EUDAT AAI

overview

Johannes Reetz, RZG
Claudio Cacciari, Cineca
Shiraz Memon, Juelich
Jens Jensen, STFC,
on behalf of EUDAT AAI Taskforce

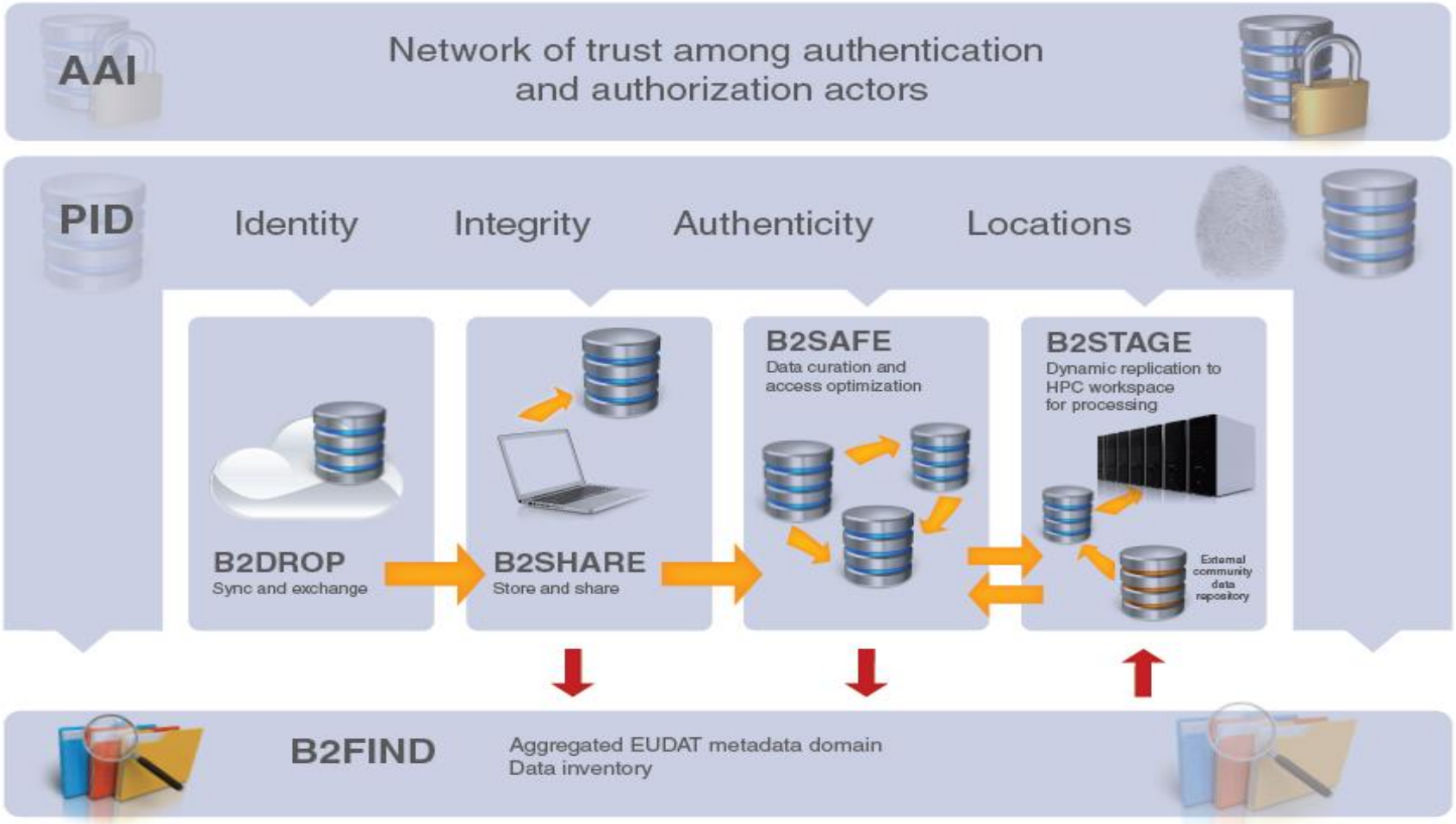
e-Infrastructure for Earth Sciences Workshop
Amsterdam, Jan 22/23, 2015

