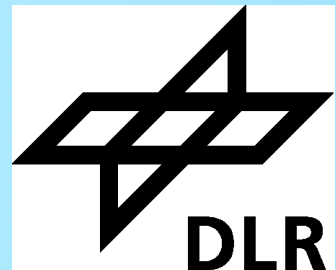


IDENTITY FEDERATIONS AT DLR EOC

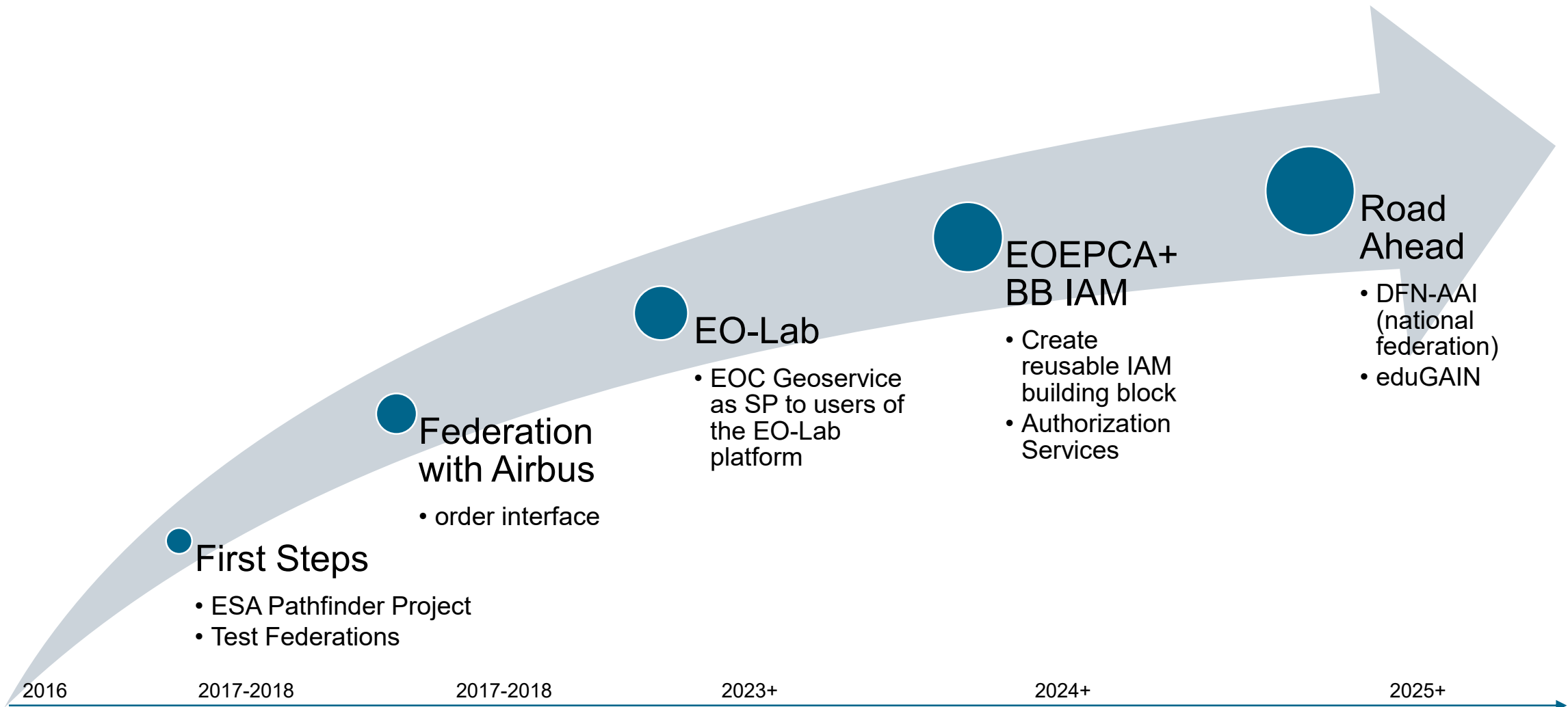
Status and Outlook



Ulrich Raape
Earth Observation Center EOC, German Aerospace Center DLR
CEOS-WGISS #58, Sioux Falls, United States & online
October 17th, 2024



