

DARIAH Update

11th FIM4R Workshop, Montreal Sept. 19, 2017

Peter Gietz, DAASI International



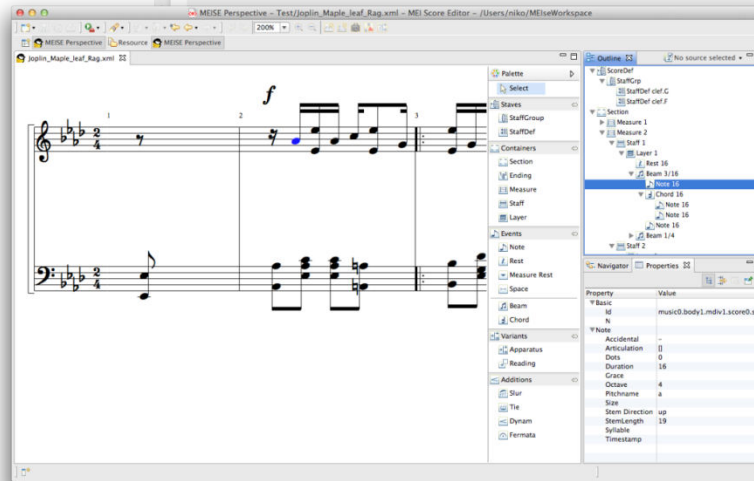
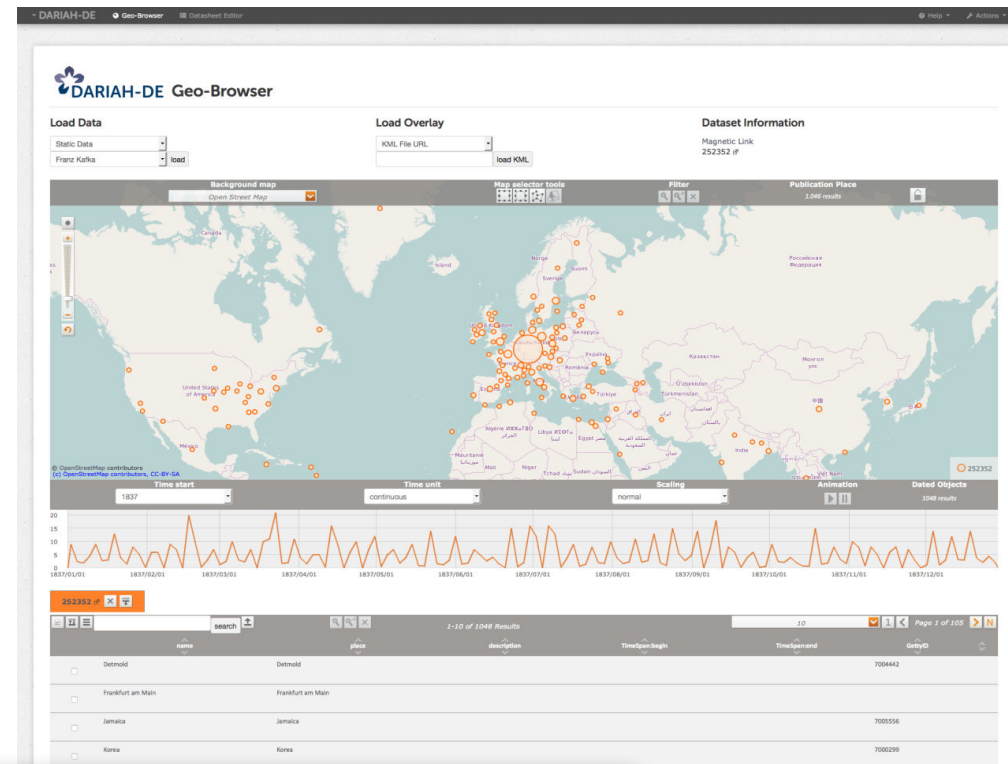
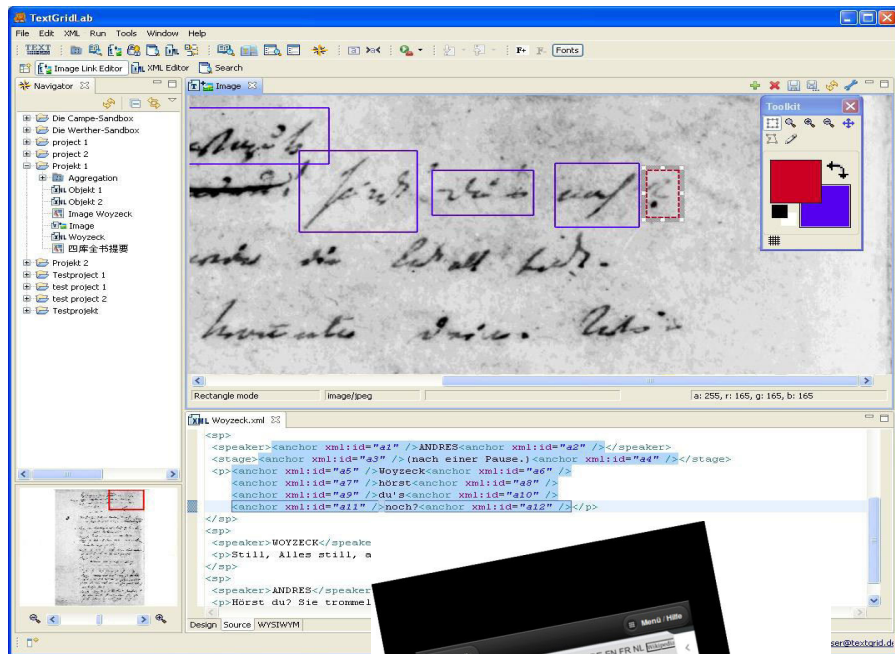
Agenda

