

# GAIA-X Authentication & Authorization Service: Security Concept

## Contents

Introduction.....	3
Project Description and Goals .....	3
Purpose of the Document .....	3
Definitions and Methodology.....	3
Scope of Application.....	3
Service Description .....	4
Delimitation Criteria and Safety Assumptions .....	4
Structural Analysis.....	4
Business Processes .....	5
Data .....	5
Service Components.....	8
Data Occurrence.....	8
Evaluation of Protection Requirements .....	11
Definition of the Protection Requirement Categories. ....	11
Protection requirements assessment for business processes .....	12
Protection requirements assessment for data.....	12
Protection requirements assessment for service components .....	12
Conclusions from the results of the protection requirements assessment.....	12
Threat Modeling.....	13
Identified Threats .....	13
Threat Analysis .....	14
Selection and Adaptation of Security Measures .....	14
Securing business processes .....	15
Securing service components.....	15
Other measures .....	15
Security Evaluation .....	15
References.....	16

## 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

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

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

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.
GAIA-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

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

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.

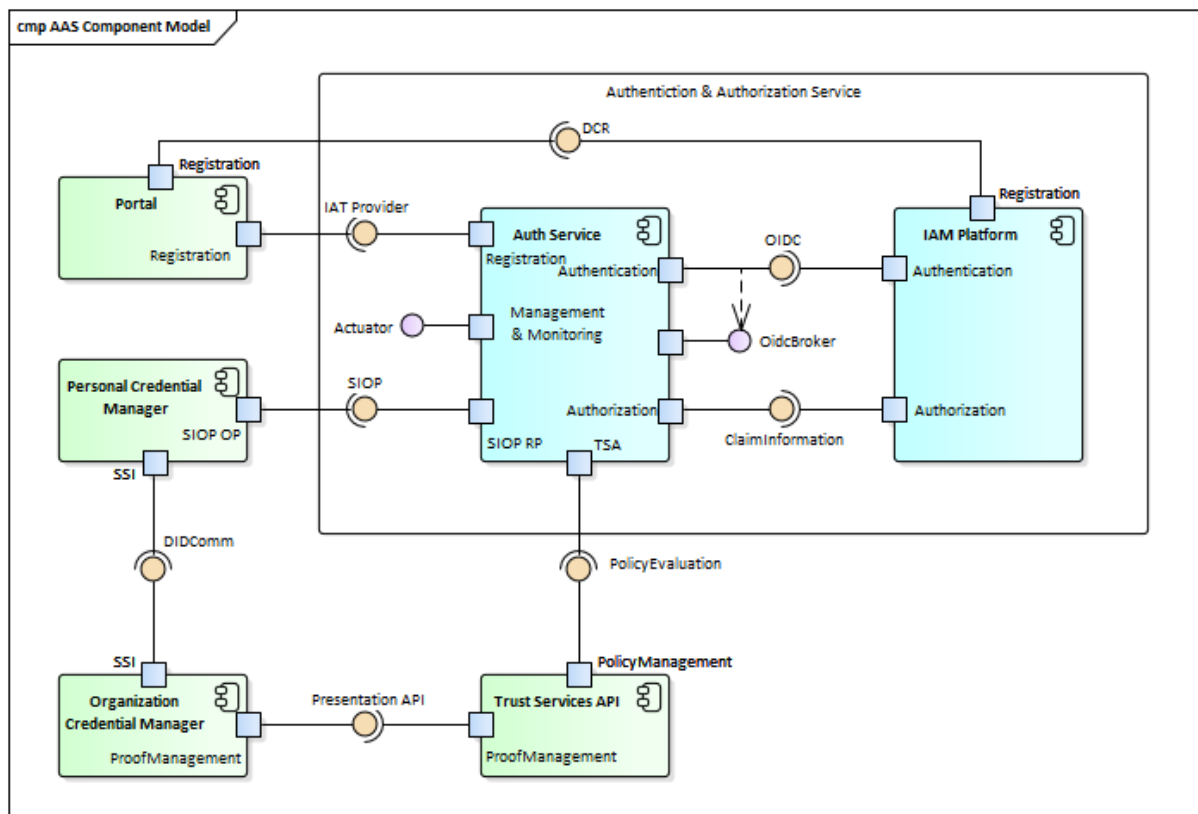
## Delimitation Criteria and Safety Assumptions

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 (see [Reference section](#) below). Major vulnerabilities identified by underlying protocols together with countermeasures are mentioned in the next chapters.

