GAIA-X Authentication & Authorization Service: Security Concept

Contents

[Introduction 3](#_Toc101529841)

[Project Description and Goals 3](#_Toc101529842)

[Purpose of the Document 3](#_Toc101529843)

[Definitions and Methodology 3](#_Toc101529844)

[Scope of Application 3](#_Toc101529845)

[Service Description 4](#_Toc101529846)

[Delimitation Criteria and Safety Assumptions 4](#_Toc101529847)

[Structural Analysis 4](#_Toc101529848)

[Business Processes 4](#_Toc101529849)

[Data 4](#_Toc101529850)

[IT-Components 5](#_Toc101529851)

[Data Occurrence 5](#_Toc101529852)

[Evaluation of Protection Requirements 5](#_Toc101529853)

[Definition of the Protection Requirement Categories 5](#_Toc101529854)

[Protection requirements assessment for business processes 5](#_Toc101529855)

[Protection requirements assessment for data 6](#_Toc101529856)

[Protection requirements assessment for IT components 6](#_Toc101529857)

[Conclusions from the results of the protection requirements assessment 6](#_Toc101529858)

[Threat Modeling 6](#_Toc101529859)

[Identified Threats 7](#_Toc101529860)

[Threat Analysis 7](#_Toc101529861)

[Ranking of Threats 7](#_Toc101529862)

[Selection and Adaptation of Security Measures 7](#_Toc101529863)

[Securing business processes 8](#_Toc101529864)

[Securing IT components 8](#_Toc101529865)

[Other measures 8](#_Toc101529866)

[Security Evaluation 8](#_Toc101529867)

[Confidentiality 8](#_Toc101529868)

[Integrity including Authenticity 8](#_Toc101529869)

[Availability 8](#_Toc101529870)

[References 8](#_Toc101529871)

# Introduction

The document discusses security concepts around GAIA-X Authentication & Authorization Service. The document assumes a basic knowledge of security methodologies and practices in the audience reading the document and does not explain these topics in detail.

## Project Description and Goals

// A brief description of the project and its objectives.

The goal of GAIA-X Authentication & Authorization Service (AAS) project is to implement a service which will enable Gaia-X participants to authenticate users and systems in a trustworthy and decentralized self-sovereign manner without the need for a central source of authority as well as to assure authorization of access and data usage based on such identity data and credentials managed decentralized.

## Purpose of the Document

// Which aspects are addressed in this document?

The intent of this document is to provide an overview of implemented functionality as well as of information security principles and concepts taken into account in implementation of the AAS project.

## Definitions and Methodology

// Which standards, norms, etc. are used as a guideline for the definitions of terms and the creation of this IT security concept?

The following standards and methodologies were considered and used in the project implementation:

|  |  |
| --- | --- |
| **Name** | **Usage** |
| OIDC/OAuth2/CIBA security and privacy considerations | Were used to explore underlying threat model and take into account measures proposed in the specified protocols. |
| OAuth2 best current practice | It was a requirement to consider OAuth2 best current practice document in service implementation. Some of the practices were used in the underlying Authorization Server implementation. |
| STRIDE methodology | Was used to prepare and analyze service threat model. |
| OWASP Top 10 Web application security risks | Were also considered at service implementation phase. No evidence of the specified risks was found at the penetration test phase. |
| EUCS controls and recommendations | Referenced in the SPBD document. Most of the security controls used in the service implementation are derived from requirements specified by this scheme. |
| GUIA-X Security and Privacy by Design | The base document specifying security and privacy requirements to deliver and operate GAIA-X Federation Services. |
| GDPR recommendations and requirements | Applied in service logging implementation. |

# Scope of Application

// This chapter defines the scope of the IT security concept. Not only technical, but also organizational aspects should be taken into account when defining the scope, so that responsibility and accountabilities can be clearly defined

## What we need to understand that the project goal is a reference implementation of the A&A Service, which can subsequently be deployed in a variety of environments and configurations. Therefore, when building a threat model, the functionality provided by the service was considered at the first place. Issues of deployment, configuration, administration and maintenance of the project in production environment were not considered because they are out of the responsibility scope of the service development team.

## Service Description

// Description of the service (its core characteristics, objective and basic operation) for which this IT security concept is created.