- Fast reshow my slides from last time
- Report on new development: OAuth2 and PDP

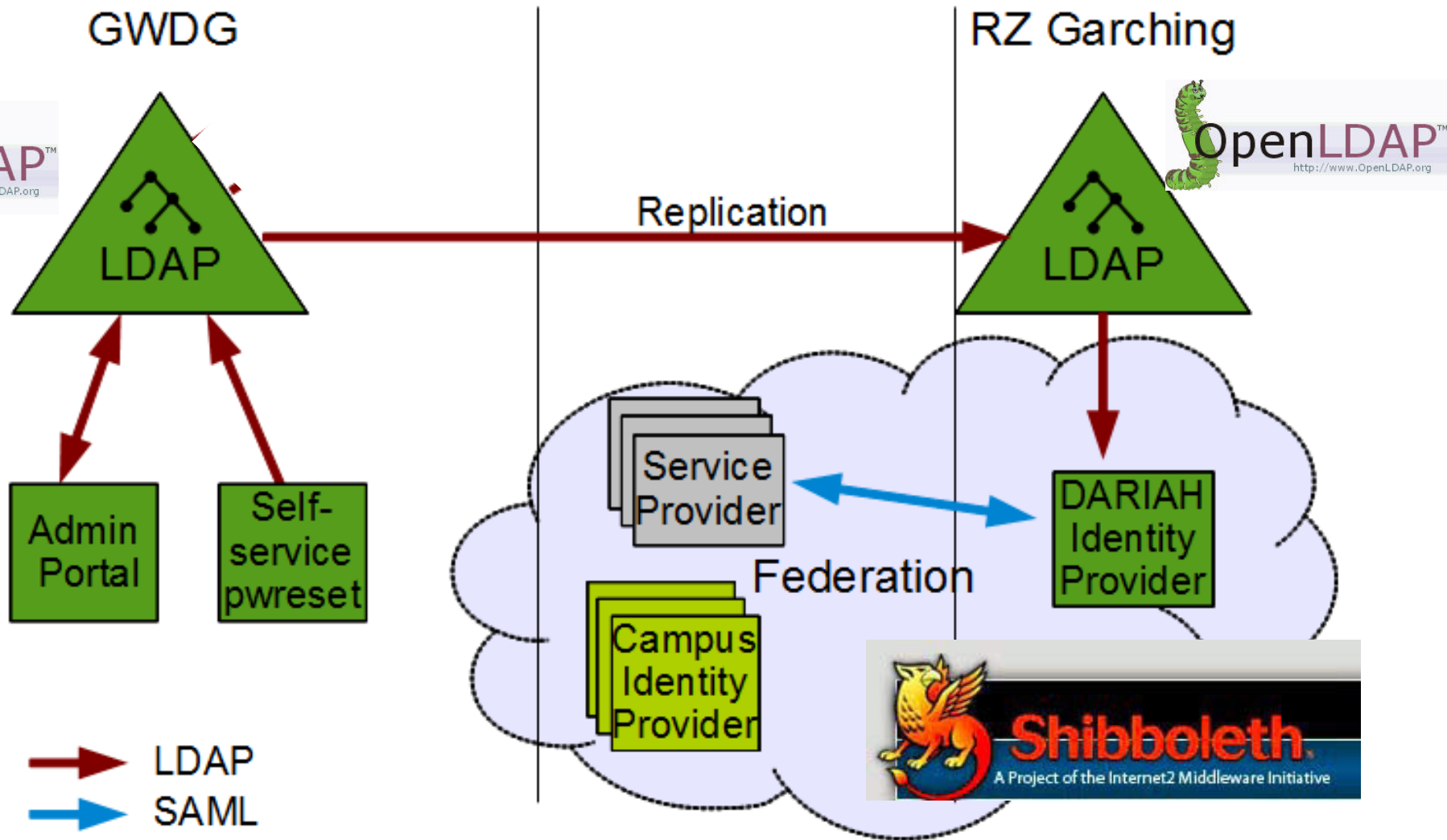
What is DARIAH

- DARIAH: Digital Research Infrastructure for the Arts and Humanities
- DARIAH is a pan-european infrastructure for arts and humanities scholars working with computational methods. It supports digital research as well as the teaching of digital research methods.
- One of the few ESFRI research infrastructures for the humanities (ERIC is in working since 2014)
- DARIAH's mission is to develop, maintain and operate an infrastructure in support of ICT-based research practices
Infrastructure is administration, software and storage services but also Curricula and Methodology
- Working with communities of practice: humanities scholars supporting their VREs