## Structural Analysis.

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

- Auth Service: major [Authentication & Authorization Service](#) component exposing endpoints required by GAIA-X LOT1 specification.
- IAM Platform: Identity and Access Management platform like keycloak, Gluu, WSO2, etc.
- [Portal](#): web application protected with AAS, implemented as GAIA-X LOT13.
- [Personal Credential Manager](#): mobile application (SSI Wallet), GAIA-X LOT2 implementation.
- [Organization Credential Manager](#): GAIA-X LOT3 implementation.
- [Trust Service API](#): GAIA-X LOT4 implementation.



## Business Processes

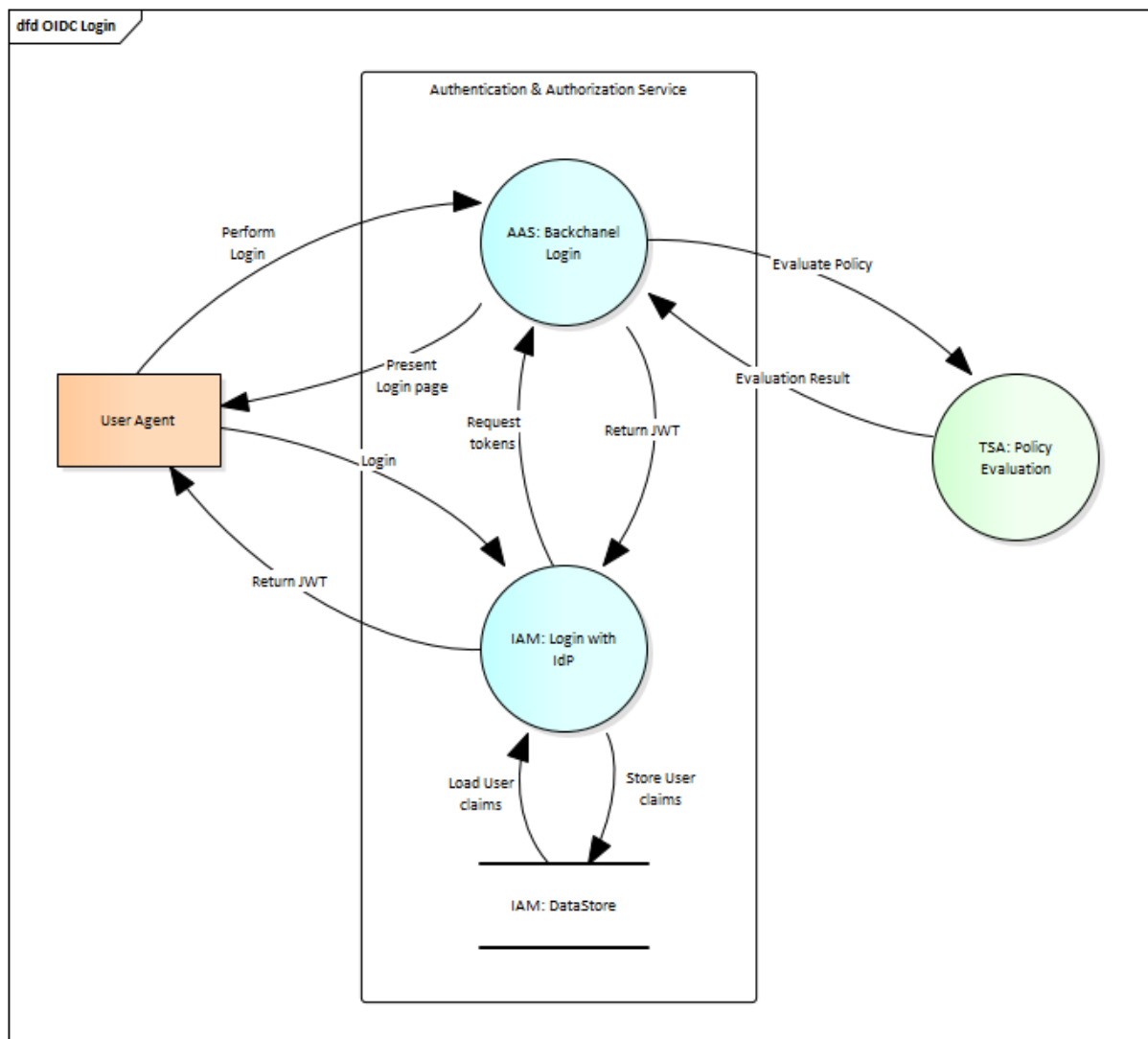
The service implements two major business functions:

- **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

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:



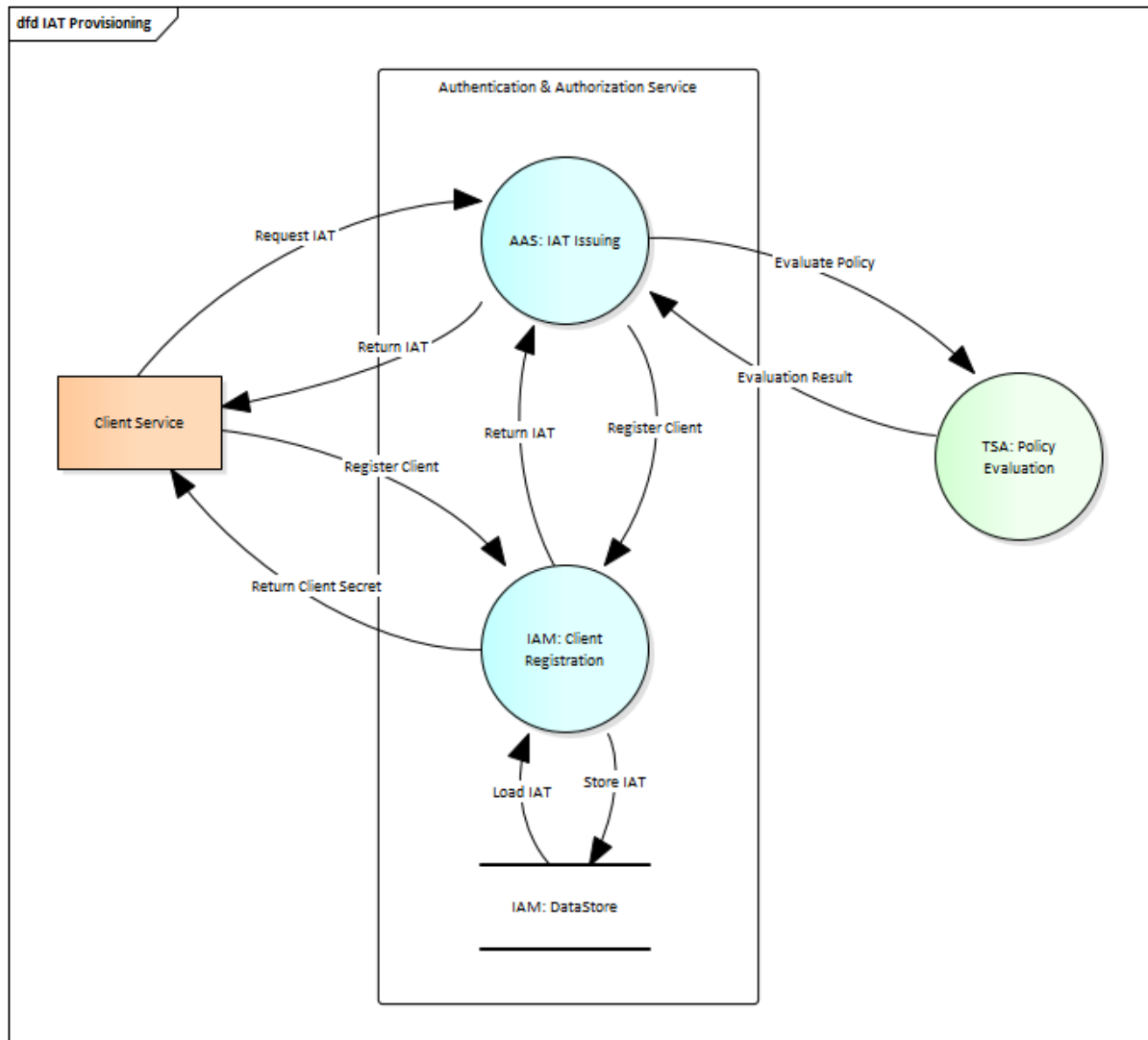
In SSI IAT Provision scenario Client Service provides its public identity data to AAS. AAS requests Service Claims from TSA and then provision these claims to IAM getting back IAT and returning it to the requesting Client Service. The IAT is a JSON Web Token (JWT) encoded with base64 algorithm. Decoded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

```

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:



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. Some of the attributes contain Personal Identifiable Information (GDPR PII).
- 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 protected application (Portal).
- 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

The service consists of two major software components:

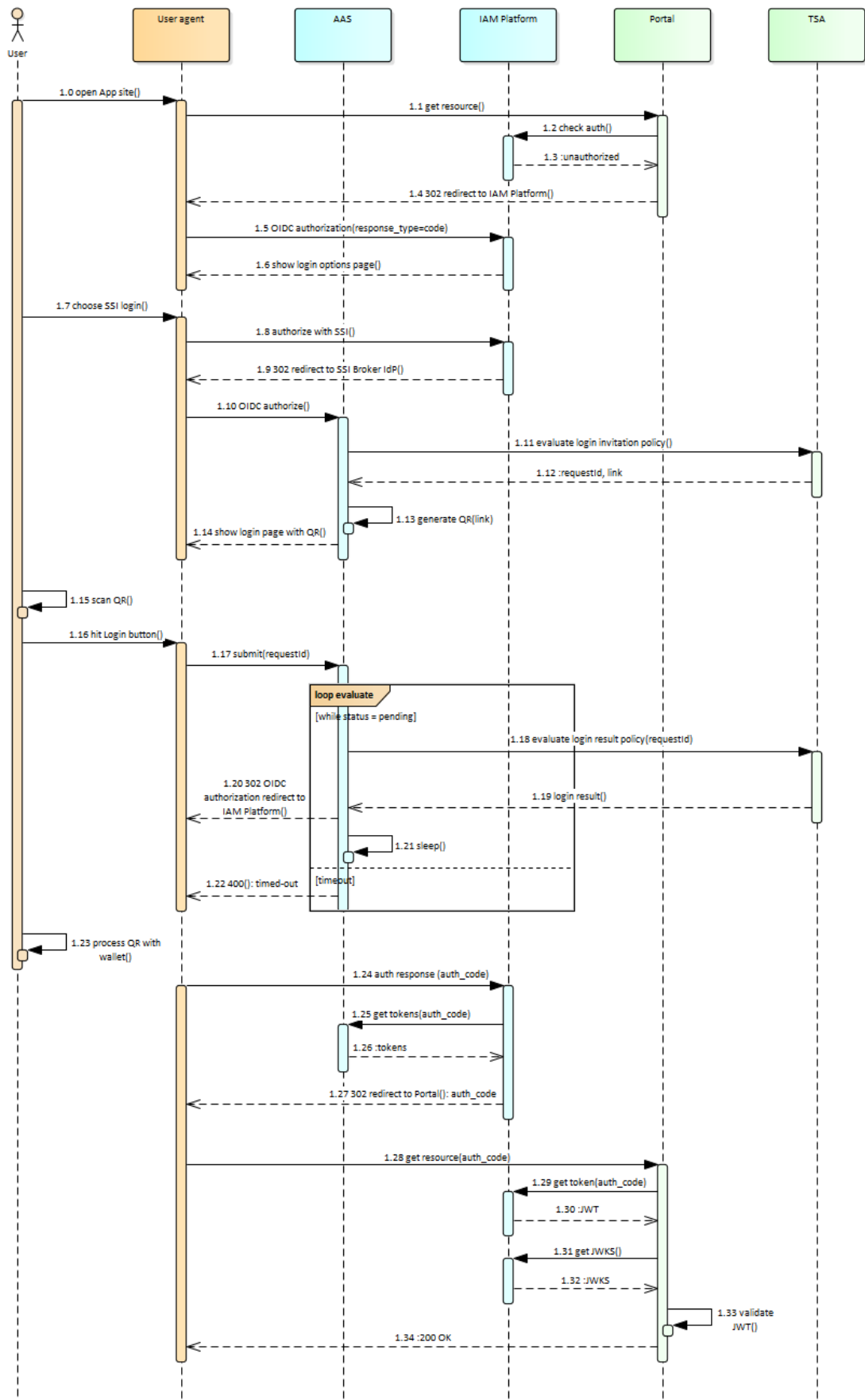
- Authentication Service: major AAS component exposing standard endpoints required by OIDC CIBA and SIOP protocols which are used in SSI Backchannel Login scenario and custom endpoints required in IAT Provision scenario. The component is implemented as a regular Spring Boot Java application. Required OpenID/OAuth2 functionality is provided by [Spring Authorization Server](#) with help of [Spring Security](#) 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

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

The SSI Backchannel login flow.

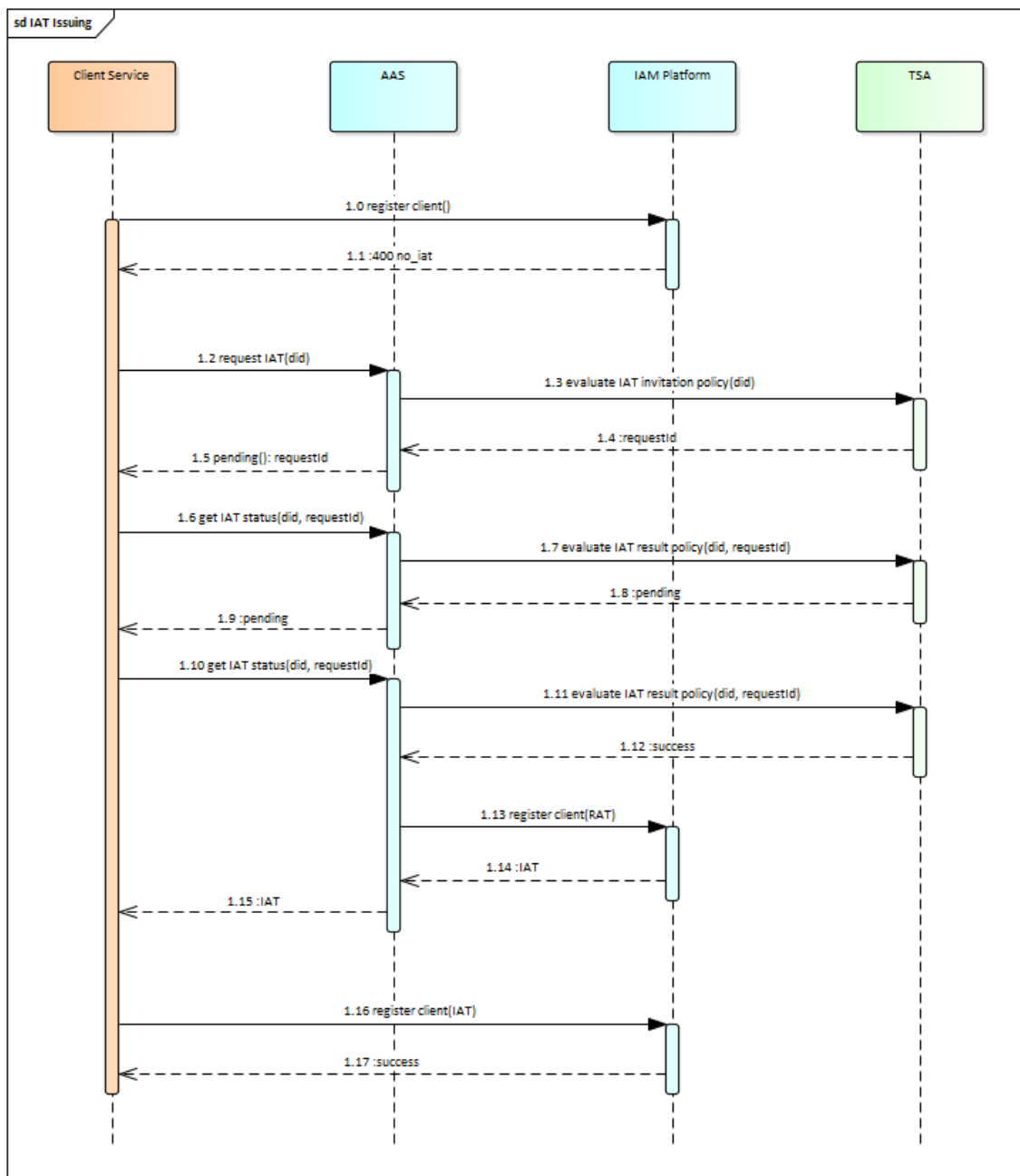
## sd SSI Backchannel Login



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.



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

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.

When determining protection requirements, it is important to consider the damage that can result from violations of the basic values of confidentiality, integrity, and availability. This is applicable when:

- Confidential information is accessed or passed on in an unauthorized manner (violation of confidentiality)
- Information is no longer correct, or systems no longer function properly (violation of integrity)