Identity Federations AT DLR EOC

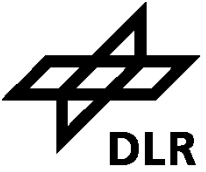


Identity Federations AT DLR EOC: The EOC IAM solution

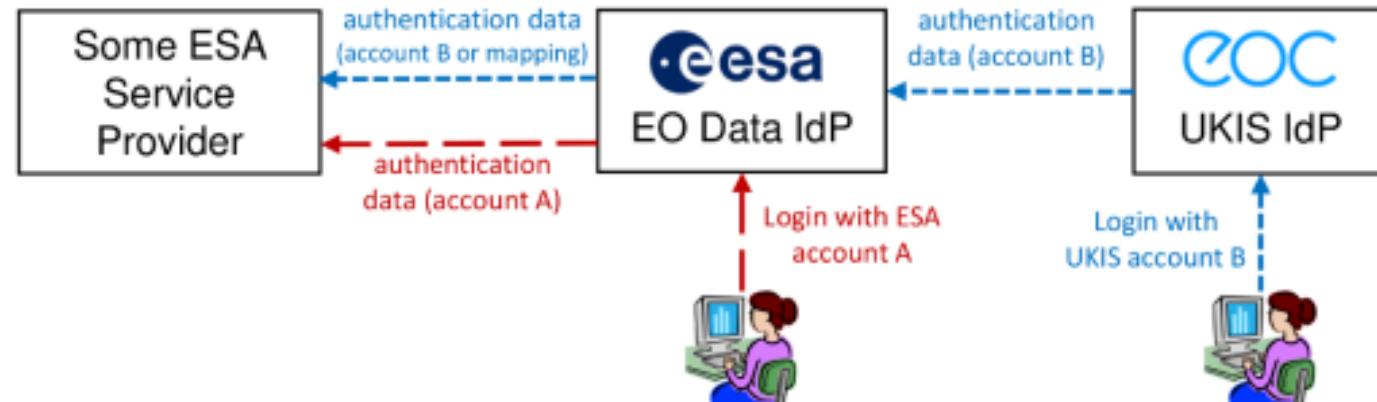


- 2016+: EOC IAM solution „User Management System“ (UMS) protects
 - German Satellite Data Archive (Deutsches Satellitendaten-Archiv D-SDA)
 - EOWEB GeoPortal (EGP) <https://eoweb.dlr.de>
 - EOC Geoservice <https://geoservice.dlr.de>
 - EnMAP Hyperspectral Mission Instrument Planning Portal <https://planning.enmap.org>
 - Ionosphere Monitoring and Prediction Center (IMPC) <https://impc.dlr.de>
 - ... and a growing number of additional systems and datasets
- Status 2024: approx. 28.000 accounts
- Approach to account “design”:
 - Initially: one account type per protected dataset/system mainly for historical and license reasons
 - Need to move towards single-sign-on (one account for n services)
 - Next level: Identity Federations