The Gaia-X concept of Authentication and Authorization is based on the SSI Standards W3C Verifiable Credentials and decentralized key management (DPKI) defined by the W3C DID Core Specification and extended with DIF Specifications for DID-based message exchange (DIDComm).

At the core of this enablement stays integration and assurance of compatibility to the existing and well-established authentication protocols such as OpenID Connect (and underlying OAuth2). Thus, the service function shall offer components which bridge between SSI-based authentication and the established OpenID Connect specification for authentication and request of claims including related proofs. In the same manner a bridge function shall be offered to authenticate system-to-system interactions utilizing OAuth2 authorization framework, with dynamic client registration and establishing trustworthy mutual TLS-authentication link backed by SSI-based self-sovereign and decentralized authentication and authorization.

## Delimitation Criteria and Safety Assumptions

// What is the focus of this IT security concept? Which aspects are not considered in detail? What is taken as a "given"?

The focus of this security concept document is to build proper Threat model for functions, provided by AAS and to propose mitigation steps for the found threats. Only custom endpoints and protocols were considered in detail. Standard authentication functions provided via OIDC/OAuth2/CIBA protocols were not taken into account in the service threat model because they’re covered by their own security and privacy considerations and risk mitigation steps are provided in their corresponding documents. Major vulnerabilities identified by underlying protocols together with countermeasures are mentioned in the next chapters.

# Structural Analysis

// During the structural analysis, all business processes, data to be processed, and IT components involved are compiled that form the basis for the IT security concept in the defined scope.

The following GAIA-X services with their relationships are used to provide required functionality:

* Auth Service: major [Authentication & Authorization Service](https://www.gxfs.eu/authentication-authorisation/) component exposing endpoints required by GAIA-X LOT1 specification.
* IAM Platform: Identity and Access Management platform like keycloak, Gluu, WSO2, etc.
* [Portal](https://www.gxfs.eu/portal/): web application protected with AAS, implemented as GAIA-X LOT13.
* [Personal Credential Manager](https://www.gxfs.eu/personal-credential-manager/): mobile application (SSI Wallet), GAIA-X LOT2 implementation.
* [Organization Credential Manager](https://www.gxfs.eu/organizational-credential-manager/): GAIA-X LOT3 implementation.
* [Trust Service API](https://www.gxfs.eu/trust-services-api/): GAIA-X LOT4 implementation.

Diagram

Description automatically generated

## Business Processes

// Which information processing processes are considered? The data processed can be derived from the consideration of the business processes.

The service implements two major business functions:

* SSI Backchannel Login scenario: this feature provides a capability for end user to login over an QR code, and an SSI Backchannel provided by the Trust Services API (TSA). The function enables an end user to use his personal SSI wallet for login to a resource protected by IAM Platform. The provider itself is configured over a standard OIDC identity provider configuration within an IAM System.
* SSI IAT Provision scenario: this feature provides a capability for client service to obtain Initial Access Token (IAT) which can be used in subsequent client registration request with IAM Platform via standard Dynamic Client Registration (DCR) interface as defined in [RFC7591]. The IAT Provider checks in the background over policies with trust relationship (TSA component) before the IAT issuing.

## Data

// Which data (and data types - e.g. general personal identification data, transaction data) are generated and handles in the described business processes?

In the SSI Backchannel Login scenario User Claims are transmitted from TSA through AAS to IAM. User Claims are standard claims corresponding to requested scopes as per OIDC Core specification but can be extended with custom scopes and claims.

Data Flow Diagram for this scenario is:

Diagram

Description automatically generated

In SSI IAT Provision scenario Client Service provides its public identity data to AAS. AAS requests Service Claims from TSA and then provision these claims to IAM getting back IAT and returning it to the requesting Client Service. The IAT is a JSON Web Token (JWT) encoded with base64 algorithm. Decoded data contains header and payload blocks like the following:

header: {

  "alg": "HS256",

  "typ": "JWT",

  "kid": "04c74eca-431d-4437-b1cb-08c61dae7548"

}

payload: {

  "exp": 0,

  "iat": 1654685928,

  "jti": "d01b13a3-4912-4669-bfb8-beff8334fbbb",

  "iss": <http://78.138.66.168:8080/realms/gaia-x>,

  "aud": <http://78.138.66.168:8080/realms/gaia-x>,

  "typ": "RegistrationAccessToken",

  "registration\_auth": "authenticated"