- Authorized users are prevented from accessing systems and information (violation of availability)

The protection a given object requires with regard to each of these basic values is thus based on the extent of the damage corresponding violations can cause. Since the extent of potential damage can typically not be determined in advance, we should define a number of categories suitable for our purposes and use them to differentiate between various levels of protection. The security concept standards recommend three basic categories of protection requirements:

- Normal: The effects of the damage are limited and manageable.
- High: The effects of the damage may be considerable.
- Very high: The effects of the damage may be catastrophic enough to threaten an organisation's existence.

The same security concept standards specify the following possible ramifications of a violation of the basic values:

- Violations of laws, regulations or contracts
- Impairment of the right to informational self-determination
- Impairment of a person's physical integrity
- Impairment of one's ability to perform tasks
- Negative internal or external consequences
- Financial consequences

Not all of them are applicable directly to AAS implementation, but we can measure damage scenarios using the first two, at least.

### Protection requirements assessment for business processes

Basing on the protection categories and goals defined above we measure our business processes as:

- SSI Backchannel Login
  - Confidentiality: protection category is High because the process works with User Claims which is personal data and we must keep them confidential.
  - Integrity including Authenticity: protection category is High
  - Availability: protection category is High
- SSI IAT Provisioning
  - Confidentiality: protection category is Normal because the process works only with public data (Service Claims and IAT constructed from them).
  - Integrity including Authenticity: protection category is Normal
  - Availability: protection category is High as unavailability of this service function may cause serious consequences for a cloud provider