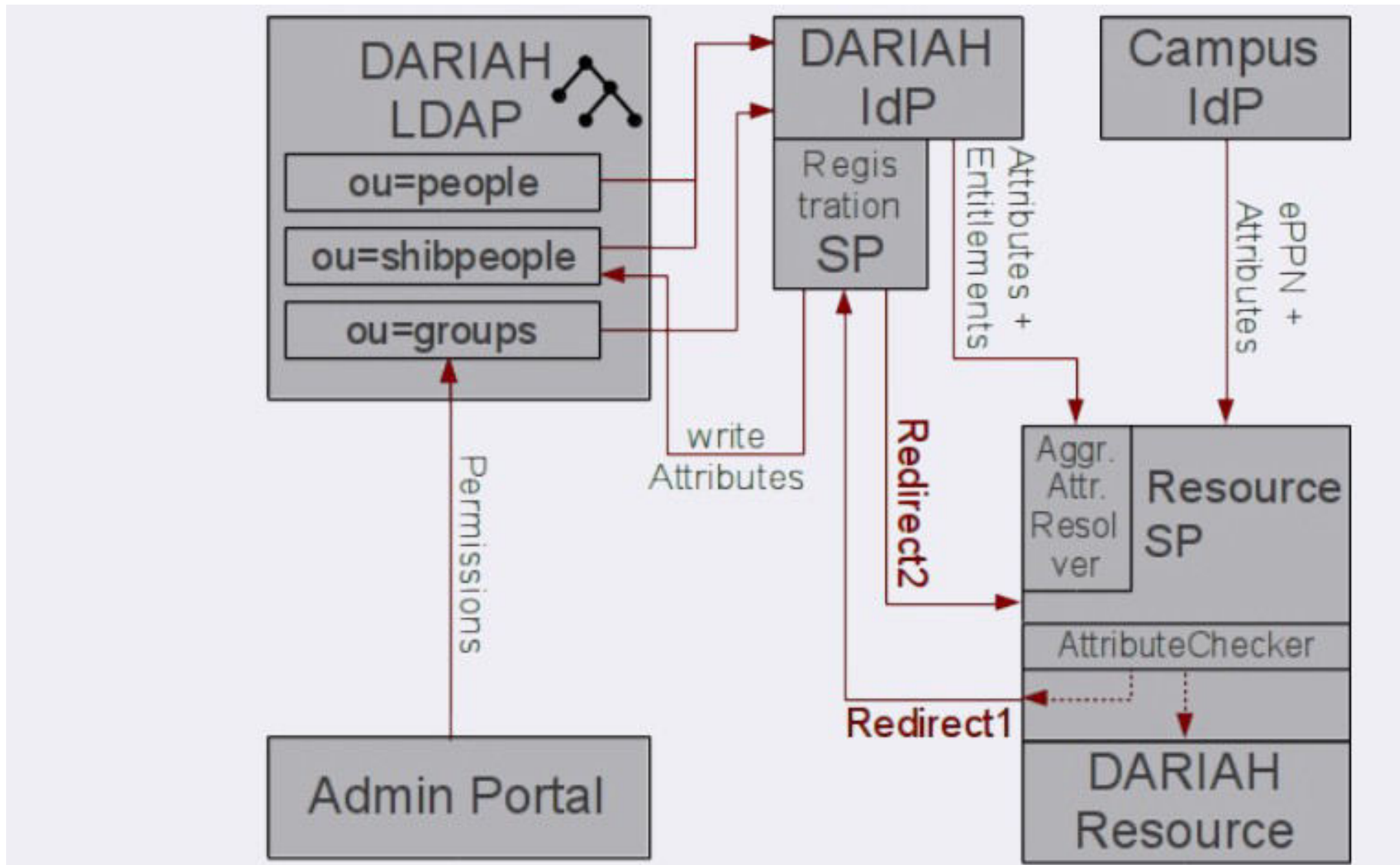
Virtual Research Environments in the humanities



