registration
IDM.AA.00018 OpenID Connect Implicit profile	<ol style="list-style-type: none"> 1) Documentation of self-conducted conformance testing of Implicit OpenID Provider profile or an official certification from OpenID Foundation. 2) Demonstrate a working integration with a standard IAM brokering OIDC Authorization to SSI OIDC Provider with OpenID Connect Implicit profile configuration. 3) The documentation must describe what to configure in the demonstration IAM. 	SSI OIDC Provider MUST fulfill all the requirements of Implicit OpenID Provider profile as defined in [OIDC.Conformance]	<p>This requirement was changed: AAS implements Authorization Code profile instead of Implicit profile.</p> <p>Tested with OIDC Conformance Suite</p>

GAIA-X Authentication & Authorization Service

DM.AA.00020 SSI Login Page	<p>1) The login page presents an QR Code and the Button Link with an SSI invitation link/proof request.</p> <p>2) The login page redirects with an error response after the time-out.</p> <p>3) The login page polls in the background the login state and redirects to the given URL after a successful login.</p> <p>4) The login page must deliver with one specific Look & Feel aligned with Gaia-X Portal UX. Information regarding Look & Feel of the Gaia-X Portal UX will be provided by eco.</p> <p>5) The login page must support required languages and display according to the browser settings or OIDC authorization request parameters as per precedence definition.</p> <p>6) The documentation must describe Look & Feel customization options and their configuration.</p>	<p>The OIDC Provider MUST contain a customizable Standard Login web page integrated into OIDC Authorization flow and endpoint as per [OIDC.Core] which shows an QR Code for login using another device hosting Personal Credential Manager as well as a button with the same link being able to open Personal Credential Manager on the same device. The button MUST trigger a registered application or page on the new browser tab, without interruption of the count-down and the status polling process.</p> <p>The SSI Login Page MUST display a progress bar which counts down a configurable time (e.g., 30 seconds).</p> <p>The login page MUST poll in the background the configured login state URL with a given request identifier for the configured amount of time.</p> <p>If the request is successful or timed-out during the waiting time the SSI Login Page MUST redirect the User Agent back to the IAM system redirect_url with appropriate response parameters as per [OIDC.Core].</p> <p>This login page MUST be styleable over CSS or html template system to customize the look and feel at the installation and configuration time. The login page should support internationalization and follow either browser settings or OIDC parameters defined for this purpose.</p>	<p>Current implementation doesn't use polling, but has a standard submit button which starts login procedure</p> <p>Manual test in JIRA GAIAAUTH-86</p>
IDM.AA.00021 QR Code Generation	<p>1) The button and the QR Code contain the link content rendered as QR Code.</p> <p>2) The QR Code must be readable by a smartphone.</p> <p>3) The presentation ID is not inside the QR Code or button link</p>	<p>The QR code contains the content of the SSI invitations/proofs, which MUST be obtained from an external URL with the values for scope and a value for "Namespace". Scope Values MUST be extracted from the authorize request.</p> <p>The link content has to be generated in a QR Code. PresentationID needs be securely stored in the browser session, so that it's available for the [IDM.AA.00028] Login State Background Polling process and not revealed outside of this context as it represents a secure token to get identity data</p>	<p>Manual test in JIRA GAIAAUTH-87</p>

