Authentication and Authorisation for Research and Collaboration

Showcase of the DARIAH-EGI pilot

David Hübner, DAASI International / DARIAH
Ioannis Igoumenos, GRNET / EGI

FIM4R meeting, Vienna
2019/02/11

Introduction

- DARIAH AAI allows ~4-5k researchers in arts & humanities access to ~ 20 production services

- DARIAH AAI "V1" has been in production for around 5 years

- Authentication through eduGAIN or homeless IDP

- AARC pilot with two goals (DARIAH's PoV):

    - Make DARIAH AAI BPA-compliant

        - Add a SP/IDP proxy and migrate existing SPs

    - Pilot interoperability with EGI

        - VM dashboard integration with group memberships managed by DARIAH

- Work on EGI side mainly focussed on dynamic provisioning of DARIAH users in EGI

Introduction cont'd

- DARIAH SP/IDP proxy in production since mid 2018

- Successfully moved all existing DARIAH services to the proxy

- Held a workshop in January (in Tübingen) to assist new SP operators to connect to the proxy

- Interoperability with EGI is done as PoC (connected to Check-In development)

- Remaining tasks in AARC2

  - ❏ Connect to VM dashboard once EGI COManage plugins are available in production

  - ❏ Evaluate policy enhancements (AUP alignment to avoid double AUP acceptance)

Some more details

- Proxy SP is in eduGAIN

- Proxy IdP not

- Currently only SAML

- Central tasks at the proxy

  - Allow users to login through their home organisation

  - Query community attributes, groups, accepted AUP...

