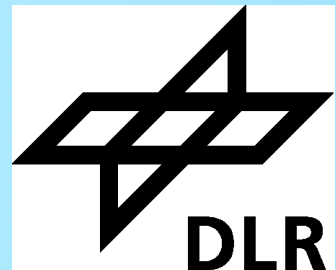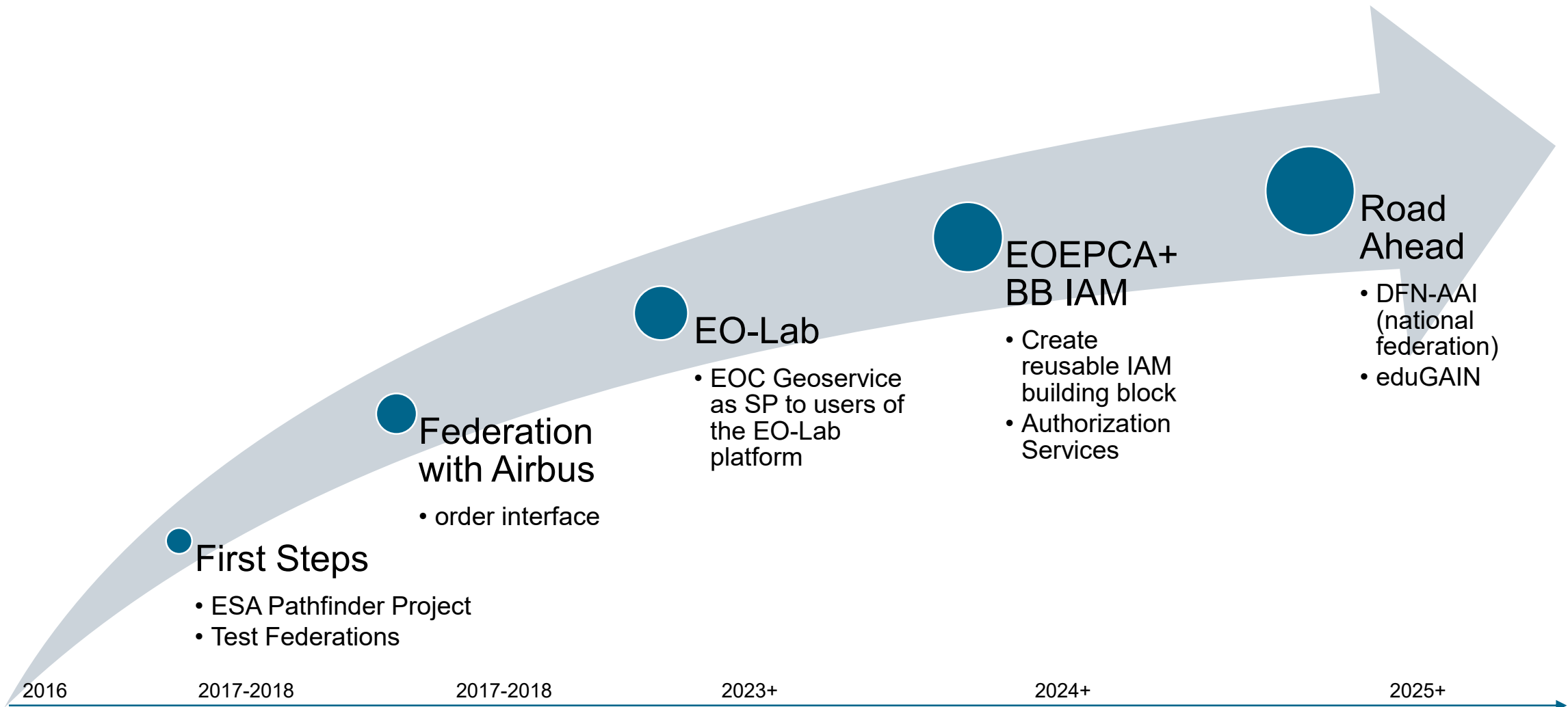# IDENTITY FEDERATIONS AT DLR EOC