EUDAT

eudat.eu

B2ACCESS
Identity & Authorisation

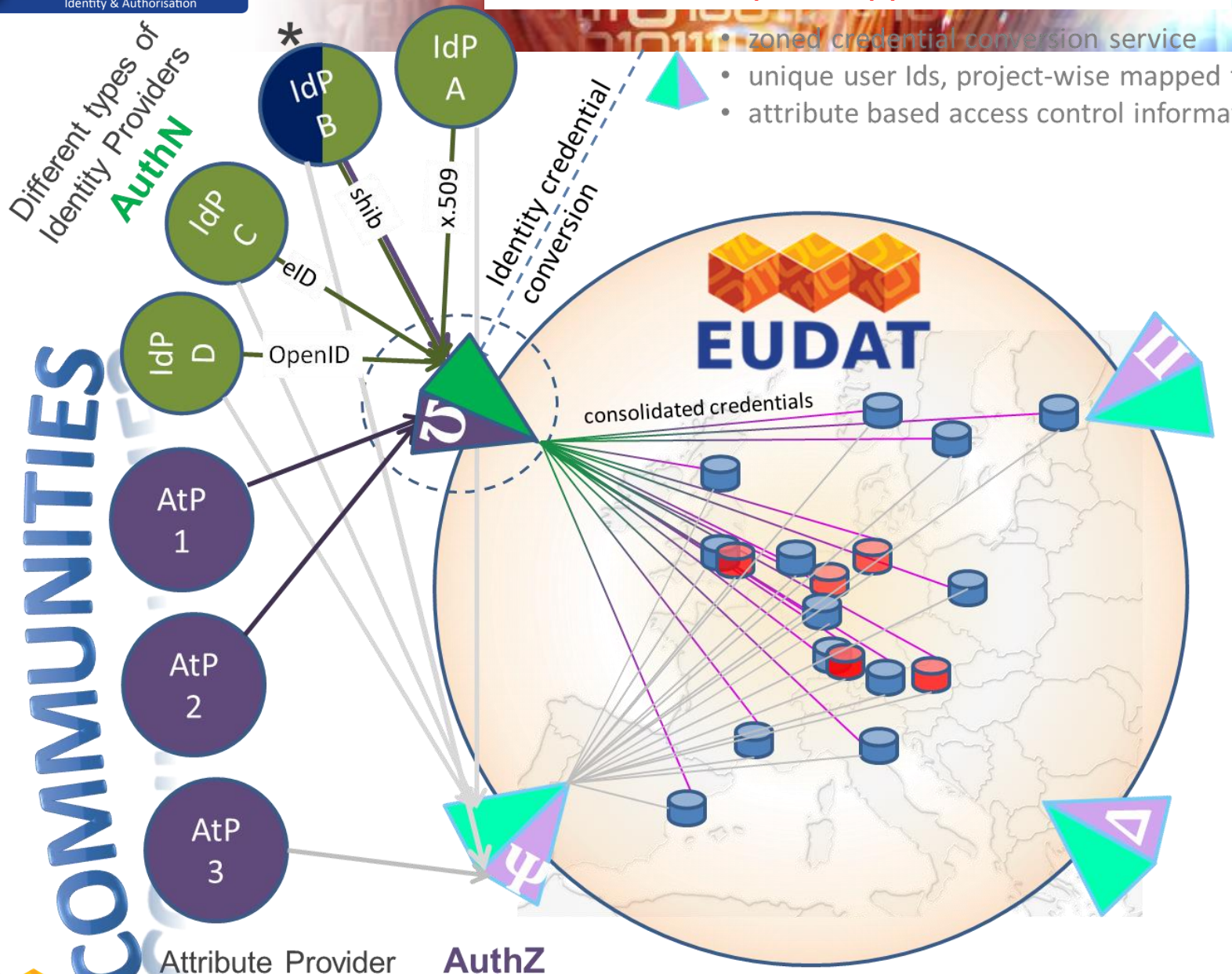
Provide access to EUDAT Services
by using existing Identity federations and protocols



EUDAT

General Conceptual Approach

- zoned credential conversion service
- unique user Ids, project-wise mapped to
- attribute based access control information



either community-managed or (*) attributes provided by user's home IdP are reused