  - Check AUP and service-specific terms of use

- Tasks at account and group membership management

  - Registration of new accounts

  - Apply for group memberships
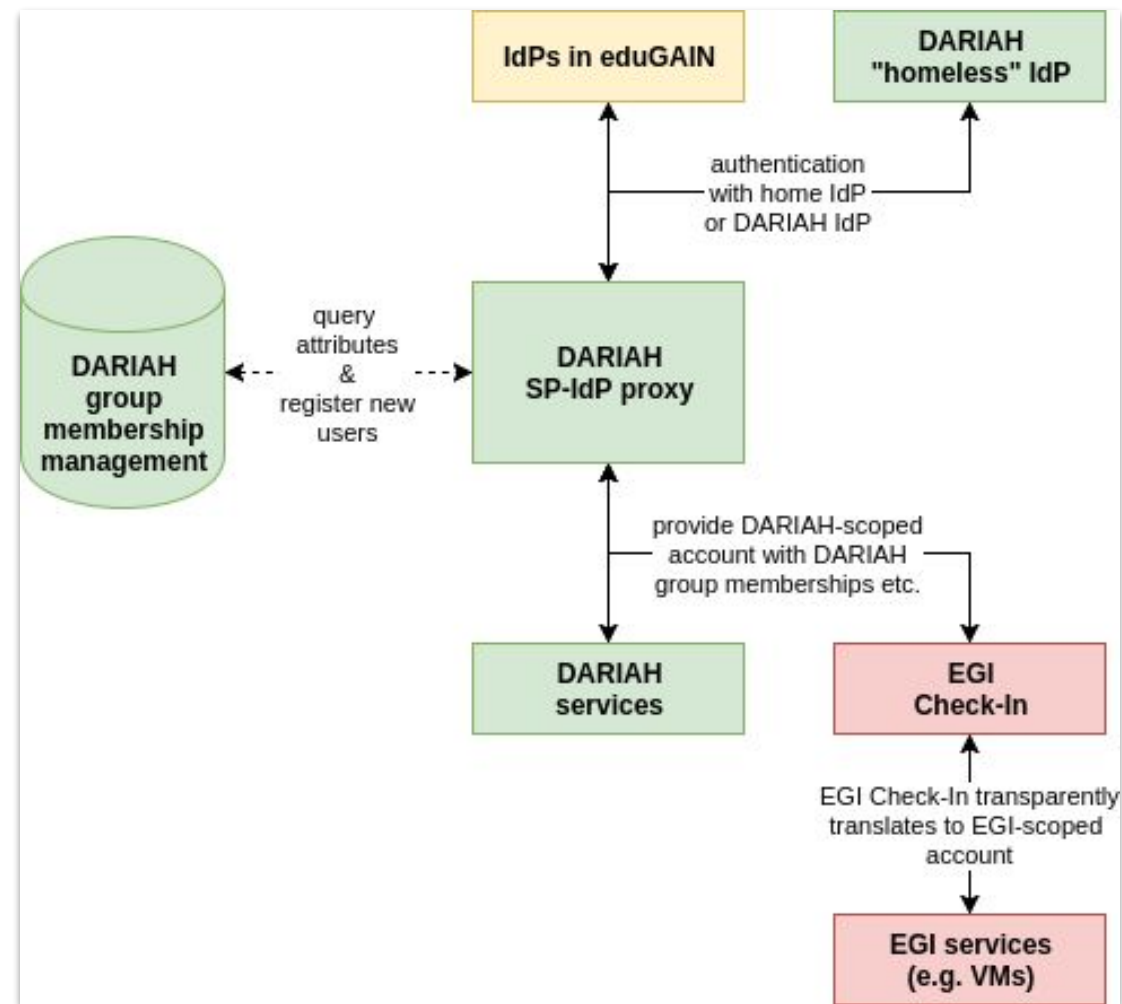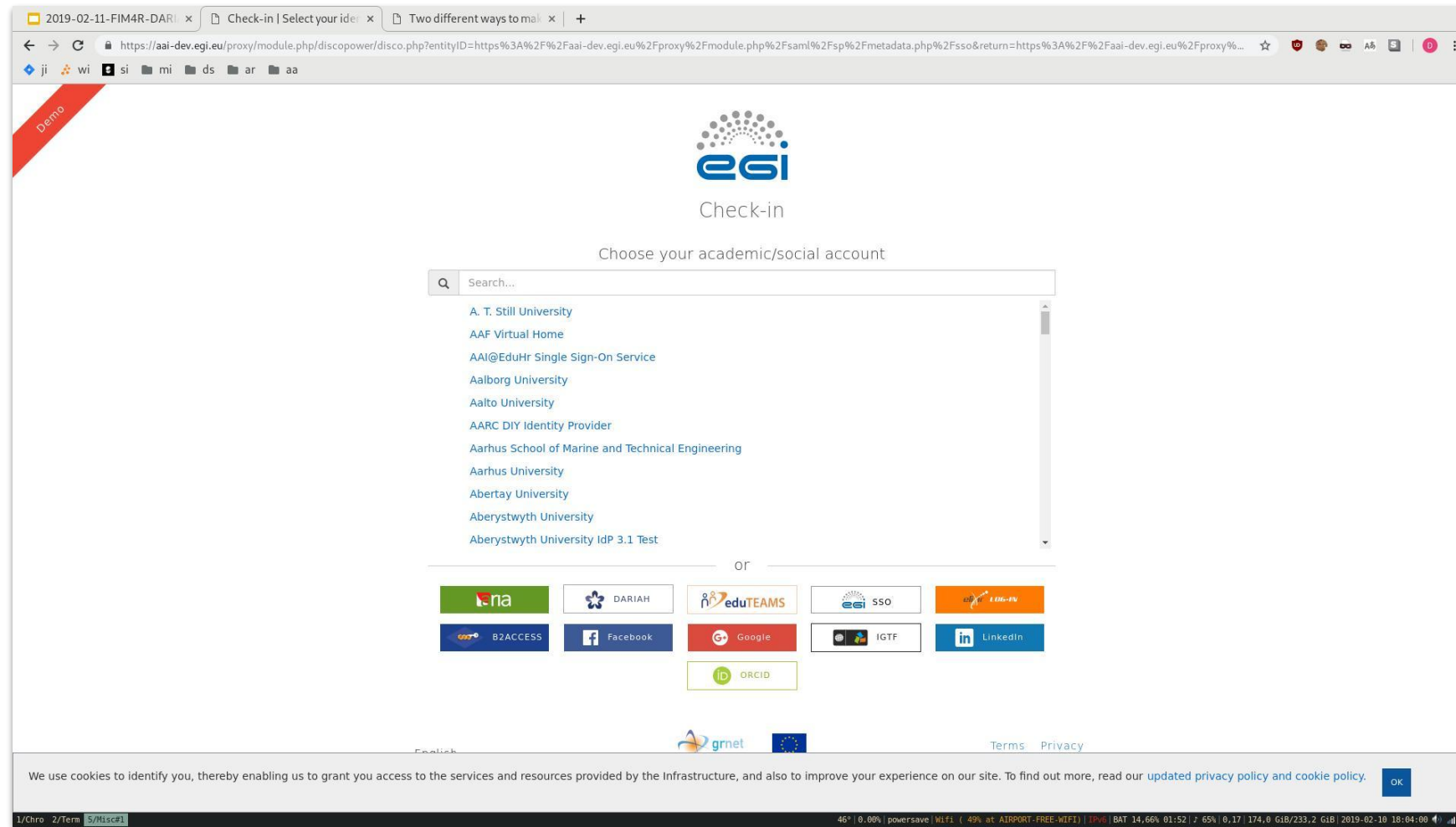
Short demo

