eduTEAMS – euDAT pilot

A community is using eduTEAMS to manage groups and members. How can we leverage relevant information from eduTEAMS for authZ in EUDAT B2ACCESS and B2SAFE services?

Christos Kanellopoulos (GEANT), Willem Elbers (CLARIN), Shiraz Memon (FZK), Niels van Dijk (SURFnet)

Requirements & assumptions

- Registration
  - Users are registered and managed on eduTeams using their home organisation accounts or any of the guest identity providers supported by the eduTeams Identity Hub
  - Users will register by authenticating via B2ACCESS, using a local B2ACCESS account or an external account managed by their home organisation or social identity provider.
- Authorization
  - Information about data projects (DataProjectID), related (distributed) services (ServiceID), service components (ServiceComponentID) and resources (ResourceID for accounting) are captured and managed via the DPMT1 and this information can be released to eduTeams by B2ACCESS (while it originates from the DPMT)
  - eduTeams allows project or customer principals to manage their user base by mapping them to the DataProjectIDs or the CustomerIDs.
  - Group information is aggregated by B2ACCESS and along with the information already available inreleased by B2ACCESS, it is made available to the EUDAT services
- Identifiers
  - EduTEAMS and B2Access will use a shared identifier from the IdP
  - B2ACCESS will release a persistent id (resource specific eudat identifier)
  - B2ACCESS will release the user identifier coming from the external identity provider

Phase 1

- Register identity on eduTEAMS MMS

- Register idnetity B2ACCESS

- Manage group and membership on eduTEAMS

- Exchange information from eduTeams to B2ACCESS

Flows
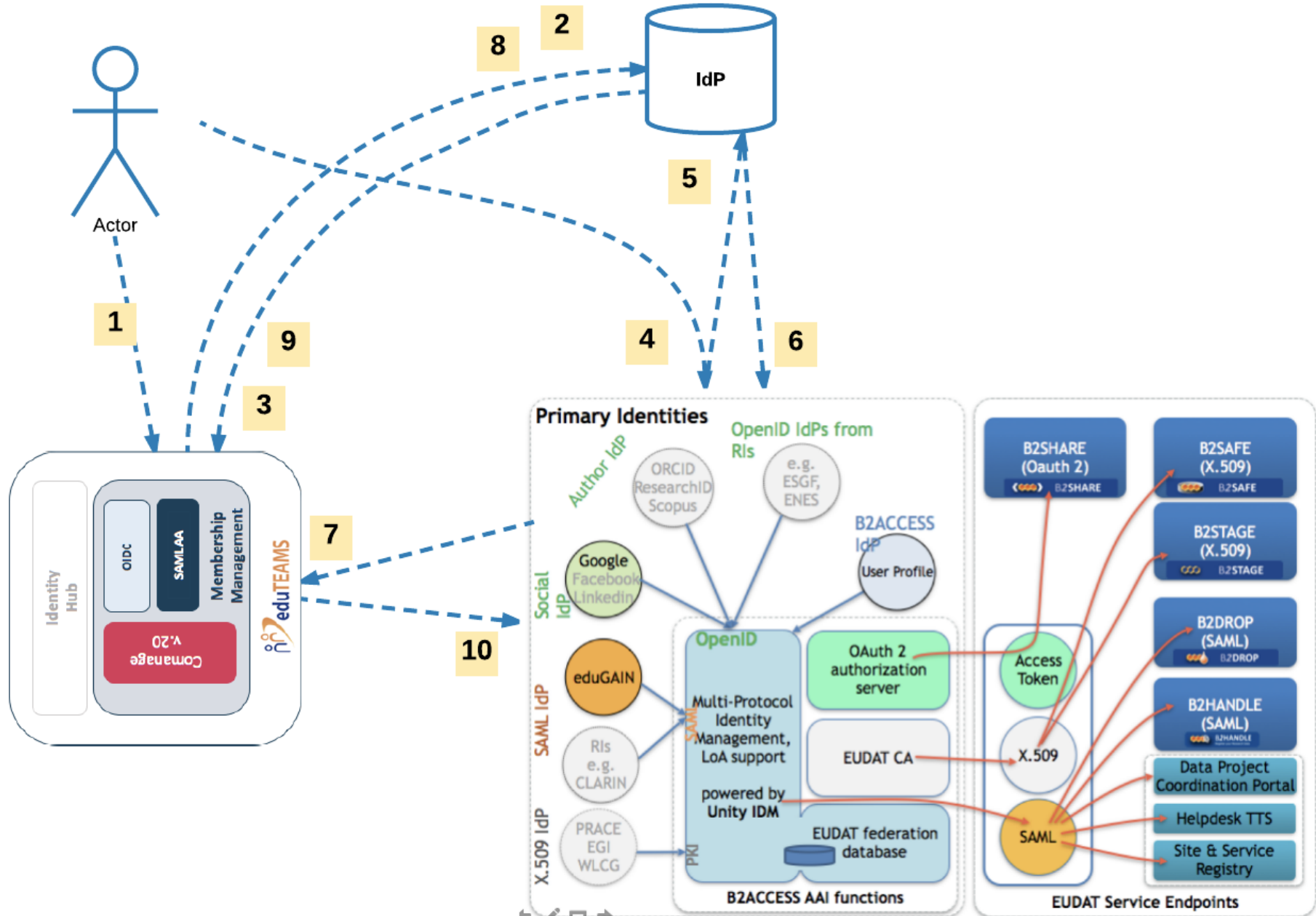
Results Phase 1

- CO set up in eduTEAMS and members registered

- Users registered in B2Access

- OIDC interface implemented and tested between eduTEAMS and B2Access, with basic flow of attributes confirmed

ToDo Phase 2

- Register more advanced AuthZ information in eduTEAMS

- Map this info in standerdized way in OIDC

- Storing and releasing the inbound eduTeams group membership attributes/information to the EUDAT's B2* services

- Validate proper AuthZ being issued based in eduTEAMS information in B2Access