ID	Use Case	Element Type	Element	Threat Type	Threat	Mitigation Status	Mitigation	Implementation
001	IAT Issuing	Data Flow	Client Service <-> AAS: IAT Issuing	Information Disclosure	Access to IAT	Full mitigation	Use TLS to protect data during transmission	TLS certificate configured at Ingress level in test env
002	IAT Issuing	Data Flow	Client Service <-> AAS: IAT Issuing	Denial of Service	Application level DoS of the AAS: IAT Issuing endpoint by flooding with requests	Partially mitigation	In the event of a DoS attack, the rate at which the endpoint accepts requests should be throttled. In addition, a DoS protection service should be deployed.	To be implemented in the upper level GAIA-X Component: API Gateway (WAF)
003	IAT Issuing	Data Flow	Client Service <-> AAS: IAT Issuing	Tempering	By tempering with the transmitted data an attacker could deny registration for a legitimate client service	Full mitigation	Use TLS to protect data during transmission	TLS certificate configured at Ingress level in test env
004	IAT Issuing	Data Flow	Client Service <-> IAM: Client Registration	Information Disclosure	Attacker could gain knowledge of the IAT and try to misuse it	Full mitigation	Use TLS to protect data during transmission	TLS certificate configured at Ingress level in test env
005	IAT Issuing	Data Flow	Client Service <-> IAM: Client Registration	Denial of Service	An attacker could try and flood the system with requests	Partially mitigation	The IAM: Client Registration endpoint should only be accessible with a valid IAT	Yes, implemented in IAM (keycloak)
006	IAT Issuing	Data Flow	Client Service <-> IAM: Client Registration	Tempering	Attacker could manipulate which service should be registered	Full mitigation	Use TLS to protect data during transmission	TLS certificate configured at Ingress level in test env
007	IAT Issuing	Data Flow	Client Service <-> IAM: Client Registration	Tempering	Attacker could manipulate the IAT token leading to a DoS for the respective client service trying to register	Full mitigation	Use TLS to protect data during transmission	TLS certificate configured at Ingress level in test env
008	IAT Issuing	Data Flow	AAS: IAT Issuing <-> TSA: Policy Evaluation	Information Disclosure	Access to data (e.g. DID) that could lead to an privacy issue	Full mitigation	Use TLS to protect data during transmission	TLS certificate configured at Ingress level in test env
009	IAT Issuing	Data Flow	AAS: IAT Issuing <-> TSA: Policy Evaluation	Denial of Service	An attacker could try and flood the system with requests	Full mitigation	The TSA: Policy Evaluation endpoint should only be accessible after a mutual authentication	Two-way certificates, must be considered at integration phase with TSA Component
010	IAT Issuing	Data Flow	AAS: IAT Issuing <-> TSA: Policy Evaluation	Tempering	By tempering with the transmitted data an attacker could manipulate the evaluation results returned by the TSA: Policy Evaluation and thus would be able to register a potentially malicious client or deny the registration of a legitimate client service	Full mitigation	Use TLS to protect data during transmission	TLS certificate configured at Ingress level in test env
011	IAT Issuing	Entity	Client Service	Spoofing	Attacker could guess the IAT and try to register a malicious client service	Full mitigation	In order to ensure that an attacker can not guess a valid IAT the key used for signing the JWT needs to have at least 120 bit of entropy.	keycloak use RS256 algorithm for JWKS protection
012	IAT Issuing	Entity	Client Service	Repudiation	A user could deny having used their IAT	Full mitigation	The IAT is consumed on use, the usage with relevant user details should be logged	Implemented at DEBUG logging level
013	IAT Issuing	Entity	TSA: Policy Evaluation	Spoofing	Should an attacker succeed in spoofing the "TSA: Policy Evaluation", the attacker may be able to register a potentially malicious client or deny registration of a legitimate client service by returning the appropriate evaluation results.	Full mitigation	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	TLS certificate configured at Ingress level in test env. Integrity with TSA Component to be considered at integration phase
014	IAT Issuing	Entity	TSA: Policy Evaluation	Repudiation	TSA: Policy Evaluation send a incorrect authentication result	Partially mitigation	All authentication processes and associated data should be logged in a pseudonymized representation.	Implemented at DEBUG logging level
015	IAT Issuing	Process	AAS: IAT Issuing	Spoofing	If an attacker could spoof the IAT Issuing process, they could intercept an IAT request and piggyback on the real authentication of a client service.	Full mitigation	Use TLS and advise users that if in doubt, they should verify the TLS certificate.	TLS certificate configured at Ingress level in test env

016	IAT Issuing	Process	AAS: IAT Issuing	Tempering	If an attacker can alter data in this process, he could approve or deny the registration for any client service.	Partially mitigation	The software should only be run on security hardened, continuously monitored and up-to-date operating systems.	To be considered at deployment phase in cloud provider env