GAIA-X Authentication & Authorization Service

IDM.AA.00022 Login State Background Polling	<ol style="list-style-type: none"> 1) Login Token with the contained claims and scopes 2) Correctly signed token 3) Redirect to IAM System on Success 4) Offer Retry or redirect back with failure to IAM System on Error 	<p>The content in the response MUST be available in the IAM system after the successful response. This MUST be realized by continuing the standard OIDC flow and forming a valid id_token including the claims from the response.</p> <p>Unsuccessful response shall be followed with an option to retry the process with [IDM.AA.00027] QR Code Generation or to fail the process and redirect back to the IAM with appropriate OIDC failure response.</p>	<p>Manual test in JIRA GAIAAUTH-87.</p> <p>Polling implemented between AAS and TSA</p>
IDM.AA.00023 Session handling and scope elevation	<ol style="list-style-type: none"> 1) Session handling by consecutive authentication requests with id_token_hint do not impose new authentication and authorization and authenticate the user in a seamless manner. 2) A request for additional proofs is conducted and added to id_token in case the requested scope of authorization is wider than previously. 3) Session duration is configurable at installation / deployment time 	<p>In case additional scopes are required the SSI OIDC Provider MUST conduct a proof request for the additional Verifiable Credentials without a need to build a new connection with an invitation QR Code/Link. The option to create a new Link MUST be available, however.</p> <p>Session handling related parameters of [OIDC.Core], like prompt or max_age shall be respected and translated into appropriate proof requests to assure required functionality.</p> <p>The proof is realized with the same methods and policies as described in [IDM.AA.00027] QR Code Generation and [IDM.AA.00028] Login State Background Polling using optional sub and max_age parameters.</p>	<p>Tests with OIDC Conformance Suite:</p> <ul style="list-style-type: none"> -oidcc-max-age-1 -oidcc-max-age-10000 -oidcc-id-token-hint
IDM.AA.00024 Offer SSI Client Registration Auth API	SSI Client Registration API is offered and documented	An API as per [IDM.AA.00017] SSI Client Registration Auth API MUST be offered to enable initiation and polling for the result of SSI-based issuance of IAT for Dynamic Client Registration.	Custom endpoint Manual test in JIRA GAIAAUTH-90
IDM.AA.00025 Policy based authorization	<ol style="list-style-type: none"> 1) IAT is issued only after successful evaluation of the Policy by Trust Services. 2) Negative evaluation of the Policy by Trust Services results in no IAT issued and an appropriate error response. 	<p>The SSI IAT Provider MUST integrate with Trust Services to conduct policy authorization checks of the client trying to obtain an Initial Access Token (IAT). IAT MUST not be issued unless the policy evaluation allows for that operation.</p>	Manual test in JIRA GAIAAUTH-90

GAIA-X Authentication & Authorization Service

IDM.AA.00026 Standard IAM Compatibility	1) A dynamic client with an IAT can be registered in the IAM system over the client registration endpoint.	The issued Initial Access Token MUST be compatible with the Client Registration Endpoint of the docked standard IAM. It MUST be possible to register with this IAT client as defined in [RFC7591].	Manual test in JIRA GAIAAUTH-90
IDM.AA.00027 Client Registration	1) A dynamic client with a software statement can be registered in the IAM system over the client registration endpoint.	The IAT Provider MUST be registered as an OAuth2 [RFC6750] Client using client credential grant within the Standard IAM to obtain Initial Access Tokens of the System.	This is out of AAS scope, so was not tested.

1.1.2 Features to be tested - SECURITY

Requirement	Acceptance criteria	Description	Comments
IDM.AA.00019 OAuth 2.0 Security Best Current Practice	Documentation of applied measures as per [BCP OAuth2]	SI OIDC Provider SHOULD employ all relevant measures for security of OAuth2.0 framework [BCP OAuth2].	OAuth2 best current practice document was considered at implementation of underlying Spring Boot Authorization Server. See AAS Security Concept document
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.	See AAS Security Concept document
IDM.AA.00029 HTTPS		All HTTP Endpoints MUST be protected by TLS 1.2 (all protocol version numbers SHOULD be superseded by upcoming standards) Each endpoint of the product MUST support TLS certificates which are configurable by the administrator of the system.	All AS endpoints support HTTPS/TLS but certificates were provided too late and not configured yet.
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. These recommendations and the recommendations of other institutions and standardization	All recommendations regarding certificates were compiled in the RecommendedTLSCipherSuites_v02 document.

GAIA-X Authentication & Authorization Service

		organization are quite similar [CryptoLen]. The recommendations can be found in the technical guidelines TR 02102-1 [TR02102-1] and TR 02102-2 [TR02102-2] or SOG-IS Agreed Cryptographic Mechanisms [SOG-IS].	
IDM.AA.000 42 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)...	We use RS-256 algorithm with key length 3072
IDM.AA.000 43 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	This must be considered by deployment team of cloud provider who will use GAIA-X services in its cloud environment
IDM.AA.000 44 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)	Considered in the AAS Security Concept and EUCS Controls documents
IDM.AA.000 45 Installation of Critical Security Updates		Node operators SHALL deploy security critical updates without undue delay	This must be considered by deployment team of cloud provider who will use GAIA-X services in its cloud environment
IDM.AA.000 46 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	The issue is mitigated completely if HTTP2 protocol used. But it requires use of HTTPS/TLS which is not configured