Since there currently is no integration of VM dashboard, we'll use an exemplary SP in EGI:

https://aai-dev.egi.eu/registry/
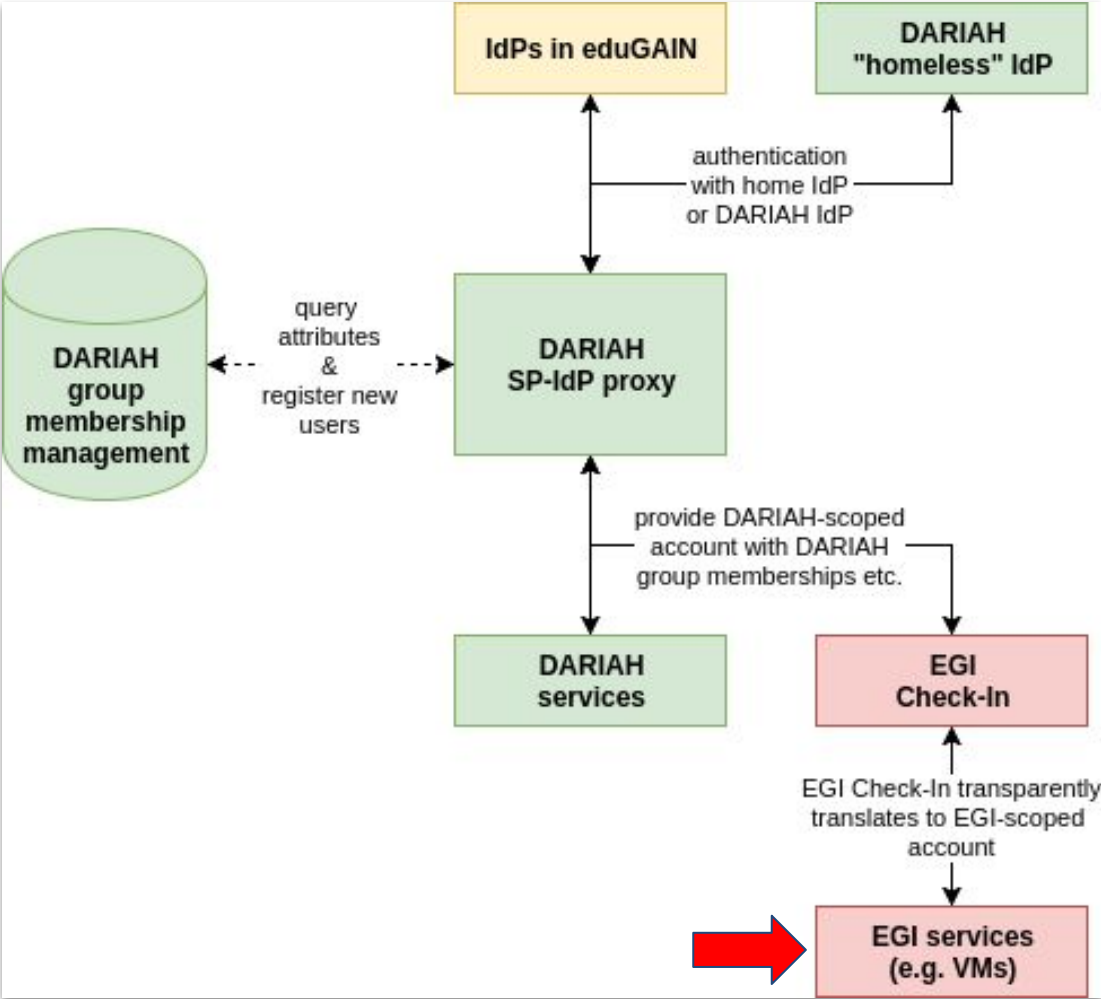