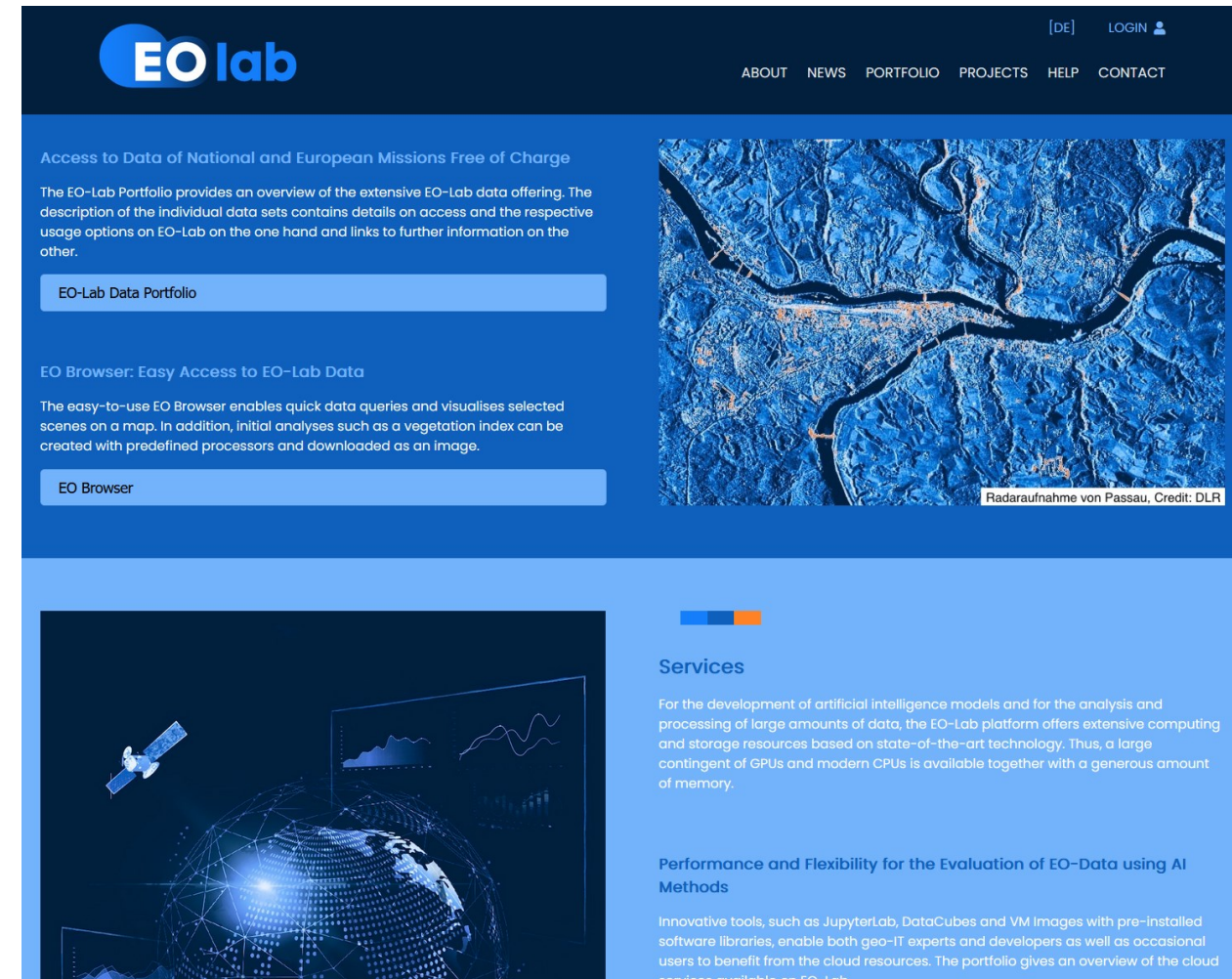
Identity Federations AT DLR EOC: The Beginning



- 2017-2018: ESA Pathfinder Project „Identity Federation – Deutschland“ (IFed-D)
 - Identity Federation Demonstrator
 - Change Detection Service as SP on DLR side
 - Analysis of Privacy Implications

