

OZG-Cloud | Bayern-ID end-to-end process

Summary

Users (Antragsteller) that complete online forms using the Bayern-ID login method could in the future communicate with the authorities via OZG-Cloud and Application Room (Antragsraum). If the application is incomplete, eg information or documents are missing, the case worker can send a notification (email) to the user (Antragsteller) via Bayern-ID postbox. The User can access the Application Room via a link in the notification, where the application can be complemented with the missing data and passed on to the case worker. If an application contains sensitive data, a TrustLevel configuration defines which login method can - or must - be used to access the application. The TrustLevel is only relevant in the Bayern-ID end-to-end process if a second login with Bayern-ID is avoided with the use of Single-Sign-On functionality

Content

- [Summary](#)
 - [Content](#)
 - [User Flow](#)
 - [Business Description](#)
 - [Background Information / First draft](#)
 - [Key Documents](#)
 - [Supported authentication methods and request types](#)
 - [Connecting Bayern-ID](#)
 - [Summary](#)
 - [Process for the user of Bayern ID Login & the Service Provider](#)
 - [Supported Service Provider](#)
 - [Important Documents](#)
 - [Open Questions](#)
 - [Specification](#)
 - [Use Case](#)
 - [UX/UI-Design](#)
 - [Requirements](#)
 - [Page History](#)
-

User Flow

1. User completes an application and sends it
 2. The application is visible in Alfa
 3. The Case Worker processes the application form in Alfa
 4. If the application is incomplete, the Case Worker sends a notification (email) to the user via Bayern-ID
 5. The notification (email) is visible in the user's postbox account in Bayern-ID. Bayern-ID sends a separate mail notification to the provided email address (not relevant for Application Room)
 6. The user opens the notification in Bayern-ID and clicks on the link to Application Room (Antragsraum)
 7. Without SSO functionality, the user logs in again (SSO is not part of the MVP)
 8. After successful login the user:
 - a. sees the messages matching the defined TrustLevel (if defined). [BUP:OZG-Cloud](#)
 - b. sees an error message alerting the user to the fact that he/she has used a login method that does not conform to the TrustLevel (too low). Note! All messages that have the **same or lower** TrustLevel are shown
 9. If the TrustLevel prevents the user for seeing the message, he/she will be prompted to log in again with the appropriate method
 10. The user opens the message and completes the necessary action
 11. The process can be re-iterated as long as the case is still open
-

Business Description

Background Information / First draft

If the application contains sensitive data, the form provider can, but must not, configure a TrustLevel. The TrustLevel (Level-1, Level-3 or Level-4) defines which login method can or must be used to access the application. If the form provider configures a TrustLevel, this must be passed on to OZG-Cloud when the user sends the application.

The MVP will not allow for Single-Sign-On functionality with Bayern-ID and a second login is necessary.

Key Documents

If the chosen login method does not match, or is lower than, the security level (TrustLevel), the message linked to this application is not shown in Application Room (Antragsraum). The Application Room only retrieves (and shows) messages relating to applications where the security level is met. Note! If the user has more than one application, it can happen that messages relating to applications other than the one clicked on via Bayern_ID, are shown, if the security level is met for those, but not the message that he /she wanted to access.

Supported authentication methods and request types

Bayern-ID documentation: P:\StMD-BUP\12_Interfaces\BayernID

Bezeichnung	Bedeutung für Drittanwendungen
STORK-QAA-Level-1	aktuelle Authentisierung mittels Benutzername/Passwort; registrierte Attributdaten ohne hoheitliche Prüfung (= selbstregistriertes Bürgerkonto bzw. eIDAS-Äquivalent)
STORK-QAA-Level-3	aktuelle Authentisierung mittels Authega-Zertifikat oder Elster Zugang; registrierte Attributdaten aus dem Melderegister (= Authega/Elster-registriertes Bürgerkonto bzw. eIDAS-Äquivalent)
STORK-QAA-Level-4	aktuelle Authentisierung mittels Online-Ausweisfunktion (ePA, eAT, EU-Karte); registrierte Attributdaten aus dem Ausweismittel (= nPA-registriertes Bürgerkonto bzw. eIDAS-Äquivalent)