Status and Outlook

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

DLR

Identity Federations AT DLR EOC

First Steps
- ESA Pathfinder Project
- Test Federations

Federation with Airbus
- order interface

EO-Lab
- EOC Geoservice as SP to users of the EO-Lab platform

EOEPCA+ BB IAM
- Create reusable IAM building block
- Authorization Services

Road Ahead
- DFN-AAI (national federation)
- eduGAIN

2016 2017-2018 2017-2018 2023+ 2024+ 2025+

Identity Federations AT DLR EOC:
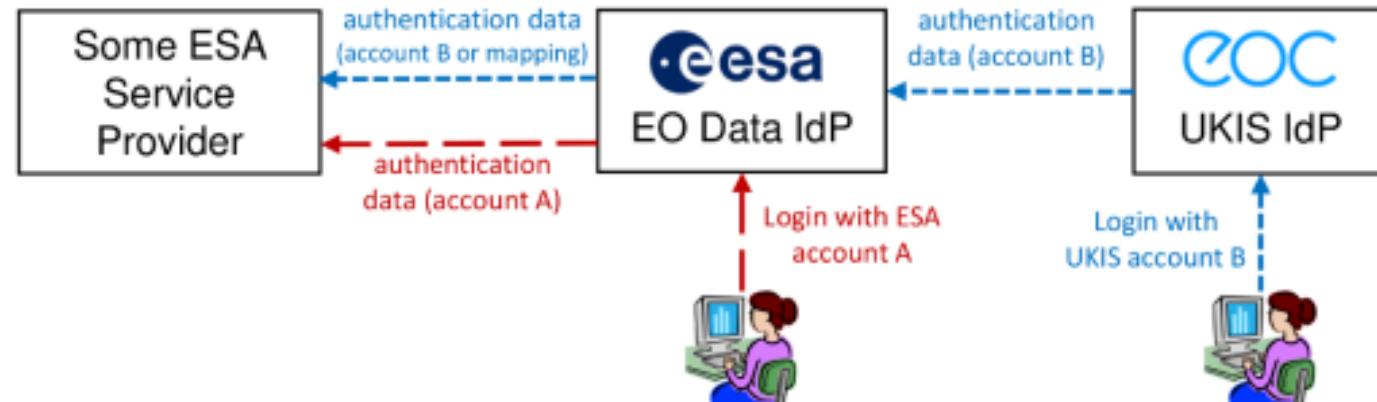# The EOC IAM solution