### Protection requirements assessment for data

We measure data processed in service business processes as:

- User Claims processed in SSI Backchannel Login scenario
  - Confidentiality: protection category is High because it is personal data (like e-mail, birthdate, etc.) and must not be disclosed according to GDPR standards.
  - Integrity including Authenticity: protection level is High, for the same reason
  - Availability: protection level is High
- Client Service Claims processed in SSI IAT Provision scenario
  - Confidentiality: protection category is Normal as it is publicly available data.
  - Integrity including Authenticity: protection category is Normal
  - Availability: protection category is Normal
- Initial Access Token produced in SSI IAT Provision scenario
  - Confidentiality: protection category is Normal because the token is built from publicly available data (Service Claims).
  - Integrity including Authenticity: protection category is Normal
  - Availability: protection category is High as unavailability of IAT will cause unavailability of the whole service function

### Protection requirements assessment for service components

Service components inherit the highest protection category from underlying business processes and data they process. Therefore, we should measure protection category for both AAS service components as High.

### Conclusions from the results of the protection requirements assessment

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

## Threat Modeling

For Threat Modeling we use STRIDE methodology. Two major business processes 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

The complete list of threats found during threat modeling is in the ThreatsMitigations document. The total number of threats found is 54. Aggregated results grouped by business process and threat type are:

- SSI Backchannel Login
  - Information Disclosure: 5 threats
  - Denial of Service: 5 threats
  - Tempering: 5 threats
  - Spoofing: 4 threats
  - Repudiation: 4 threats
  - Elevation of Privilege: 2 threats
- SSI IAT Provision
  - Information Disclosure: 6 threats