GAIA-X Authentication & Authorization Service

		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.	yet
IDM.AA.000 47 HTTP Pentesting		<p>All HTTP parts of the product has to be pen tested, for the following criteria:</p> <ol style="list-style-type: none"> 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 	Tested by MMS team, pen-test results provided
IDM.AA.000 48 Storage of Secrets		<p>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</p>	All secrets are stored as k8s secrets.
IDM.AA.000 49 Secret Distribution and Usage		<p>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.</p>	This must be considered by deployment team of cloud provider who will use GAIA-X services in its cloud environment

GAIA-X Authentication & Authorization Service

IDM.AA.000 50 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.	This must be considered by deployment team of cloud provider who will use GAIA-X services in its cloud environment
IDM.AA.000 51 Secure Timestamps		All timestamps MUST be issued according to [RFC3161].	Not implemented
IDM.AA.000 52 Special Availability and Scalability Requirements for Secret Storage Components		Secret Storage components play a central role in storage, encryption, and digital signing in the GaiaX 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	All secrets are stored as k8s secrets.

1.1.3 Features to be tested – OTHER NON-FUNCTIONAL

Requirement	Acceptance criteria	Description	Test
IDM.AA.000 30 HTTP Protocol Definitions		All HTTP Endpoints MUST follow [RFC7231] and [RFC5789], but it MAY be chosen what of the protocols is necessary to realize the functionality. For problem reports the [RFC7807] MUST be used in combination with Standard HTTP Error Codes.	All AAS endpoints support REST API standards which is based on HTTP.

GAIA-X Authentication & Authorization Service

IDM.AA.000 31 Configuration		All components MUST support one of the major configuration formats (yaml, json, ini, environment variables) wherever configuration is required. If environment variables are overwriting an actively set configuration, a warning SHOULD be logged.	All system configuration done in yaml files and can be overwritten with system variables. All system variables are logged on the service start.
IDM.AA.000 32 Data Minimization		From GDPR perspective the product MUST NOT log data which is related to personal information. (e.g., User Names, Birth Dates etc.) The product MUST only log data, which is relevant to technical operations, except for the purpose that, in the event of an incident, enable reconstruction of the sequence of the message exchange for establishing the place and the nature of the incident. The data shall be stored for a period of time in accordance with national requirements and, as a minimum, shall consist of the following elements: (a) node's identification (b) message identification (c) message data and time All logged data/information MUST be documented in the GDPR design decisions for a GDPR review.	Implemented according to GDPR recommendations. No PII information is logged. Logs are stored for 30 days only
IDM.AA.000 33 Logging Frameworks		The product MUST support logging frameworks e.g., graylog, fluentD or logstash to support logging and analysis by enterprise infrastructures. The supported framework MAY be chosen for the first version, but it MUST support potentially the most common open-source logging solutions. The final solution MUST be aligned with the other subcomponents. It MUST be sketched in the operations concept how the support of multiple solutions is given in the future.	Service implementation use log4j/logback frameworks for logging. The mentioned cluster logging frameworks can be configured and used in cloud provider environment by its deployment team
IDM.AA.000 34 Monitoring		The product MUST support monitoring frameworks e.g., Grafana to support the analysis of incoming	The service exposes its metrics in Prometheus

GAIA-X Authentication & Authorization Service

Frameworks		data by the enterprise infrastructures. The supported framework MAY be chosen for the first version, but it MUST support potentially the most common monitoring solutions. (e.g., Zabbix) The final solution MUST be aligned with the other subcomponents. It MUST be sketched in the operations concept how the support of multiple solutions is given in the future.	format. Provider's deployment team can install Prometheus and Grafana servers in the service environment and then perform service monitoring with mentioned products
IDM.AA.000 35 Alerting Frameworks		Additional to the Monitoring Frameworks an Alerting framework (e.g., Prometheus or Cloud Based) MUST/MAY be in place at least in the System nodes to promptly communicate to e.g., System Administrators or owners the occurrence of an event in form of a security incident or application/system malfunction or anomaly.	Not implemented in the service itself. Provider's deployment team can configure log monitoring with Grafana/Loki products and then configure required alerts in Grafana based on logs monitoring
IDM.AA.000 36 Performance Scalability		The performance of the product MUST be scalable. This MUST be demonstrated in a load demonstration example. The optimal scalability SHOULD be in the best case a linear behavior of minimum 50% more performance by each additional instance.	Load tests were provided, but scalability tests were not performed
IDM.AA.000 37 Performance by Design		The product SHOULD be designed and implemented in a way, that the implementation is non-blocking and performance oriented. It SHOULD be a microservice architecture, but it MAY follow other concepts. The decision MUST be documented.	The service implemented in Spring Boot microservice style
IDM.AA.000 38 Recovery Point Objective (RPO)		The RPO for the product MUST be 0 for a single and multiple instance(s). It MAY be higher by configuration or deployment, decided by the user	Readiness/Liveness probes are implemented and can be used by Kubernetes to provide required RPO