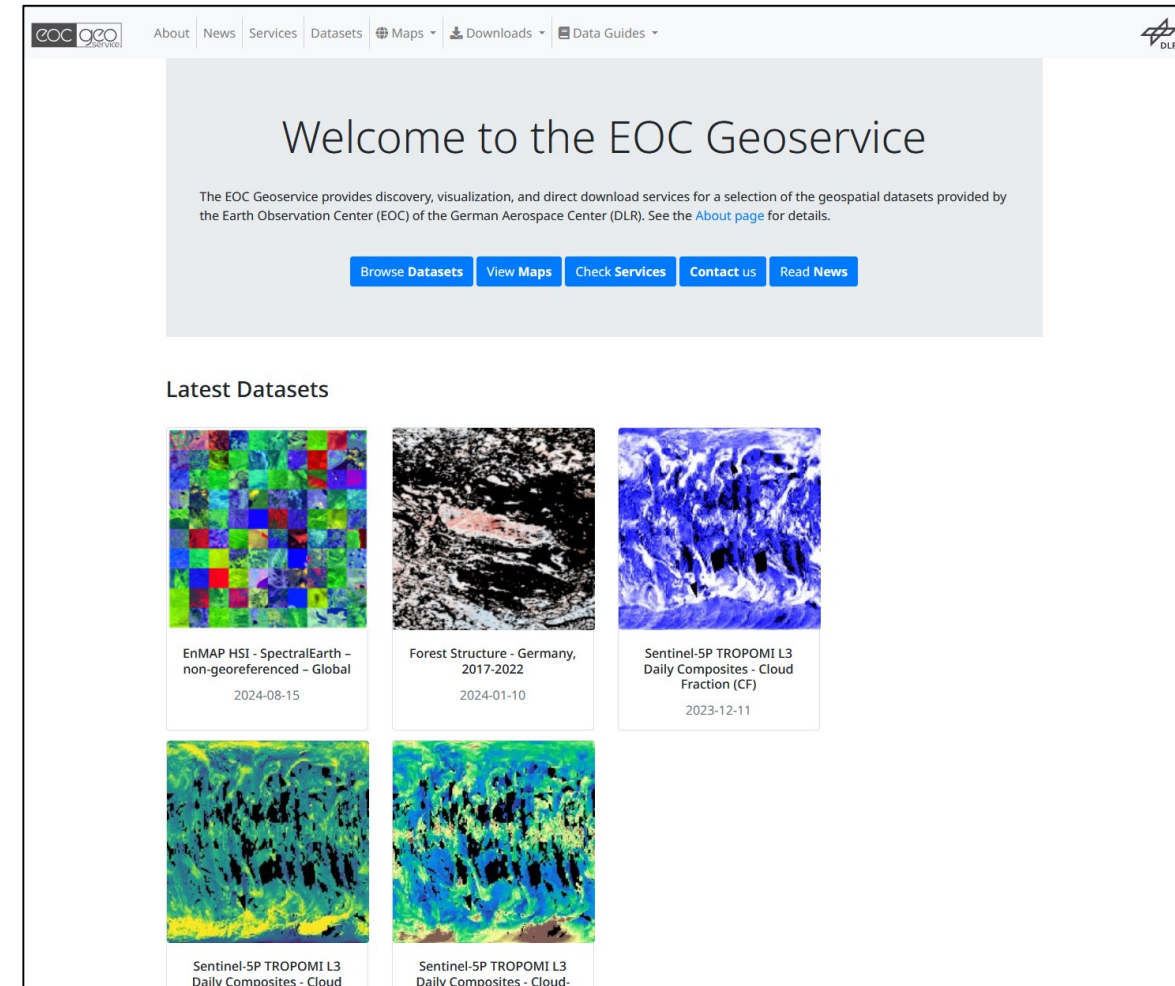


- The EO-Lab cloud is part of the Strategy "Artificial Intelligence" of the German Federal Government