- 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)
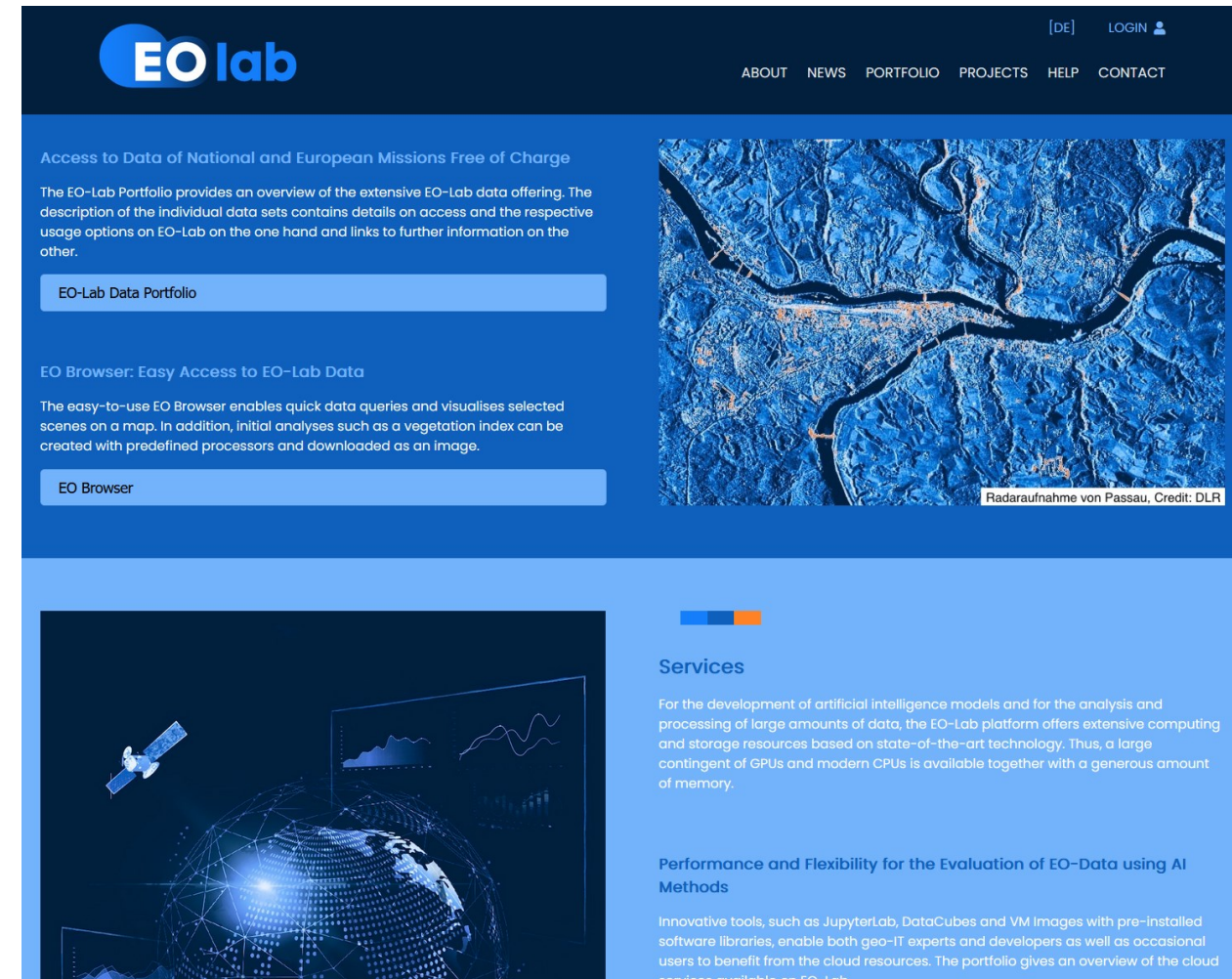   - Next level: Identity Federations