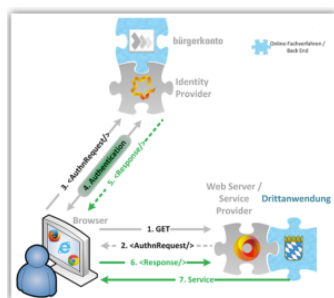
Check "Das Servicekonto im Bayerischen Portal Verband" in the section important documents.

Connecting Bayern-ID

Summary

In Bayern Portal citizens activate individual user accounts on the BayernPortal and manage their personal data and additional information there. The personal data fields for the citizen account are either filled in voluntarily (when using a user name/password pair) or automatically when using the BayernPortal for the first time, e.g. using an ID card.

Specialised portals as so-called third-party applications in the Bavarian Portal Network (like Antragsraum) connect indirectly to the BayernPortal via defined standard protocols and benefit from the centralised management of personal user data in the user account in the interests of data economy. This means that re-registration in the connected third-party applications is no longer necessary.



Process for the user of Bayern ID Login & the Service Provider

The authentication and authorisation process of service users in interaction with the open infrastructure and a third-party application connected to it. The illustrated process in seven sub-steps follows the internationally widespread standards of the OASIS Consortium, as they are also used in the core of the eCard API of the new German electronic ID card nPA.

The specialised portal then sends an authentication request to the BayernID Identity Provider as the authentication instance and the user is redirected there.

This currently takes the form of an OASIS SAMLv2-compliant authentication request via HTTP-REDIRECT or HTTP-POST via the user's browser (*step 2*). This request is not sent directly to the identity provider, but indirectly via the service requester's browser (*step 3*).

The identity provider now asks the service requester to identify himself to him as a known user using a preselected or freely authentication procedure to identify himself as a known user.

Only in the course of a positive authentication (*step 4*), the identity provider creates a response message, which is expanded using the data stored for the person in the user account. From this point onwards, the service user can legally recognised as an authenticated user within the infrastructure of the Bavarian Portal Network.

The generated response message is encrypted as a SAML response (BSI-compliant) and signed with the inclusion of signed in *step 5* to the browser of the potential service user. From there, the SAML response is forwarded to the third-party application.

The service provider receives the SAML response (*step 6*) via HTTP POST on a specially publicised endpoint within the third-party application and first checks the message for authenticity and integrity. Only then does the third-party application assesses whether the content of the response message from the identity provider fulfils the further requirements of the specialist procedure

The service provider then grants access to the initially protected resource (e.g. send function of the request or personal data view) and executes the original access request. The response is generated on the associated application server and sent to the service user's browser (*step 7*).

Supported Service Provider

Service providers must implement one of the two request types HTTP-REDIRECT or HTTP-POST-Binding, as well as act as HTTP-POST endpoint for SAML v2 tokens (AssertionConsumerService Location).

This endpoint handling for the response is generally possible in two ways: via direct token generation and utilisation within the specialist application (e.g. via open source libraries) via indirect token generation and utilisation using a reverse proxy (e.g. via configurable implementations from various manufacturers) before the specialised application.

More technical details in the document "Das Servicekonto im Bayerischen Portal Verband"

Important Documents



Open Questions



Mockups are needed for the error message if the security level has not been met

Specification

Use Case

UX/UI-Design

Requirements

Tickets:

Technical Documentation: [?](#)

Page History

Version	Date	Author	Comment
8	08.11.2023 08:39	Katharina Schlia	
7	07.11.2023 17:08	Katharina Schlia	
6	07.11.2023 16:53	Katharina Schlia	
5	07.11.2023 16:49	Katharina Schlia	
4	07.11.2023 16:42	Katharina Schlia	