DARIAH community at EGI Check-In
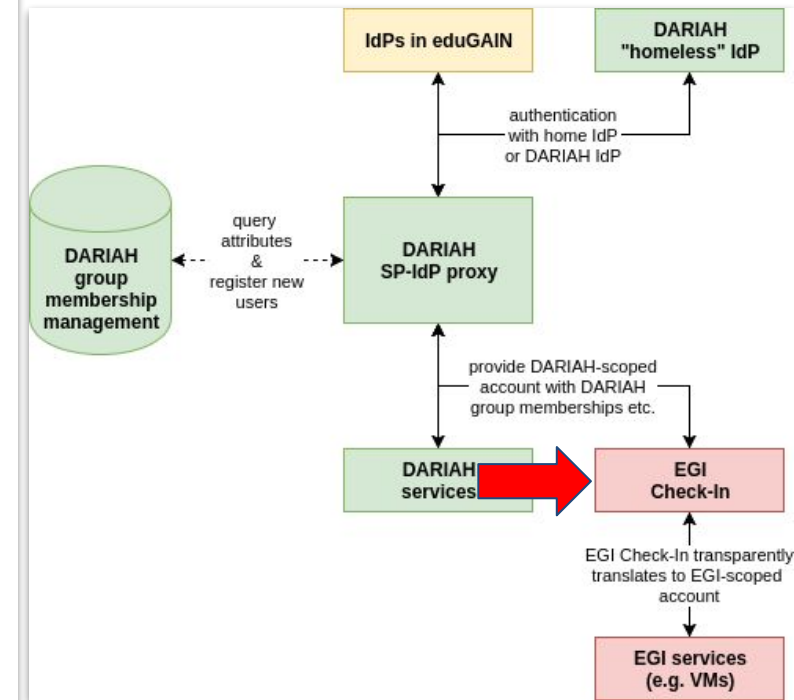
Discovery within DARIAH community
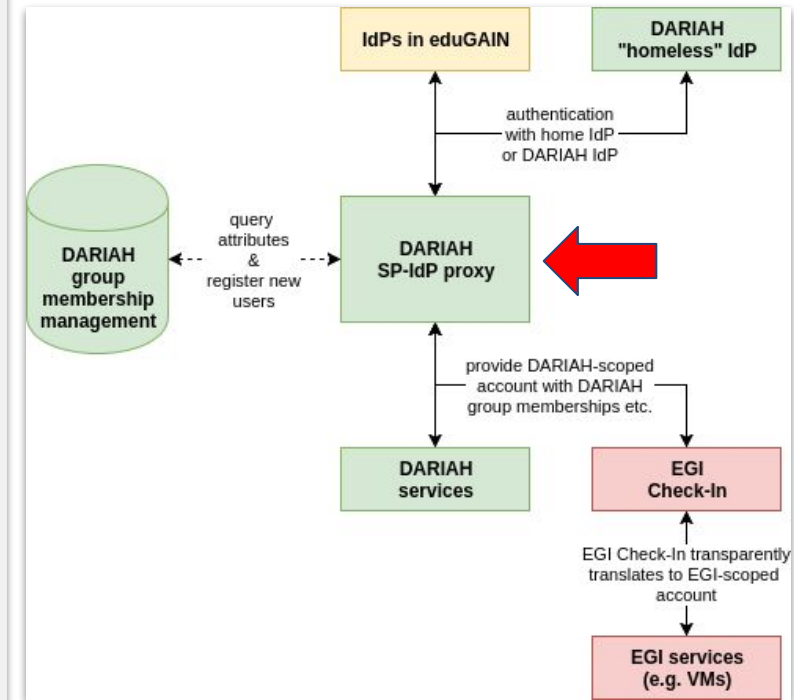