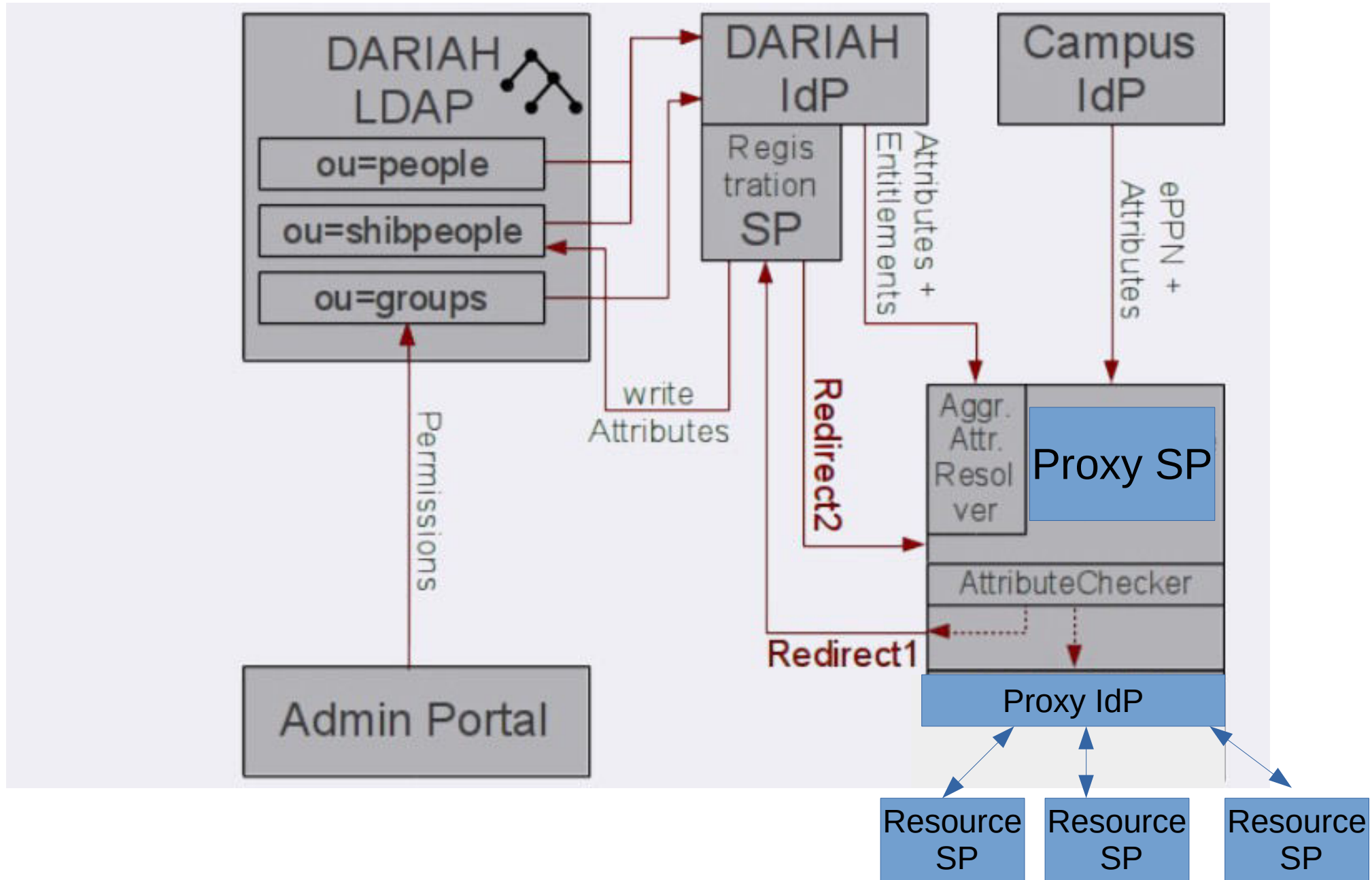
DARIAH AAI



DARIAH AAI



DARIAH AAI NG



DARIAH AAI ng

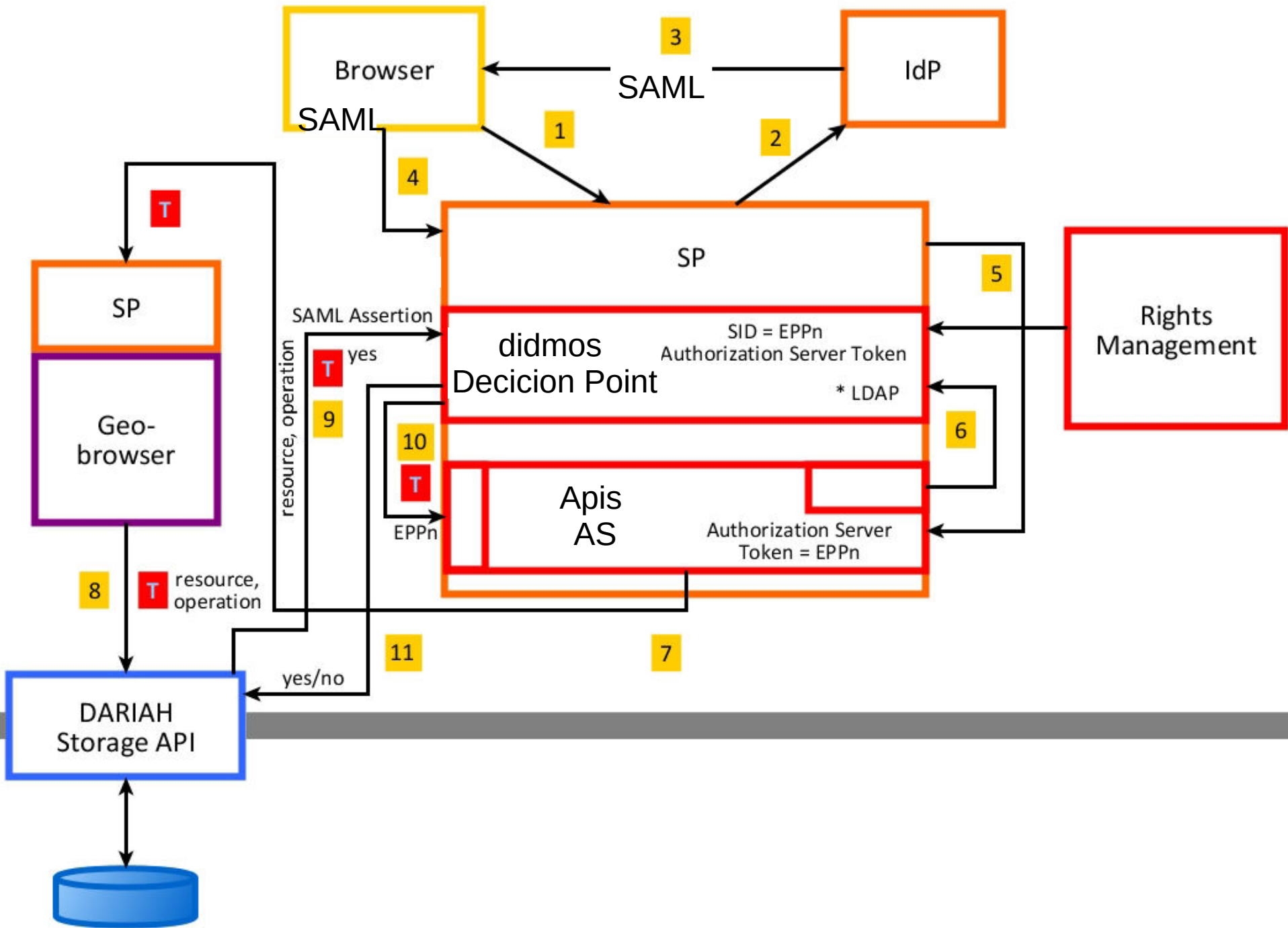
- The proxy model is compliant with the AARC JRA1 Blueprint Architecture
- It is implemented by now and will be production ready soon
- Already now a lot of DARIAH services implement the more complicated non-proxied SP
- Now that we are making much easier, we expect even faster uptake
- Now it will also be easier to support things like sirtfi and to integrate with other infrastructures, as EGI