017	IAT Issuing	Process	AAS: IAT Issuing	Repudiation	If the logs generated by the system are stored on the same system, the logs could be corrupted in the event of a system failure or maliciously manipulated by an attacker.	Partially mitigation	All logs should be collected centrally and stored in a secure manner (e.g. append only logs/DBs).	To be considered at deployment phase in cloud provider env
018	IAT Issuing	Process	AAS: IAT Issuing	Information Disclosure	Attacker could steal an IAT token and use the token to register a malicious client before the legitimate user can use the token	Partially mitigation	The software should only be run on security hardened, continuously monitored and up-to-date operating systems.	To be considered at deployment phase in cloud provider env
019	IAT Issuing	Process	AAS: IAT Issuing	Denial of Service	As the process does accept unauthenticated requests that have a certain degree of leverage (a certain amount of work has to be done for every request), a possible DoS attack via request flooding could make the service unavailable.	Partially mitigation	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.	To be implemented in the upper level GAIA-X Component: API Gateway (WAF)
020	IAT Issuing	Process	AAS: IAT Issuing	Elevation of Privilege	If an attacker is able to extended their privileges they could access all functionality of the AAS process (including functionality from other use cases)	Partially mitigation	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.	To be considered at deployment phase in cloud provider env
021	IAT Issuing	Process	IAM: Client Registration	Spoofing	By spoofing this process, the attacker could gain access to the RAT (send by AAS: IAT Issuing) or the IAT (send by the Client Service), these could be used to authenticate in the context of the respective user.	Partially mitigation	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.	TLS certificate confiured at Ingress level in test env. Communication via private network to be considered at deploymenmt phase in cloud provider env
022	IAT Issuing	Process	IAM: Client Registration	Tempering	If an attacker can alter data in this process, he could approve or deny the registration for any client service	Partially mitigation	The software should only be run on security hardened, continuously monitored and up-to-date operating systems.	To be considered at deployment phase in cloud provider env
023	IAT Issuing	Process	IAM: Client Registration	Repudiation	If the logs generated by the system are stored on the same system, the logs could be corrupted in the event of a system failure or maliciously manipulated by an attacker.	Partially mitigation	All logs should be collected centrally and stored in a secure manner (e.g. append only logs/DBs).	To be considered at deployment phase in cloud provider env
024	IAT Issuing	Process	IAM: Client Registration	Information Disclosure	An attacker could gain access to the IAT that are processed and stored by this process.	Partially mitigation	The software should only be run on security hardened, continuously monitored and up-to-date operating systems.	To be considered at deployment phase in cloud provider env
025	IAT Issuing	Process	IAM: Client Registration	Denial of Service	An attacker could try to flood the process with requests.	Partially mitigation	The process requires authentication to interact with it. Since the token used for authentication is consumed when used, an attacker would have to acquire a new token for each request.	To be implemented in the upper level GAIA-X Component: API Gateway (WAF)

026	IAT Issuing	Process	IAM: Client Registration	Elevation of Privilege	If an attacker is able to extended their privileges they could access all functionality of the IAM process (including functionality from other use cases). This includes access to the PII stored in the IAM: Datastore	Partially mitigation	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.	To be considered at deployment phase in cloud provider env
027	IAT Issuing	Data Store	IAM: Data Store	Tempering	By tempering with the IATs stored in the IAM: Data Store an attacker could effectively make it impossible to register new client services within the system.	Partially mitigation	The database should only be run on security hardened, continuously monitored and up-to-date operating systems.	To be considered at deployment phase in cloud provider env
028	IAT Issuing	Data Store	IAM: Data Store	Information Disclosure	An attacker that would be able to access data stored on the IAM: Data Store would be able to access client registration information and IATs and thus would be able to register possible malicious client services.	Partially mitigation	The database should only be run on security hardened, continuously monitored and up-to-date operating systems. Additionally the database permissions should be chosen as restrictive as possible.	To be considered at deployment phase in cloud provider env