Login at DARIAH homeless IDP
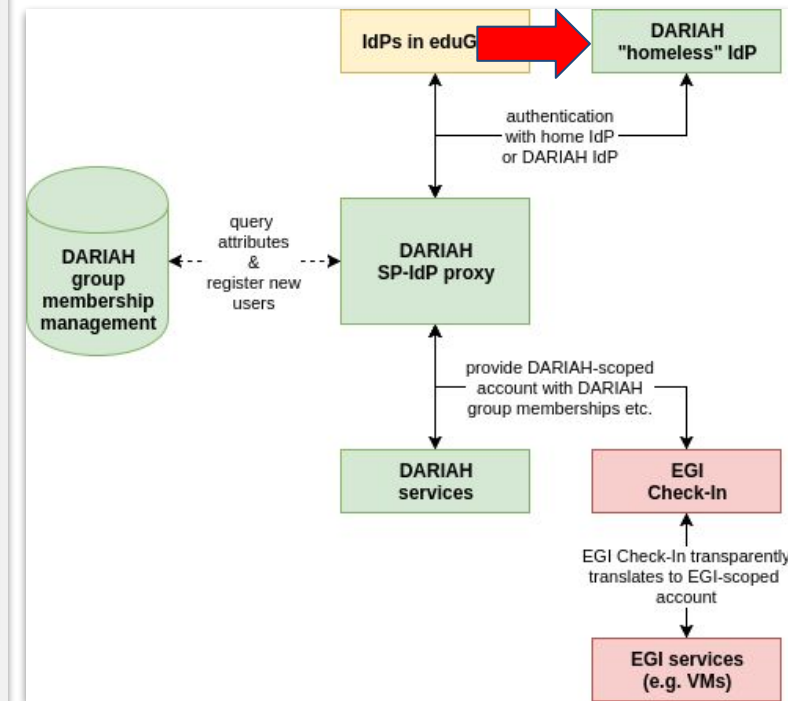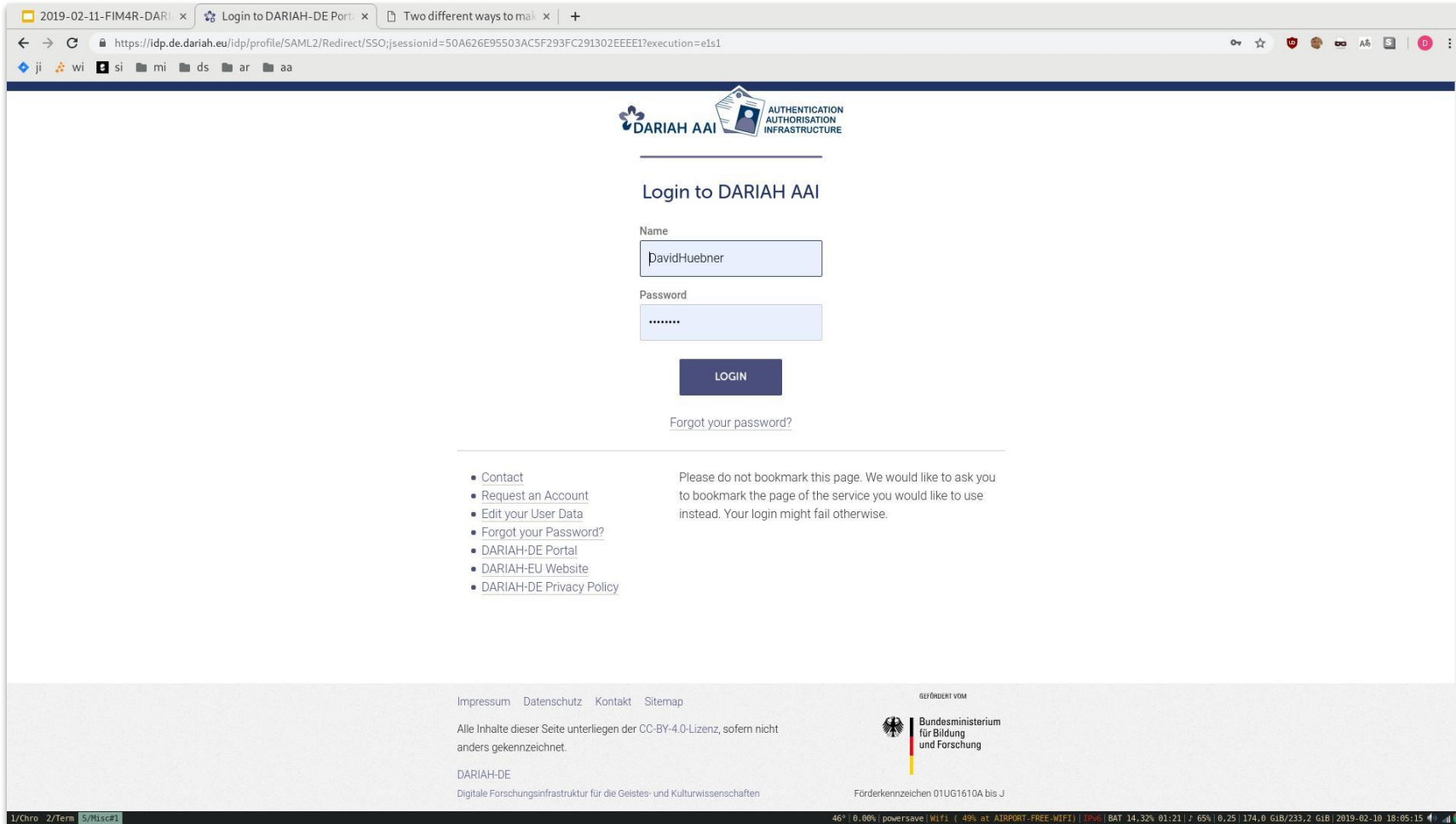
Attribute aggregation etc. at the proxy