The screenshot shows the EO-Lab website interface. At the top, there is a dark blue header with the EOlab logo on the left and navigation links [DE], LOGIN, ABOUT, NEWS, PORTFOLIO, PROJECTS, HELP, CONTACT on the right. The main content area is divided into two columns. The left column contains two sections: "Access to Data of National and European Missions Free of Charge" with a description and a button for "EO-Lab Data Portfolio", and "EO Browser: Easy Access to EO-Lab Data" with a description and a button for "EO Browser". The right column features a large blue-toned satellite image of a river valley with a caption "Radaraufnahme von Passau, Credit: DLR". Below this, there is a section titled "Services" with a description of AI services and a section titled "Performance and Flexibility for the Evaluation of EO-Data using AI Methods" with a description of AI tools. The bottom of the page shows a dark blue footer with a satellite and globe graphic.

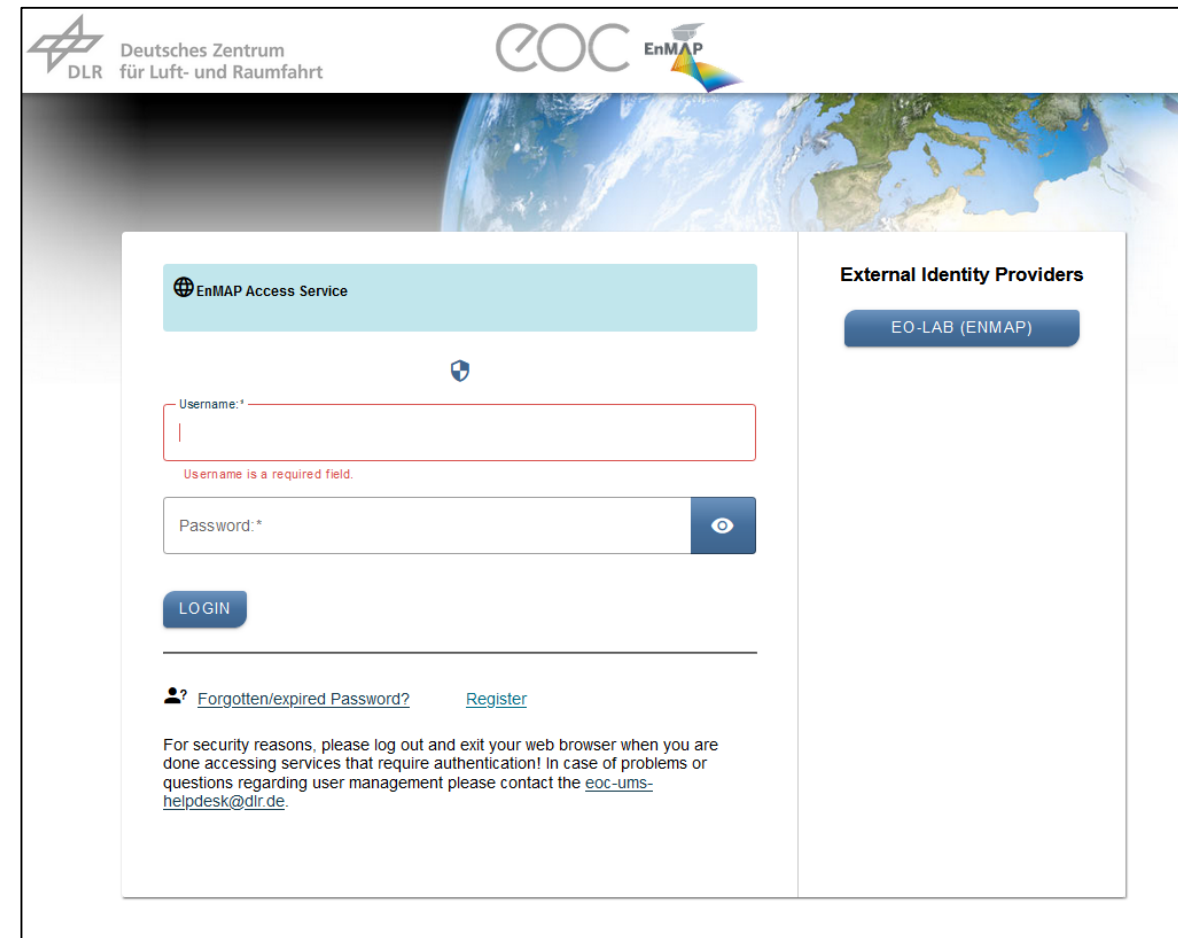
- The EO-Lab cloud is part of the Strategy "Artificial Intelligence" of the German Federal Government
- The EOC Geoservice hosts a wide range of free and restricted datasets