GAIA-X Authentication & Authorization Service

IDM.AA.000 39 Recovery Time Objective (RTO)		The RTO for the product MUST be one Minute for a single instance. For multiple instances the RTO MUST be 0.	Readiness/Liveness probes are implemented and can be used by Kubernetes to provide required RTO
IDM.AA.000 40 Mitigation of Single Point of Failure threats		Critical components in the Gaia-X Ecosystem MUST be identified and strategies to warranty their availability and scalability MUST be implemented.	Multi-instance service deployment was not tested.

1.1.4 Features not to be tested

These features are not to be tested because they are not included in the software requirement specs

- Hardware Interfaces
- Database logical
- Communications Interfaces

1.2 Test Type

In the project GAIA-X, there're several types of testing should be conducted.

- **Integration** Testing (Individual software modules are combined and tested as a group)
 - **System** Testing: Conducted on a **complete, integrated** system to evaluate the system's compliance with its specified requirements
 - **API testing**: Test all the APIs create for the software under tested
- **Security testing**
 - **Code Testing**: Code review, automated SAST testing and automated testing for hardcoded secrets of only the self-implemented components and configurations
 - **Vulnerability Scanning**: Software composition analysis (SCA) of the whole solution checking for vulnerable dependencies as well as incompatible software licenses
 - **Penetration Testing**: Penetration test of the whole system with scope on the self-developed parts including DAST testing
 - **Compliance Testing**: automated checks of used configurations with focus on system hardening
 - **Security (Unit) Tests**: Security function/controls used in the code (e.g. authentication) must be verified with test cases.

1.3 Risk and Issues

Risk	Mitigation
The project schedule is too tight.	Set Test Priority for each of the test activity.

1.4 Test Logistics

1.4.1 Who will test?

The project should use team member as the tester.

1.4.2 When will tests occur?

The tester will start the test execution when all the following inputs are ready

- Software is available for testing
- Test Specification is created
- Test Environment is built
- Test Cases are written

2 TEST OBJECTIVE

The test objectives are to **verify** the Functionality of Authentication and Authorization Service of GAIA-X, the project should focus on testing the **login using different methods** such as using QR code, ...etc. to **guarantee** all these operations can work **normally** in real business environment.

3 TEST TOOLS

3.1 OpenID Conformance Suite

3.2 Security tools

- Secret scanning
 - TruffleHog
- SCA
 - DependencyCheck (OWASP)
 - For Open Source License Compliance I normally propose WhiteSource, but this is not a FOSS solution.
- SAST
 - SonarQube
- Configuration Compliance (SAST)
 - Checkov

3.3 JIRA – for reporting bugs?

4 TEST CRITERIA

4.1 Suspension Criteria

If the team members report that there are **40%** of test cases **failed**, suspend testing until the development team fixes all the failed cases.

4.2 Exit Criteria

Specifies the criteria that denote a **successful** completion of a test phase

- **Run** rate is mandatory to be **100%** unless a clear reason is given.
- **Pass** rate is **80%**, achieving the pass rate is **mandatory**.

5 RESOURCE PLANNING

5.1 System Resource

No.	Resources	Descriptions
1.	Server/CLOUD	
2.	Test tool	
3.	Test environment	

5.2 Human Resource

No.	Member	Tasks
1.	Test Manager	Manage the whole project Define project directions Acquire appropriate resources
2.	Tester	Identifying and describing appropriate test techniques/tools/automation architecture Verify and assess the Test Approach Execute the tests, Log results, Report the defects. Outsourced members

6 TEST ENVIRONMENT

The Test Environment should be setup

7 SCHEDULE & ESTIMATION

7.1 All project task and estimation

Task	Members	Estimate effort
Create the test specification	Test Designer	30 man-hours
Perform Test Execution	Tester, Test Administrator	160 man-hours
Test Report	Tester	20 man-hours
Total		210 man-hours

8 TEST DELIVERABLES

Test deliverables are provided as below

8.1 Before testing phase

- Test plans document.
- Test cases documents
- Test Design specifications.

8.2 During the testing

- Test Tool
- Simulators
- Test Data
- Error logs and execution logs.

8.3 After the testing cycles is over

- Test Results/reports
- Defect Report
- Release notes