}

Data Flow Diagram for this scenario is:

Diagram

Description automatically generated

To summarize the Data transmitted between system components:

* Policy Evaluation Request: a request from AAS to TSA to perform policy evaluation and return evaluation result – User Claims. The request can contain public requestor identifier (usually DID).
* Request ID: a surrogate identifier (UUID, most probably) of policy evaluation request communicated between TSA and AAS.
* User Claims: a set of key/value pairs with standard user attributes like first/last/middle name, birthdate, email, etc.
* Service Claims: also set of key/value pairs regarding particular service to be registered in the system for future authentication protection.
* Authorization Code: a string communicated between AAS and IAM as part of OIDC Authorization Code flow.
* JWT: JSON Web Token structure containing User/Service Claims, encoded with base64 algorithm and signed. Communicated from AAS to IAM and then from IAM to User Agent.
* JWKS: JSON Web Key Set – a structure containing public keys to validate JWT signature.
* RAT: Registration Access Token, transferred from AAS to IAM in JWT form.
* IAT: Initial Access Token, transferred from IAM to AAS and then to Client Service in JWT form.

## Service Components

// Which IT components (including communication links) are involved in the respective business processes?

The service consists of two major software components:

* Authentication Service: major AAS component exposing standard endpoints required by OIDC CIBA and SIOP protocols which are used in SSI Backchannel Login scenario and custom endpoints required in IAT Provision scenario. The component is implemented as a regular Spring Boot Java application. Required OpenID/OAuth2 functionality is provided by [Spring Authorization Server](https://docs.spring.io/spring-security-oauth2-boot/docs/2.2.x-SNAPSHOT/reference/html/boot-features-security-oauth2-authorization-server.html) with help of [Spring Security](https://spring.io/projects/spring-security-oauth) components.
* Identity and Access Management Platform: the system providing standard Authentication and Authorization capabilities to protect external (web)applications. In the LOT1 implementation Keycloak was chosen to fulfill the required functionality.

## Data Occurrence

// In which IT components is the above data processed?

The business scenarios explained above are detailed in the following sequence diagrams.

The SSI Backchannel login flow.

Diagram

Description automatically generated

Data transmission is:

* Step 1.11: Login Policy Evaluation Request from AAS to TSA
* Step 1.12: Request ID from TSA to AAS
* Step 1.18: Request ID from AAS to TSA
* Step 1.19: User Claims from TSA to AAS
* Step 1.20, 1.24: Authorization Code from AAS through User Agent to IAM
* Step 1.25: Authorization Code (in Authorization header) from IAM to AAS
* Step 1.26: JWT with User Claims from AAS to IAM
* Step 1.26, 1.28: Authorization Code from IAM through User Agent to Portal
* Step 1.29: Authorization Code (in Authorization header) from Portal to IAM
* Step 1.30: JWT with User Claims from IAM to Portal

The SSI IAT Provision flow.

Diagram

Description automatically generated with medium confidence

Data transmission is:

* Step 1.3: IAT Policy Evaluation Request from AAS to TSA
* Step 1.4: Request ID from TSA to AAS
* Step 1.5: Request ID from AAS to Client Service
* Step 1.6, 1.10: Request ID from Client Service to AAS
* Step 1.7, 1.11: Request ID from AAS to TSA
* Step 1.12: Service Claims from TSA to AAS
* Step 1.13: RAT and Service Claims from AAS to IAM
* Step 1.14: IAT from IAM to TSA
* Step 1.15: IAT from AAS to Client Service

# Evaluation of Protection Requirements

// The chapter on identifying protection requirements describes the protection requirements for business processes, the data they contain, and the IT components involved in the respective business processes. The aim of a security concept is to protect assets according to their criticality by means of appropriate hardening/securing of IT components. To this end, the expected damage that could occur if the three protection goals (confidentiality, integrity including authenticity, availability) are compromised is considered below for the processed information. The protection requirements of the IT components that process the information are derived directly from the protection requirements of processed assets.

This document section defines the protection levels and assigns them to business processes, data which they process and components implementing the processes.

## Definition of the Protection Requirement Categories

// This includes discussion of the classification/quantification of the need for protection (which regulatory requirements are observed?). It is important that there is a common understanding of the notation used.