The screenshot shows the EOC Geoservice website interface. At the top, there is a navigation bar with links for 'About', 'News', 'Services', 'Datasets', 'Maps', 'Downloads', and 'Data Guides'. The main heading reads 'Welcome to the EOC Geoservice'. Below this, a paragraph states: 'The EOC Geoservice provides discovery, visualization, and direct download services for a selection of the geospatial datasets provided by the Earth Observation Center (EOC) of the German Aerospace Center (DLR). See the [About page](#) for details.' A row of five buttons is displayed: 'Browse Datasets', 'View Maps', 'Check Services', 'Contact us', and 'Read News'. The 'Latest Datasets' section features five dataset cards, each with a thumbnail image, title, and date:

Dataset Title	Date
EnMAP HSI - SpectralEarth - non-georeferenced - Global	2024-08-15
Forest Structure - Germany, 2017-2022	2024-01-10
Sentinel-5P TROPOMI L3 Daily Composites - Cloud Fraction (CF)	2023-12-11
Sentinel-5P TROPOMI L3 Daily Composites - Cloud	
Sentinel-5P TROPOMI L3 Daily Composites - Cloud	

- The EO-Lab cloud is part of the Strategy "Artificial Intelligence" of the German Federal Government
- The EOC Geoservice hosts a wide range of free and restricted datasets
- The EOC UMS acts as Service Provider to the EO-Lab Identity Provider for a set of protected datasets



Deutsches Zentrum für Luft- und Raumfahrt

EOC EnMAP

EnMAP Access Service

Username: *

Username is a required field.

Password: *

LOGIN

External Identity Providers

EO-LAB (ENMAP)

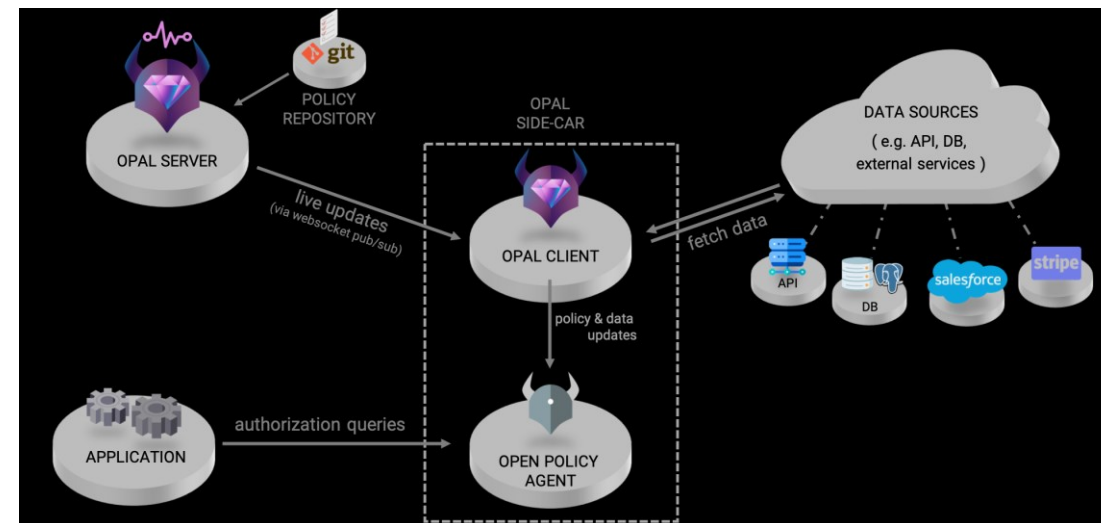
Forgotten/expired Password? Register

For security reasons, please log out and exit your web browser when you are done accessing services that require authentication! In case of problems or questions regarding user management please contact the eoc-ums-helpdesk@dlr.de.