urn:mace:egi.eu:group:fedcloud.egi.eu:role=member#aaiproxy.de.dariah.eu
urn:mace:egi.eu:group:fedcloud.egi.eu:role=vm_operator#aaiproxy.de.dariah.eu

RCauth plugin

Associate subject DN of certificate issued by RCauth to user profile

- RCauth DN linking plugin for Comanage
  - Implemented as COmanage Organisational Identity Source
  - Integrated as an OIDC client to the MasterPortal

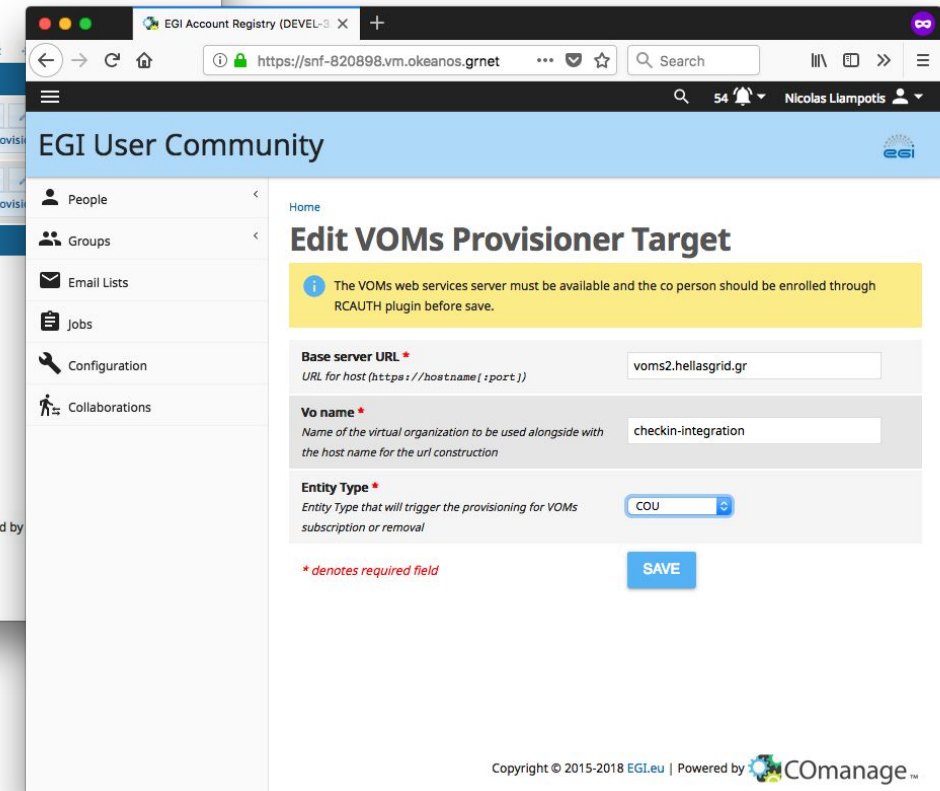# Filling in the missing pieces
RCauth plugin