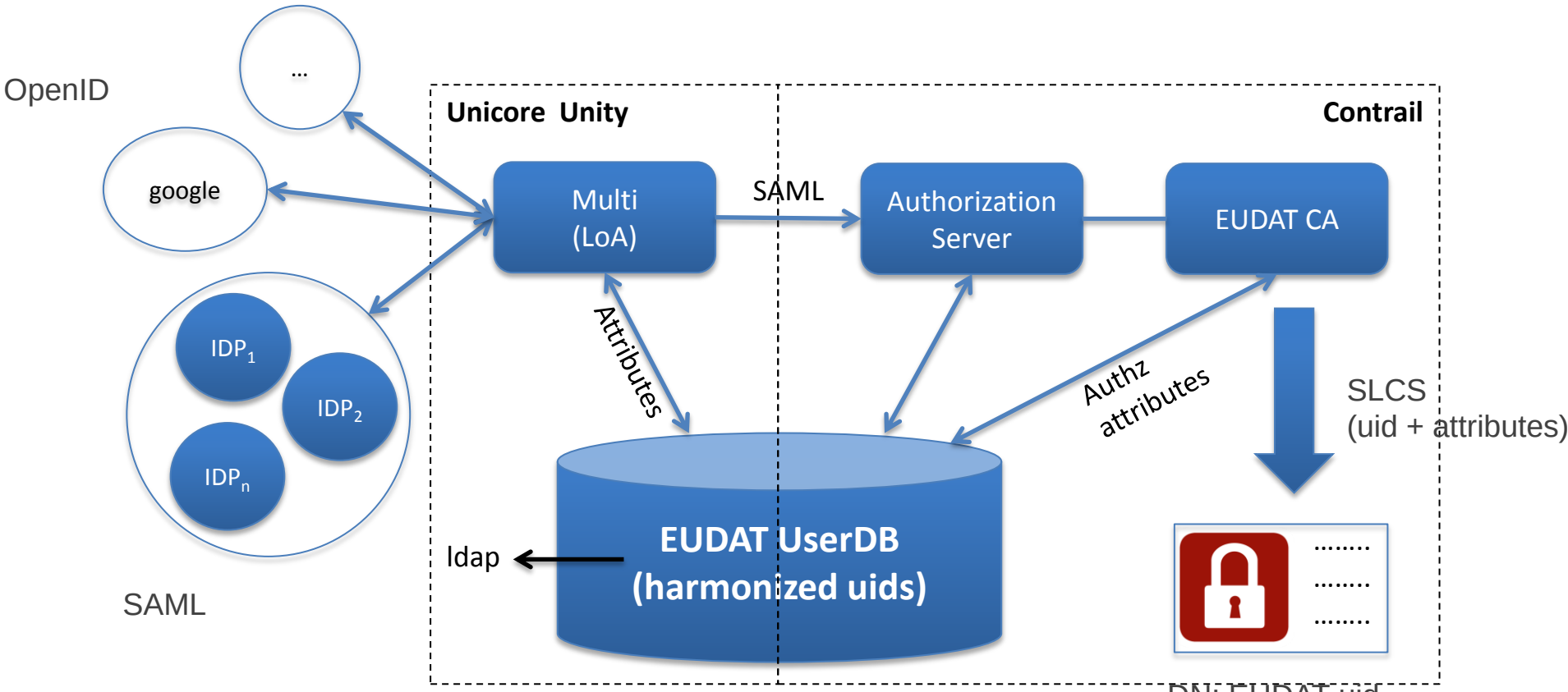
B2ACCESS
Identity & Authorisation

Federated AAI in two steps

- Authenticating *to* EUDAT
  - making use of **external** IdP federations **!**
  - EUDAT's run an own IdP (e.g. for user who are not affiliated to an institutional IdP)
  - Multi-protocol: SAML, OpenID Connect, X.509
- Authenticating *in* EUDAT
  - creating internal short-lived X.509 credential with AuZ
    - drives a range of protocols (Web and non-Web)
    - hidden from users (option to download)
  - mainly OAuth2 for delegation, not necessarily GSI