  - Denial of Service: 6 threats
  - Tempering: 7 threats
  - Spoofing: 4 threats
  - Repudiation: 4 threats
  - Elevation of Privilege: 2 threats

As SSI Backchannel Login scenario uses standard OIDC protocol, a number of threats were found in [the OIDC specification](#):

- 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](#).

## Threat Analysis

At threat modelling the following entities, data flows, processes and data stores 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
  - Data Store: IAM: Data Store
- 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
  - Data Store: IAM: Data Store

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

## Selection and Adaptation of Security Measures

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](#). They are mitigated by countermeasures [proposed by IAM provider](#).

A comprehensive list of all measures proposed by EUCS with their applicability to the system was compiled in [the accompanying EUCS Controls.xlsx spreadsheet](#).

## Securing business processes

All threats found during threat analysis are explained in detail in the ThreatModel and ThreatsMitigations documents. 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

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

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

Due to the scope and restrictions of the project, an evaluation of the effectiveness and completeness of the proposed security measures cannot be made at this time. It is strongly recommended that any party wishing to deploy the project in a production environment perform a full security evaluation with respect to the deployment environment and use cases covered.

## References

STRIDE: [https://owasp.org/www-community/Threat\\_Modeling\\_Process](https://owasp.org/www-community/Threat_Modeling_Process)

SIOP Security considerations: [https://openid.net/specs/openid-connect-self-issued-v2-1\\_0.html#name-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](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](https://openid.net/specs/openid-client-initiated-backchannel-authentication-core-1_0.html#rfc.section.14)