1

2

3

4
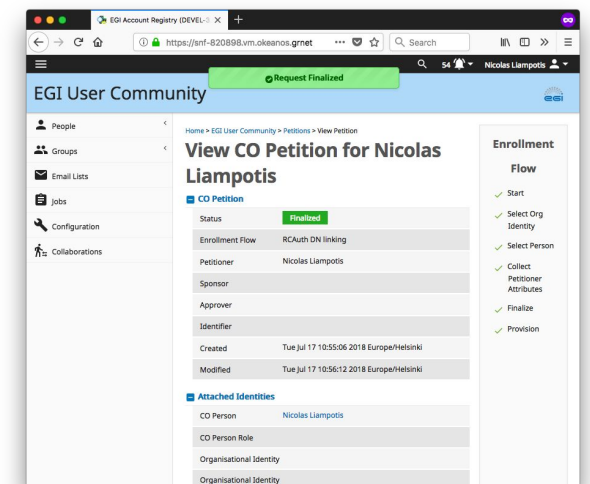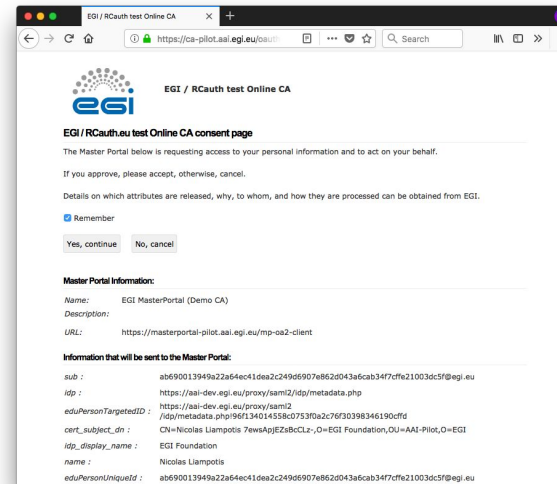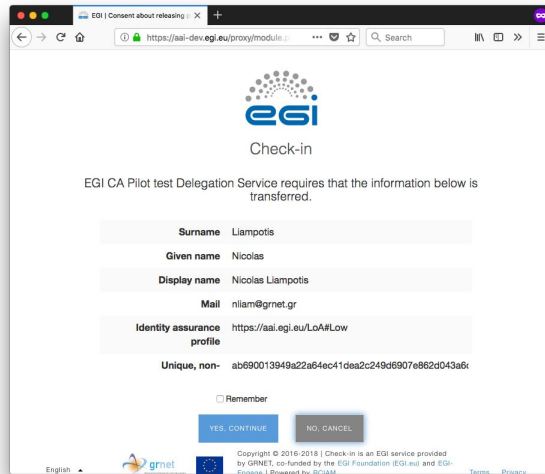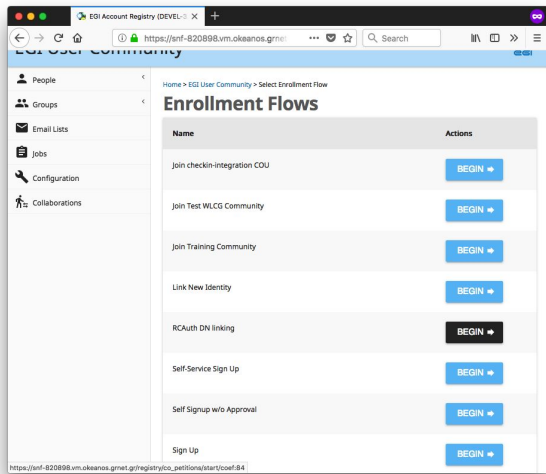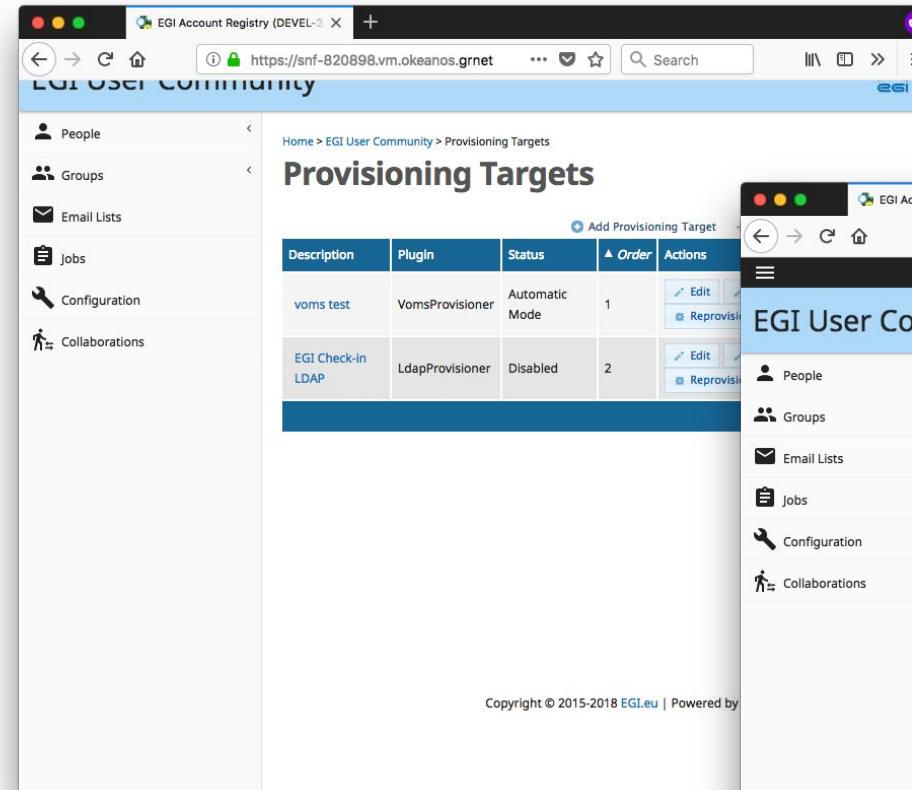
VOMS Provisioning: VOMS plugin

VOMS provisioning plugin for COmanage

- Implemented as COmanage Provisioning plugin
- Requires VOMS-admin access to VOMS servers
- Evaluates(if required) the registrattion periodically

User Profile

Thank you
Any Questions?

david.huebner@daasi.de

AARC

https://aarc-project.eu