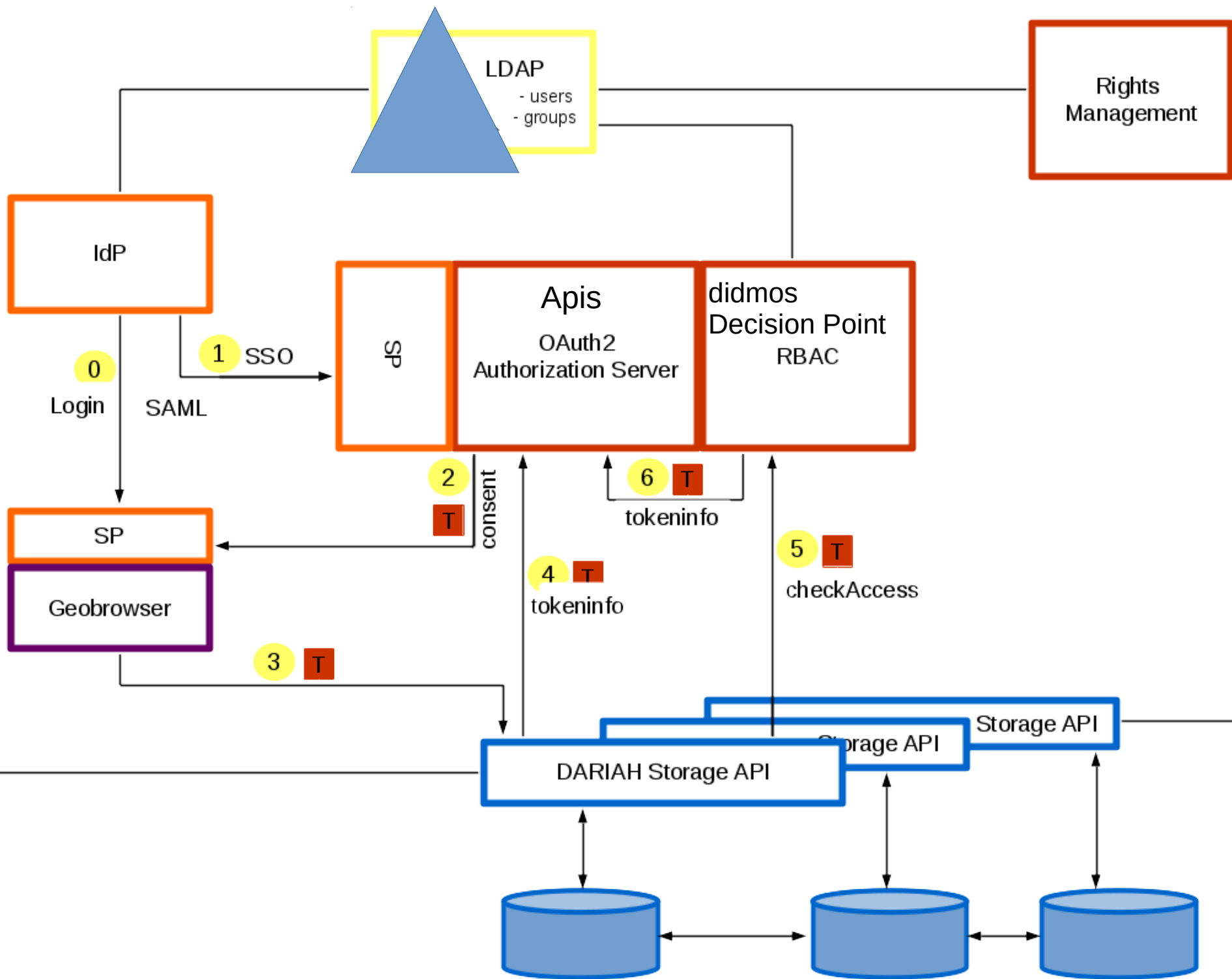
Current figures

- We currently have > 4080 DARIAH Users (still growing, almost 400 more than last February)
- We currently have 300 different user groups (20 more)
- Every project usually uses three or four privilege groups, thus ca. 85 projects (5 more)
 - X-users, X-contributors, [X-developoppers], X-admins

Central Policy Decision Point

- If more than one system trusts an access policy it makes sense to have a central policy decision point
 - Manage the access rules only once
 - Policy Enforcement Point
 - doesn't have to deal with managing and evaluating access policy
 - Just needs to get access decisions from the PDP via simple and standardized protocols
- DARIAH uses the RBAC compliant open-source PDP „didmos Decision Point“ in combination with apis OAuth2 Authorization Server





