Three Steps to integrate the German eIDAS-Middleware

Version 1.1

30. April 2021

The eIDAS integration of the German eID scheme is done via the middleware integration model in accordance with the eIDAS Technical specifications. For this purpose, Germany provides a middleware (*German eIDAS-Middleware*) that is operated by other Member States (MS). This document describes the steps to perform the integration of the German middleware for public sector services of other MS.

Responsible contact person for the integration is the German Point of Single Contact (PoSC) of the Federal Ministry of the Interior (*DV2@bmi.bund.de*). The PoSC will provide MS with all necessary information and may delegate the process to corresponding experts and institutions.

Steps

1 Middleware provisioning

The German middleware can be obtained in the following ways:

1. The supplier of the German middleware provides a public repository for downloading the middleware: *https://github.com/Governikus/eidas-middleware*.
2. The German middleware is published in conjunction with the CEF/DIGIT eIDAS node package.

Test ID Cards will be sent to you for testing of the successful setup in step 2.

Please contact eid@bsi.bund.de to start the integration process.

Contact: eid@bsi.bund.de

The German middleware is delivered together with the eIDAS-Middleware User Guide which includes the installation and configuration description.

The German middleware is provided as preconfigured Virtual Machine, Docker Image and Spring Boot Application under EUPL, according to the eIDAS Technical Specifications.

2 Installation and testing

Install the German middleware according to the User Guide.

As part of the installation, the German middleware needs to be configured according to the respective parameters of the operational environment:

- Configure URLs, metadata and certificates.
- For installation and testing with the testing cards, the necessary material will be provided by the middleware supplier.
- For the production system with real eIDs, the necessary material will be issued as described in the next step.

The setup takes usually not more than 1-2 days.

Our supplier Governikus GmbH will support the whole installation process. The support is in operation during business hours.

3 Migration to the production system

In order to ensure that certificates are issued to the correct entities, issuance of authorization certificates requires an identification of the certificate holder. In the context of public sector bodies under eIDAS, identification of the authorized MS Representative is done via the mechanisms specified within the eIDAS cooperation network by the German PoSC or his/her commissioner. The Member State Representative and the German PoSC or his/her commissioner may also exchange S/MIME or pgp certificates for a trustworthy communication.

Our supplier Governikus GmbH will support the whole technical part of the registration process. The support is in operation during business hours.

After successful identification, the issuance process is as follows:

- The Member State generates TLS certificates for PKI communication of the German middleware with the corresponding authorisation CA and the identified Member State Representative transmit the TLS certificates for PKI communication of the German middleware and the TLS certificates of the German middleware (to be included in the authorisation certificate for online authentication) to the German PoSC or his/her commissioner.
- The German PoSC or his/her commissioner verifies the certificates (with the identified Member State Representative) and forwards the TLS certificates to the authorisation CA. The TLS certificates of the authorisation CA are already installed on the German middleware as part of the initialisation script.
- The Member State initiates generation of an initial certificate signing request for the production environment (automatically generated by the German middleware) and submission of request via the PKI interface to the authorisation CA.
- As soon as registration data has been configured at the Authorisation CA, the Member State initiates generation of an initial certificate signing request for the production environment (automatically generated by the German middleware) and submission of request via the PKI interface to the Authorisation CA.
- The Authorisation CA issues the authorization certificate. It sends the initial authorization certificate via the PKI communication interface to the German middleware. Afterwards, the German middleware is ready for production.

The PoSC is available under DV2@bmi.bund.de while the commissioner is available under eid@bsi.bund.de.

After completion of this registration process, authorisation certificates and revocation lists will be updated automatically by the German middleware.

Our supplier Governikus GmbH will support the whole installation process. The support is in operation during business hours.