EUDAT

EUDAT AAI approach

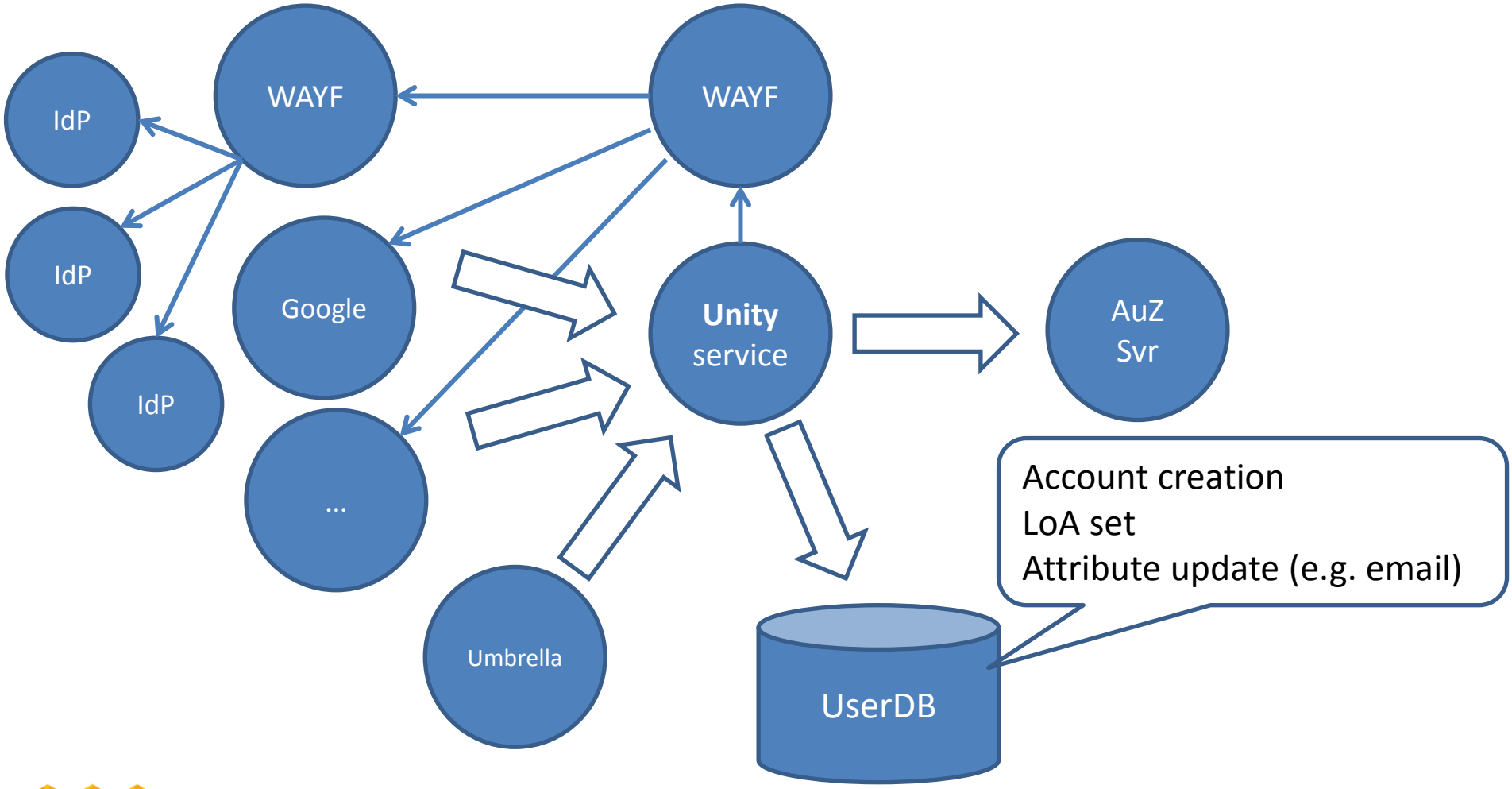


DN: EUDAT uid
Attributes:

- Community uid
- …

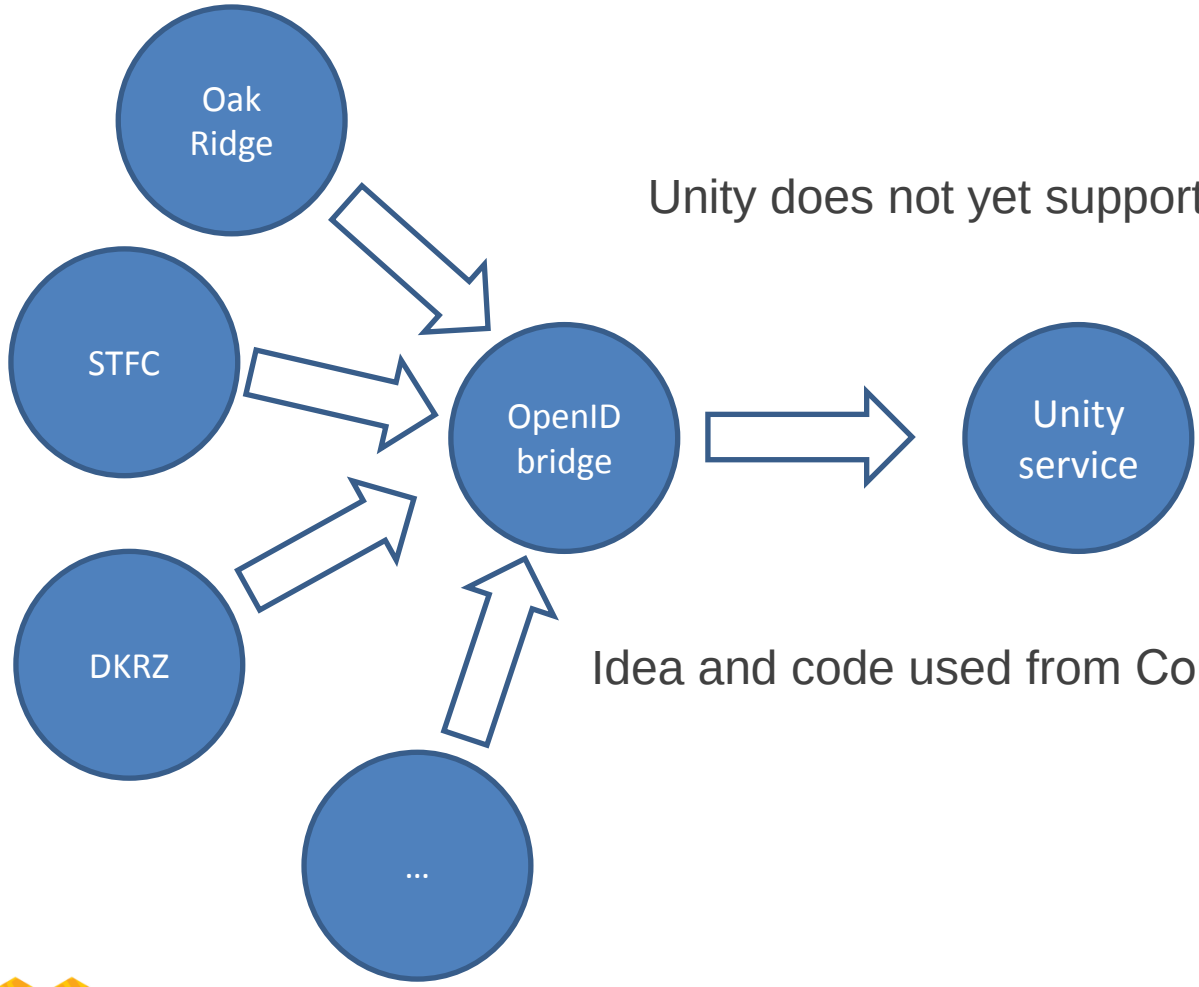
B2ACCESS
Identity & Authorisation