029	IAT Issuing	Data Store	IAM: Data Store	Denial of Service	In case of a DoS attack on the IAM: Data Store the system would not be longer able to accept client registrations, as it would not be possible to store the respective IATs.	Full mitigation	The Data Store should only be accessible via a private network.	To be considered at deployment phase in cloud provider env
030	SSI Backchannel login	Data Flow	User Agent <-> AAS: Backchannel Login	Information Disclosure	Attacker could steal a RequestID	Full mitigation	Use TLS to protect data during transmission	TLS certificate configured at Ingress level in test env
031	SSI Backchannel login	Data Flow	User Agent <-> AAS: Backchannel Login	Denial of Service	Application level DoS of the AAS: Backchannel Login endpoint by flooding with requests	Partially mitigation	In the event of a DoS attack, the rate at which the endpoint accepts requests should be throttled. In addition, a DoS protection service should be deployed.	To be implemented in the upper level GAIA-X Component: API Gateway (WAF)
032	SSI Backchannel login	Data Flow	User Agent <-> AAS: Backchannel Login	Tempering	An attacker could manipulate the link contained in the QR code. This could either lead to a DoS for the user or the user could be tricked to authenticated with a malicious endpoint under the control of the attacker.	Full mitigation	Use TLS to protect data during transmission	TLS certificate configured at Ingress level in test env
033	SSI Backchannel login	Data Flow	AAS: Backchannel Login <-> TSA: Policy Evaluation	Information Disclosure	Even though only publicly known and accessible information is transmitted between these endpoints, it would still be a privacy issue if an attacker would be able to get access to the communicated information.	Full mitigation	Use TLS to protect data during transmission	TLS certificate configured at Ingress level in test env
034	SSI Backchannel login	Data Flow	AAS: Backchannel Login <-> TSA: Policy Evaluation	Denial of Service	An attacker could try and flood the system with requests	Full mitigation	The TSA: Policy Evaluation endpoint should only be accessible after a mutual authentication	Two-way certificates, must be considered at integration phase with TSA Component
035	SSI Backchannel login	Data Flow	AAS: Backchannel Login <-> TSA: Policy Evaluation	Tempering	By tempering with the transmitted data an attacker could manipulate the evaluation results returned by the TSA: Policy Evaluation and thus would be able to register a potentially malicious client or deny the registration of a legitimate client service	Full mitigation	Use TLS to protect data during transmission	TLS certificate configured at Ingress level in test env

036	SSI Backchannel login	Entity	User Agent	Spoofing	Spoofing the User Agent could only be achieved with knowledge of the RequestID. An attack would either have to guess the RequestID (UUID) or use another vulnerability to gain knowledge of the RequestID.	Full mitigation	Use a CSPRNG with enough entropy to generate the IAT. The random part of the IAT should have at least a size of 120 Bit	keycloak use RS256 algorithm for JWKS protection
037	SSI Backchannel login	Entity	User Agent	Repudiation	User Agent could deny having used their RequestID or auth_code	Partially mitigation	The RequestID/auth_code are consumed on use, the usage with relevant user details should be logged	Implemented at DEBUG logging level
038	SSI Backchannel login	Entity	TSA: Policy Evaluation	Spoofing	If an attacker could spoof the TSA: Policy Evaluation process, they could intercept an authentication request and piggyback on the real authentication of a User Agent to authenticate their own malicious User Agent.	Full mitigation	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	TLS certificate configured at Ingress level in test env. Integrity with TSA Component to be considered at integration phase
039	SSI Backchannel login	Entity	TSA: Policy Evaluation	Repudiation	TSA: Policy Evaluation send a incorrect authentication result	Partially mitigation	All authentication processes and associated data should be logged in a pseudonymized representation.	Implemented at DEBUG logging level
040	SSI Backchannel login	Process	AAS: Backchannel Login	Spoofing	If an attacker could spoof the AAS: Backchannel Login process, they could intercept an authentication request and piggyback on the real authentication of a User Agent to authenticate their own malicious User Agent.	Full mitigation	Use TLS and advise users that if in doubt, they should verify the TLS certificate.	TLS certificate configured at Ingress level in test env
041	SSI Backchannel login	Process	AAS: Backchannel Login	Tempering	If an attacker can alter data in this process, he could approve or deny the authentication for any User Agent.	Partially mitigation	The software should only be run on security hardened, continuously monitored and up-to-date operating systems.	To be considered at deployment phase in cloud provider env
042	SSI Backchannel login	Process	AAS: Backchannel Login	Repudiation	If the logs generated by the system are stored on the same system, the logs could be corrupted in the event of a system failure or maliciously manipulated by an attacker.	Partially mitigation	All logs should be collected centrally and stored in a secure manner (e.g. append only logs/DBs).	To be considered at deployment phase in cloud provider env