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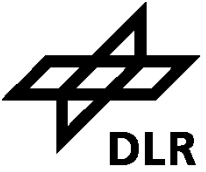
- 2017-2018: ESA Pathfinder Project „Identity Federation – Deutschland" (IFed-D)
  - Identity Federation Demonstrator
  - Change Detection Service as SP on DLR side
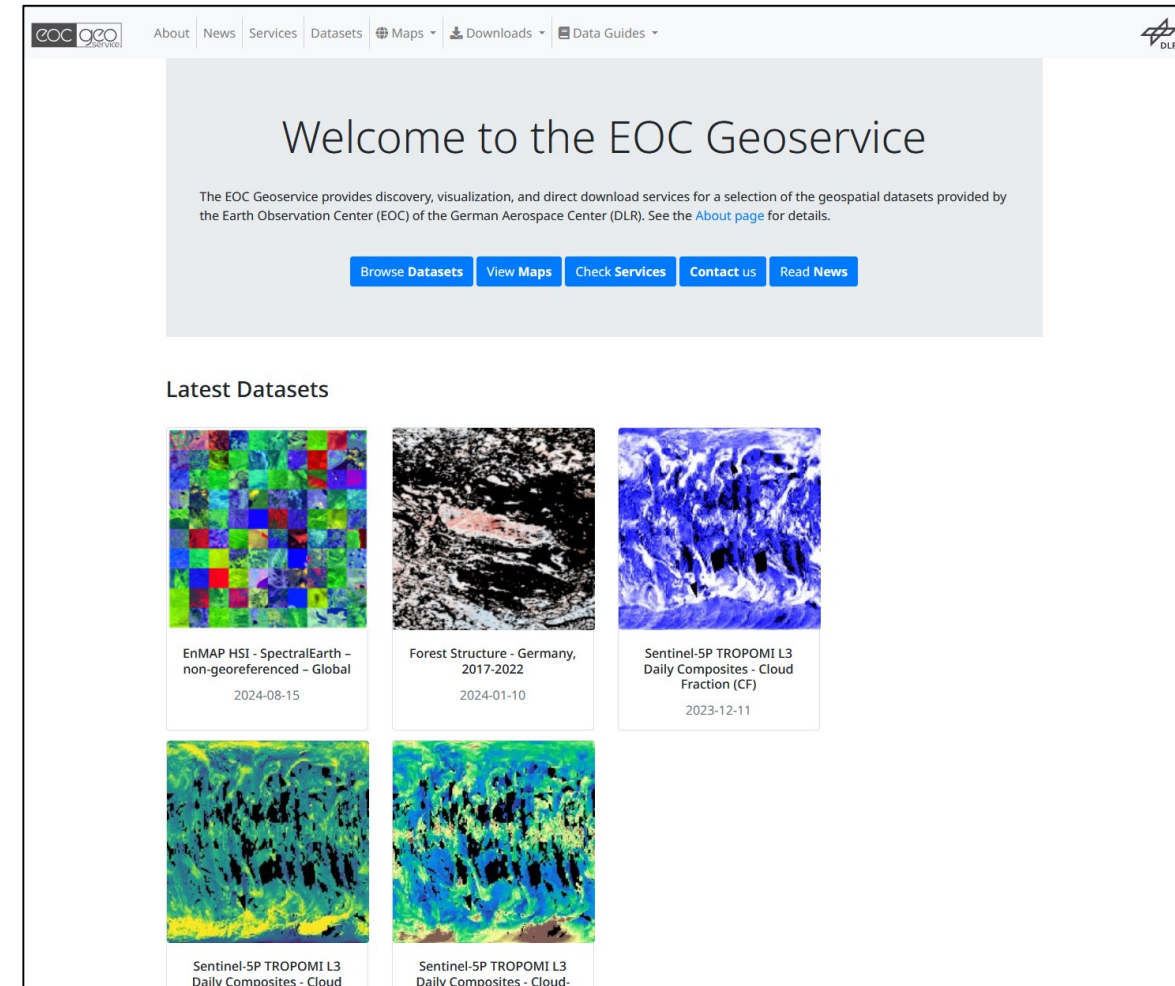 - Analysis of Privacy Implications

Identity Federations AT DLR EOC: EOlab

- The EO-Lab cloud is part of the Strategy "Artificial Intelligence" of the German Federal Government
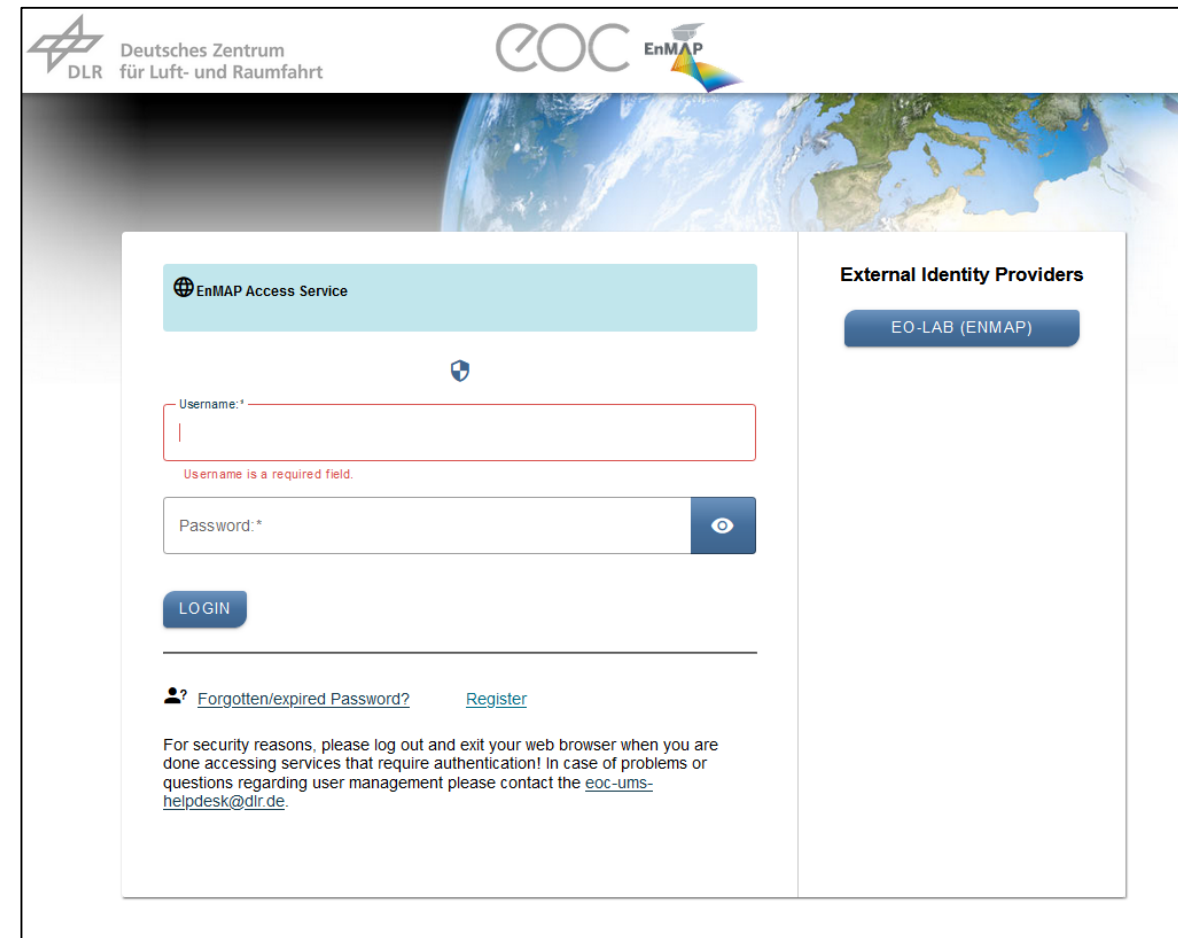
Identity Federations AT DLR EOC: EOlab