- The EO-Lab cloud is part of the Strategy "Artificial Intelligence" of the German Federal Government
- The EOC Geoservice hosts a wide range of free and restricted datasets
- The EOC UMS acts as „Service Provider“ to the EO-Lab Identity Provider for a set of protected datasets
- Specific legal restrictions for some datasets are taken care of by EOC UMS:
 - Export control regulations require sanction list checks
 - License requirements determine the set of mandatory attributes to be communicated
 - Long-term access documentation for datasets subject to the German Satellite Data Security Act (SatDSiG)
 - Concept of „shadow accounts“

Identity Federations AT DLR EOC: ESA project EOEPKA+

- ESA project „EO Exploitation Platform Common Architecture – plus“ (EOEPKA+)
 - Design and Deployment of an IAM building block for federated applications/platforms together with partner Werum Software & Systems AG
 - Authorization services based on OpenPolicyAgent (OPA) and Open Policy Administration Layer (OPAL)
 - OPA: open source, general-purpose policy engine providing a high-level declarative language “Rego” (policy as code)
 - OPAL allows for real-time management of policies
- Test and demonstrator activities related to federated discovery / federated access



Identity Federations AT DLR EOC: terrabyte



- terrabyte: an innovative High Performance Data Analytics (HPDA) platform
 - operated by the DLR and the Leibniz Supercomputing Center (LRZ), an institution of the Bavarian Academy of Sciences and Humanities
 - LRZ and DLR participate in the national German Research Identity Federation DFN-AAI
 - used for identity mapping (map DLR account to required LRZ account)

A screenshot of the terrabyte login page. It features the terrabyte logo at the top, followed by the text "Sign in with your LRZ account obtained from [terrabyte-register](#)". Below this are input fields for "Username" and "Password", a blue "Sign In" button, and a link for "Reset your password". At the bottom, there are links for "About us", "Privacy policy", and "Servicedesk".A screenshot of the DFN-AAI-eduGAIN organization selection page. It features the DFN-AAI-eduGAIN logo and the DFN logo at the top. The main heading is "Select your organisation". Below this is a text box with the instruction: "In order to access the service [register.terrabyte.lrz.de](#) please select or search the organisation you are affiliated with." There is a dropdown menu with "DLR - Deutsches Zentrum fuer Luft- und Raumfahrt e.V." selected and a "Select" button. Below the dropdown are two checkboxes: "Remember selection for this web browser session." and "Remember selection permanently and bypass this step from now on." At the bottom, there are links for "DFN-AAI", "Imprint", and "Data Privacy".

Identity Federations AT DLR EOC: Current Topics and Outlook



- Privacy-related Topics
 - Cross-legislational transfer of personal data
 - Minimize personal data footprint
- Standards, Best Practices
 - AARC Blueprint Architecture
 - Security Standards (NIST etc.)
 - Protocols: moving from SAML/CAS protocol to OAuth2, OIDC
 - Standards and Policies of National Federations and eduGAIN
- Adaptive Authentication
 - Risk-based authentication
 - Passwordless authentication (passkeys)
- Authentication Services, Policy Management
 - From ABAC/RBAC towards Policy Based Access Control, incl. geo-aware Policies
 - Policy Lifecycle Management



Thank you!

Questions?

Ulrich Raape
German Aerospace Center DLR
Earth Observation Center EOC
ulrich.raape@dlr.de