043	SSI Backchannel login	Process	AAS: Backchannel Login	Information Disclosure	An attacker that can access the data processed by this process, is able to steal the RequestID, auth_code or the authentication token used to access resources in the scope of the respective user.	Partially mitigation	The software should only be run on security hardened, continuously monitored and up-to-date operating systems.	To be considered at deployment phase in cloud provider env
044	SSI Backchannel login	Process	AAS: Backchannel Login	Denial of Service	As the process does accept unauthenticated requests that have a certain degree of leverage (a certain amount of work has to be done for every request), a possible DoS attack via request flooding could make the service unavailable. In this case no new Client Services can be registered in the system	Partially mitigation	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.	To be implemented in the upper level GAIA-X Component: API Gateway (WAF)
045	SSI Backchannel login	Process	AAS: Backchannel Login	Elevation of Privilege	As the AAS: Backchannel Login is separated from all other processes an attacker which can escalate their privileges could only access data and functionality of the AAS: Backchannel Login.	Partially mitigation	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.	To be considered at deployment phase in cloud provider env

046	SSI Backchannel login	Process	IAM: Login with IDP	Spoofing	If an attacker is able to spoof the IAM: Login with IDP process, they could gain access to any auth_codes send by the User Agent and use this to authenticate a malicious User Agent with the system.	Partially mitigation	Use TLS and advise users that if in doubt, they should verify the TLS certificate.	TLS certificate configured at Ingress level in test env
047	SSI Backchannel login	Process	IAM: Login with IDP	Tempering	If an attacker can alter data in this process, he could approve or deny the authentication for any User Agent.	Partially mitigation	The software should only be run on security hardened, continuously monitored and up-to-date operating systems.	To be considered at deployment phase in cloud provider env
048	SSI Backchannel login	Process	IAM: Login with IDP	Repudiation	If the logs generated by the system are stored on the same system, the logs could be corrupted in the event of a system failure or maliciously manipulated by an attacker.	Partially mitigation	All logs should be collected centrally and stored in a secure manner (e.g. append only logs/DBs).	To be considered at deployment phase in cloud provider env
049	SSI Backchannel login	Process	IAM: Login with IDP	Information Disclosure	An attacker that can access the data processed by this process, is able to steal the authentication token used to access resources in the scope of the respective user.	Partially mitigation	The software should only be run on security hardened, continuously monitored and up-to-date operating systems.	To be considered at deployment phase in cloud provider env
050	SSI Backchannel login	Process	IAM: Login with IDP	Denial of Service	An attacker could try to flood the process with requests.	Partially mitigation	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.	To be implemented in the upper level GAIA-X Component: API Gateway (WAF)
051	SSI Backchannel login	Process	IAM: Login with IDP	Elevation of Privilege	As the IAM: Login with IDP is separated from all other processes an attacker which can escalate their privileges could only access data and functionality of the IAM: Login with IDP	Partially mitigation	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.	To be considered at deployment phase in cloud provider env
052	SSI Backchannel login	Data Store	IAM: Data Store	Tempering	By tempering with the User Claims stored in the IAM: Data Store an attacker could manipulate the stored PII or other attributes and possible disrupt or misuse the service.	Partially mitigation	The database should only be run on security hardened, continuously monitored and up-to-date operating systems.	To be considered at deployment phase in cloud provider env
053	SSI Backchannel login	Data Store	IAM: Data Store	Information Disclosure	An attacker that would be able to access data stored on the IAM: Data Store would be able to access PII of all users registered with the system.	Partially mitigation	The database should only be run on security hardened, continuously monitored and up-to-date operating systems. Additionally the database permissions should be chosen as restrictive as possible.	To be considered at deployment phase in cloud provider env
054	SSI Backchannel login	Data Store	IAM: Data Store	Denial of Service	In case of a DoS attack on the IAM: Data Store the system would not be longer able to process authentication actions, thus disrupting the whole SSI backchannel login.	Full mitigation	The Data Store should only be accessible via a private network.	To be considered at deployment phase in cloud provider env