How does the WAYF (auth bridge) work?



EUDAT

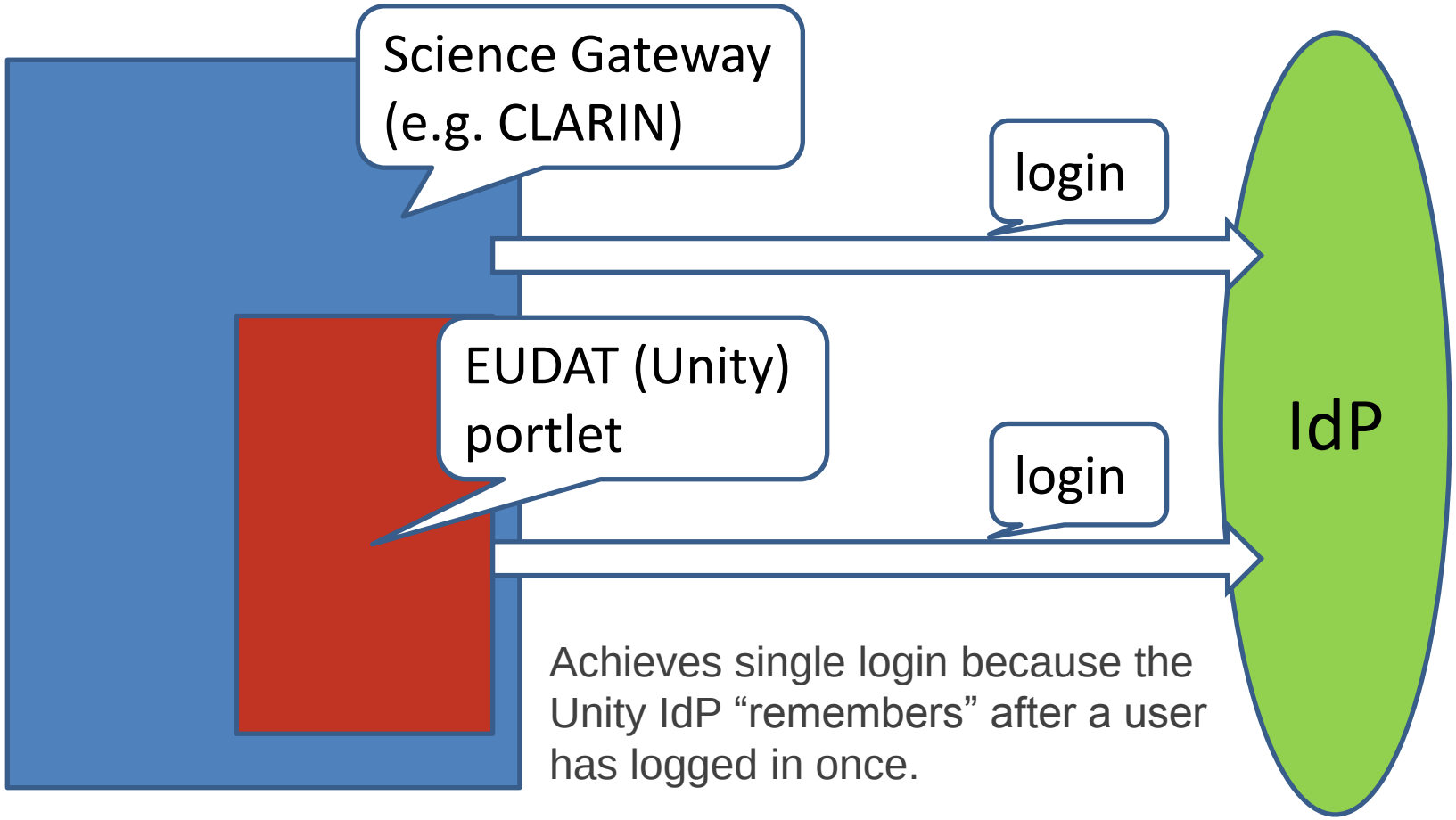
Support for OpenID via a bridge (ENES)