AAS is a cloud service which implementation suppose to be deployed as infrastructural service in cloud service provider environment together with other GAIA-X services. According to the Security and Privacy by Design document which is accompanying all GAIA-X service specifications there were three levels of Assurance defined:

* Basic: Cloud services with basic level store, process or transmit public data, such as web sites.
* Substantial: Cloud services with substantial level come in touch with sensitive data, such as personal data or e-mails, and have to keep them confidential.
* High: Cloud services at level high, work with critical data, such as company secrets or digital identities.

Assurance levels are based on the European Cybersecurity Certification Scheme for Cloud Services. So, we can map the assurance levels from SPBD document with standard Protection Categories specified in security concept standards:

* Normal: The effects of the damage are limited and manageable. Assurance level: Basic.
* High: The effects of the damage may be considerable. Assurance level: Substantial.
* Very high: The effects of the damage may be catastrophic enough to threaten an organization’s existence. Assurance level: High.

## Protection requirements assessment for business processes

// What is the protection requirement for the information processing process?

Basing on the protection levels defined above we measure our business processes as:

* SSI Backchannel Login: protection level is High because the process works with User Claims which is personal data and have to keep it confidential.
* SSI IAT Provisioning: protection level is Normal because the process works with Service Claims which is public data and IAT (constructed from the Service Claims) only.

## Protection requirements assessment for data

// What is the protection requirement for the data (depending on the data type - e.g., general personal identification information, transaction data)? The relevance of business processes can help in assessing the need for protection of the data.

We measure data processed in service business processes as:

* User Claims processed in SSI Backchannel Login scenario: protection level is High because it is personal data (like e-mail, birthdate, etc.) and must not be disclosed according to GDPR standards.
* Client Service Claims processed in SSI IAT Provision scenario: protection level is Normal as it is publicly available data.
* Initial Access Token produced in SSI IAT Provision scenario: protection level is Basic because the token is built from publicly available data (Service Claims).

## Protection requirements assessment for service components

// What is the protection requirement for the IT components? Components always inherit the highest protection requirement for the data they process.

GAIA-X Security and Privacy by Design (SPBD) specification defines Assurance Level for AAS as High, so we measure our service components as:

* Authentication Service: protection level is Very High according to SPBD Assurance level assigned to the service.
* Identity and Access Management Platform: protection level is Very High according to the same SPBD specification.

## Conclusions from the results of the protection requirements assessment

// The results achieved in the protection requirements assessment provide an indication of the further course of action for the security concept - what do these steps look like?

As we assigned Protection Levels to our assets, now we can use this information to properly identify and measure possible threats.

# Threat Modeling

// To identify and quantify the threats to the system, the results of the system analysis are combined with the identified protection needs of the business processes, data and IT components and checked for relevant threats. This can be done in a variety of ways, but a structured approach is needed to ensure that all threats are considered. The documentation of the actual modeling does not have to be reproduced in full in this document, but rather the results should be documented here.

// Common catalogs of threats (e.g., EUCS, ISO27001) can be referenced at this point.

For Threat Modeling we use STRIDE methodology. Two major business processed were considered for Threat modeling and analysis:

* SSI Backchannel Login scenario
* SSI IAT Provision scenario

Detailed Threat Model and Analysis is provided in accompanying ThreatModel\_vxx.docx document. Results were collected in the spreadsheet ThreatsMitigations\_vxx.xlsx. As it was already mentioned above, we threat modelled in detail custom endpoints and communications only. Standard authentication functions provided via OIDC/OAuth2/CIBA protocols are covered by their own security and privacy considerations documents and were not taken into account here.

## Identified Threats

// List of all identified threats to the system security.

The complete list of threats found during threat modeling is in the ThreatsMitigations document. The total number of threats found is 48. Aggregated results grouped by business process and threat type are:

* SSI Backchannel Login
  + Information Disclosure: 4 threats
  + Denial of Service: 4 threats
  + Tempering: 4 threats
  + Spoofing: 4 threats
  + Repudiation: 4 threats
  + Elevation of Privilege: 2 threats
* SSI IAT Provision
  + Information Disclosure: 5 threats
  + Denial of Service: 5 threats
  + Tempering: 6 threats
  + Spoofing: 4 threats
  + Repudiation: 4 threats
  + Elevation of Privilege: 2 threats

As SSI Backchannel Login scenario use standard OIDC protocol, a number of threats were found in [the OIDC specification](https://openid.net/specs/openid-connect-core-1_0.html#Security):

* Information Disclosure: 3 threats
* Denial of Service: no
* Tempering: 2 threats
* Spoofing: 2 threats
* Repudiation: 2 threats
* Elevation of Privilege: no

Also, some threats were identified by the underlying [OAuth2 threat model](https://datatracker.ietf.org/doc/html/rfc6819#section-4).