- 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

Identity Federations AT DLR EOC: EOlab

- 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

Identity Federations AT DLR EOC: EOlab

- 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 EOEPCA+

- ESA project „EO Exploitation Platform Common Architecture – plus" (EOEPCA+)
    - 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
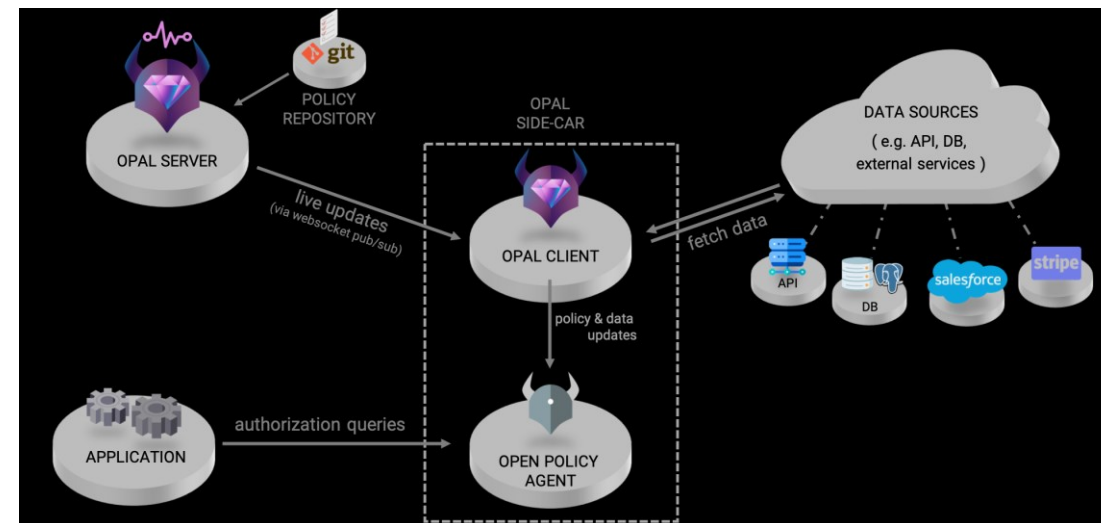
Identity Federations AT DLR EOC: terrabyte

- 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)

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