Unity does not yet support OpenID directly

Idea and code used from Contrail: build a “bridge IdP”

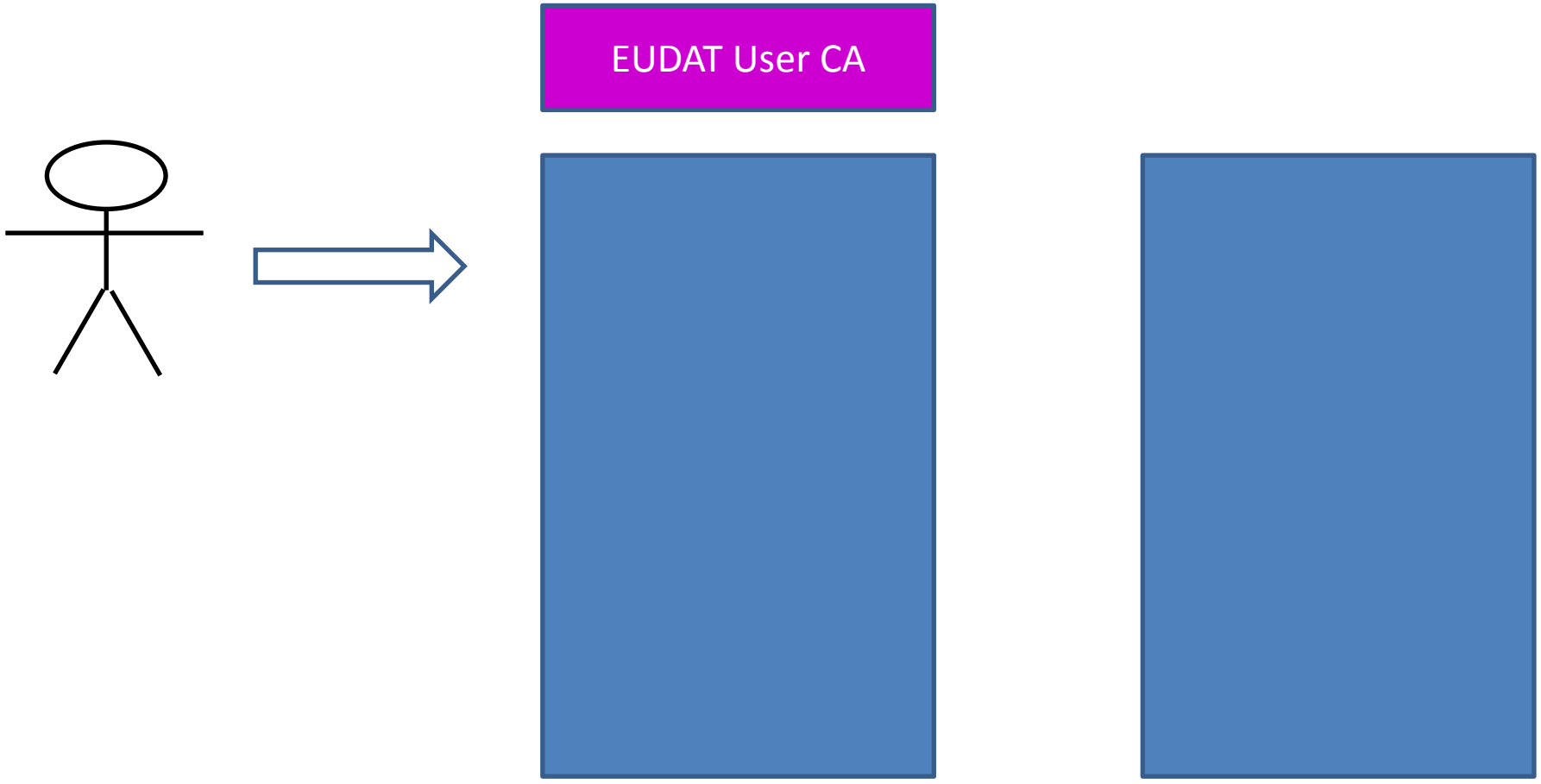
EUDAT portlet for the CLARIN science gateway