## Threat Analysis

// In depth analysis of identified threats to the system security (e.g., as text or by using Threat Tree Diagrams etc.)

At threat modelling the following entities, data flows, and processes were considered:

* SSI Backchannel Login
  + Entity: User Agent
  + Entity: Trust Services API (TSA)
  + Data Flow: User Agent ⬄ AAS: Backchannel Login
  + Data Flow: AAS: Backchannel Login ⬄ TSA: Policy Evaluation
  + Process: AAS: Backchannel Login
  + Process: IAM: Login with IdP
* SSI IAT provision
  + Entity: Client Service
  + Entity: Trust Services API (TSA)
  + Data Flow: Client Service ⬄ AAS: IAT Issuing
  + Data Flow: Client Service ⬄ IAM: Client Registration
  + Data Flow: AAS: IAT Issuing ⬄ TSA: Policy Evaluation
  + Process: AAS: IAT Issuing
  + Process: IAM: Client Registration

Detailed threat explanation and analysis is provided in the ThreatModel and ThreatsMitigations documents.

# Selection and Adaptation of Security Measures

// Based on the results of the threat modeling, security measures are selected and adapted in this chapter to counter the identified threats, and the resulting necessary security measures are documented. Both the previously defined scope and the security assumptions made are taken into account. Measures can always be of a technical, organizational or personnel nature.

// Common catalogs of measures (e.g., EUCS, SeAScure SDLC) can be referenced at this point.

Despite the fact that the threat analysis considered two main business processes, they revealed very similar threats and, accordingly, the means of eliminating them are also the same. The main ways to eliminate the identified threats are:

* Use TLS to protect data during transmission
* Use WAF to protect against DoS attacks
* Use security hardened, continuously monitored and up-to-date operating systems
* All logs should be collected centrally and stored in a secure manner

Together with standard measures suggested by OIDC/OAuth2 protocols:

* Pass any sensitive information between AAS and IAM in in form of signed/encrypted JWT
* Use of TLS protected channel
* Use of signed ID Token to mitigate Token Substitution attacks
* Access Token lifetimes should be kept to single use or very short lifetimes
* When used with symmetric signing or encryption operations, secret values must contain sufficient entropy to generate cryptographically strong keys

There are also several risks related to possible disclosure of all user credentials when attacker [gets access to IAM database](https://datatracker.ietf.org/doc/html/rfc6819#section-4.3.4). They are mitigated by countermeasures [proposed by IAM provider](https://www.keycloak.org/docs/latest/server_admin/#mitigating-security-threats).

A comprehensive list of all measures proposed by EUCS with their applicability to the system was compiled in [the accompanying EUCS\_Controls.xslx spreadsheet](https://gitlab.com/gaia-x/data-infrastructure-federation-services/authenticationauthorization/-/blob/main/doc/security/EUCS_Controlls.xlsx).

## Securing business processes

// What measures are taken to secure business processes?

Proposed measures to secure business processes are:

* SSI Backchannel Login
  + The software should only be run on security hardened, continuously monitored and up-to-date operating systems.
  + Use TLS and advise users that if in doubt, they should verify the TLS certificate.
  + All logs should be collected centrally and stored in a secure manner (e.g., append only logs/DBs).
  + In the event of a DoS attack, the rate at which the process accepts requests should be throttled. In addition, a DoS protection service should be deployed.
  + The process requires authentication to interact with it. In case of an application-level DoS attack the respective credentials used for the attack should be suspended.
* SSI IAT Provision
  + The software should only be run on security hardened, continuously monitored and up-to-date operating systems.
  + In addition, the IAM process should run separately from all other processes on the system to further isolate it from additional system components.
  + Use TLS and advise users that if in doubt, they should verify the TLS certificate.
  + For internal communication (with AAS: IAT Issuing), in addition to checking the TLS certificate, communication should take place via a private network.
  + All logs should be collected centrally and stored in a secure manner (e.g., append only logs/DBs).
  + In the event of a DoS attack, the rate at which the process accepts requests should be throttled. In addition, a DoS protection service should be deployed.