PDP flow

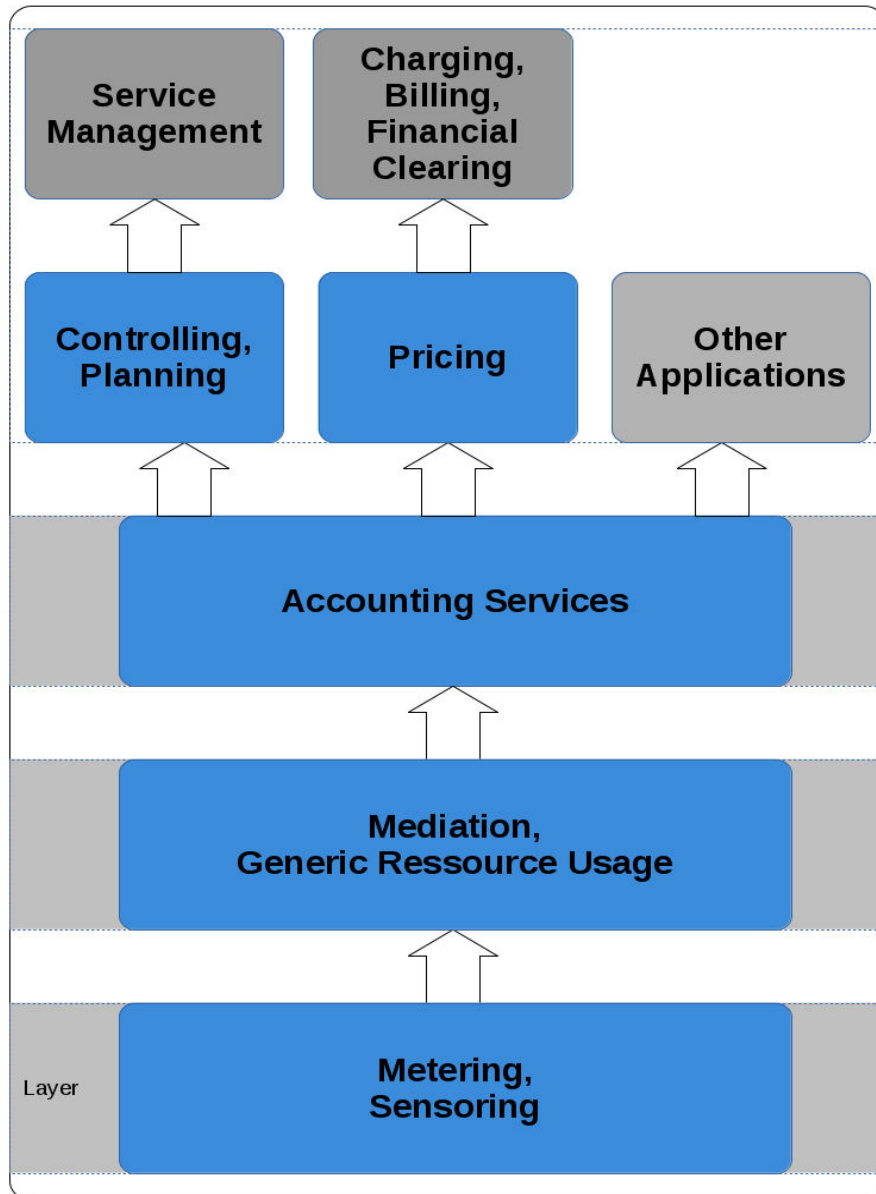
- 0: service has a session with the user
- 1: If service needs to access protected resources user gets redirected to the SP protecting the PDP
- 2: SP initiates normal SAML AuthN flow
- 3-4: SAML assertion gets to the PDP
- 5: OAuth2 token for user which is valid in Storage API
- 6: PDP creates a session connected with OAuth2 token and user ID (EPPN), and with the roles of that ID
- 7-9 OAuth2/SAML flow
- PDP checks token validity
- PDP sends policy decision to storage API

New work on Accounting

- Requirements for Accounting in DARIAH
- Concept for Accounting
- Integration into DARIAH AAI



New work on Accounting



Inspired by:
Joachim Götze, Tino Fleuren, Bernd Reuther, Paul Müller. A Model for Policy-based Automation of Usage Accounting across Multiple Cloud Infrastructures. 2013 39th Euromicro Conference on Software Engineering and Advanced Applications. s.l. : IEEE, 2013

Questions on Accounting

- How to integrate into PDP
 - Metered data need to be taken into account
 - e.g. if quota has exceeded, it influences the access decision
- How to integrate into user and group management
 - We already have the notion of users and their relation to projects
 - Accounting will rather be done project-wise than user-wise

Lessons

- Going into production early is a good thing
 - But maintaining the production service keeps you from implementing next versions
 - AARC has been very helpfull here for input on what to do next and for the possibility of piloting new technologies