## Securing service components

// What measures - according to their protection needs - are taken to secure IT components?

As it was mentioned above, at this stage we do not know the environment in which the service will be deployed and cannot control the processes of its deployment and maintenance. Therefore, we can consider only software components which perform the functionality required by the service. So, the measures proposed to secure business processes are equally applicable to the service components implementing our business processes.

## Other measures

// What further security measures will be taken?

When the service will be deployed in a Cloud Provider production environment, an additional security assessment of the solution will need to be performed, taking into account the business processes for deploying and maintaining the system on the service provider's side.

# Security Evaluation

// The goal of the security evaluation is to evaluate the security measures listed in the previous chapter in terms of their effectiveness in implementing the protection goals (confidentiality, integrity including authenticity and availability) for the service's data. Additionally, any remaining risk that has not been mitigated has do be documented here.

To accomplish this task we should provide a correspondence between protection goals and threat types used in STRIDE methodology. The corresponding mapping is:

* Confidentiality: affected by Information Disclosure and Elevation of Privilege threats.
* Integrity including authenticity: affected by Tempering, Spoofing, Repudiation and Elevation of Privilege threats.
* Availability: affected by Denial-of-Service threats

## Confidentiality

// Which security measures affect (and in what way) the confidentiality protection goal?

Confidentiality should be protected with the following measures:

* Use TLS to protect data during transmission
* The software should only be run on security hardened, continuously monitored and up-to-date operating systems
* In addition, the AAS process should run separately from all other processes on the system to further isolate it from additional system components

## Integrity including Authenticity

// Which security measures affect (and in what way) the protection goal integrity including authenticity?

To protect integrity and authenticity the measures are:

* Use TLS to protect data during transmission. It is important to check the certificate of the TSA entity to ensure that the communication is with the legitimate entity. Advise users that if in doubt, they should verify the TLS certificate
* For internal communication between service components (AAS ⬄ IAM), in addition to checking the TLS certificate, communication should take place via a private network
* In order to ensure that an attacker cannot guess a valid IAT the key used for signing the JWT needs to have at least 120 bits of entropy
* When corresponding ID (IAT/request\_id/auth\_code) are consumed on use, the usage with relevant user details should be logged
* All authentication processes and associated data should be logged in a pseudonymized representation
* All logs should be collected centrally and stored in a secure manner (e.g., append only logs/DBs)
* The software should only be run on security hardened, continuously monitored and up-to-date operating systems
* In addition, the AAS process should run separately from all other processes on the system to further isolate it from additional system components

## Availability

// Which security measures affect (and in what way) the availability protection target?

The following measures were proposed to protect the service availability:

* In the event of a DoS attack, the rate at which the process accepts requests should be throttled. In addition, a DoS protection service should be deployed.
* All processes should require authentication to interact with them. In case of an application-level DoS attack the respective credentials used for the attack should be suspended.
* As an additional measure we can also propose a scaled service deployment when many service instances can be (auto-)started in order to handle increasing request rate.

# References

STRIDE: <https://www.koenig-solutions.com/blog/stride-methodology-in-threat-modelling#:~:text=What%20is%20the%20STRIDE%20Methodology,Authentication%2C%20and%20Non%2DRepudiation>.

STRIDE: <https://en.wikipedia.org/wiki/STRIDE_(security)>

SIOP Security considerations: <https://openid.net/specs/openid-connect-self-issued-v2-1_0.html#name-security-considerations>

OIDC Security considerations: <https://openid.net/specs/openid-connect-core-1_0.html#Security>

OAuth2 threat model: <https://datatracker.ietf.org/doc/html/rfc6819>

OAuth2 Security Best Current Practice: <https://datatracker.ietf.org/doc/html/draft-ietf-oauth-security-topics-16>

OWASP top 10: <https://owasp.org/www-project-top-ten/>

OIDC CIBA security considerations: <https://openid.net/specs/openid-client-initiated-backchannel-authentication-core-1_0.html#rfc.section.14>