Non-Web (command-line) access to the Unity IdP supported as well (Unity has a REST interface)

B2ACCESS
Identity & Authorisation

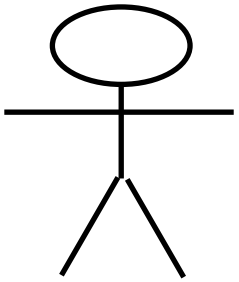
Accessing Data Via Portal

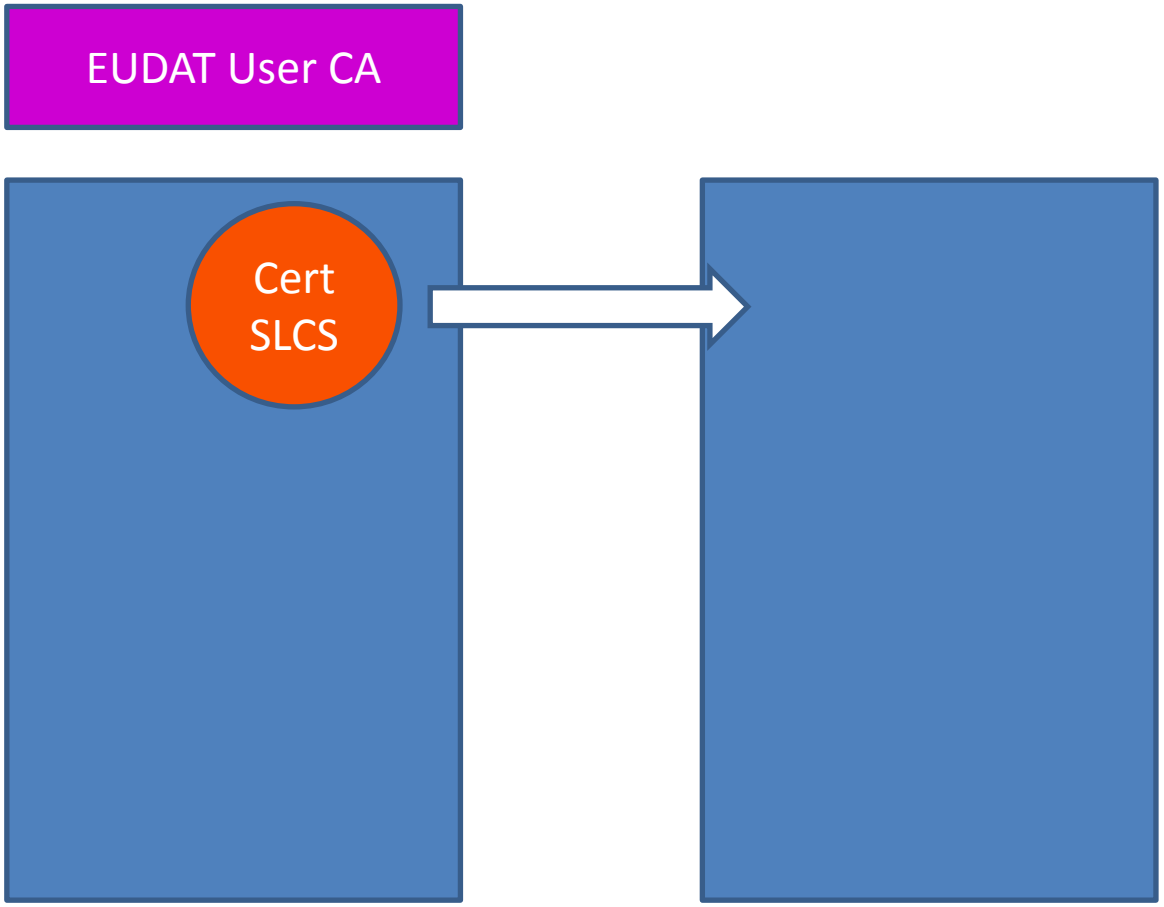


EUDAT

B2ACCESS
Identity & Authorisation

Accessing Data Via Portal

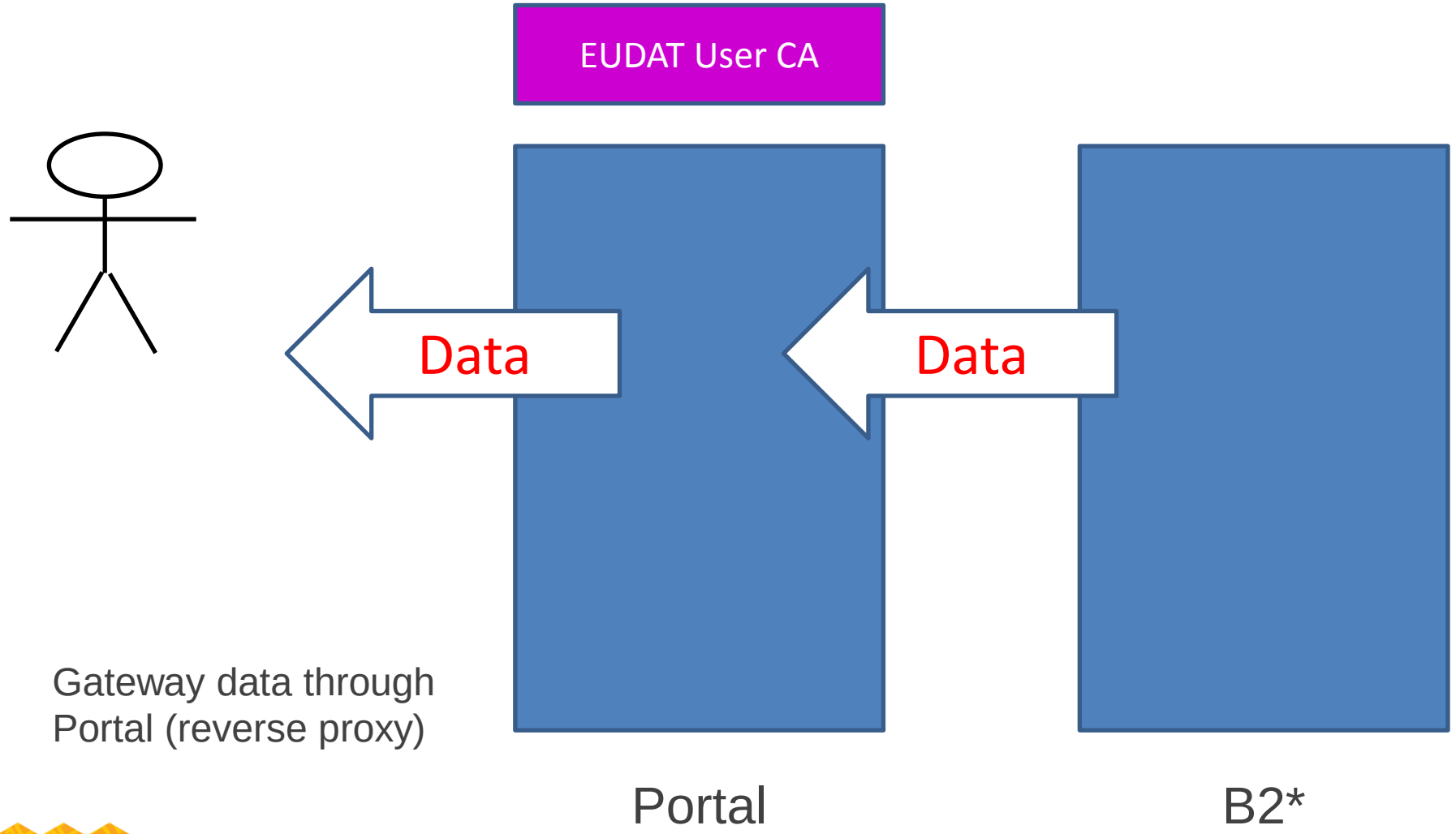




EUDAT

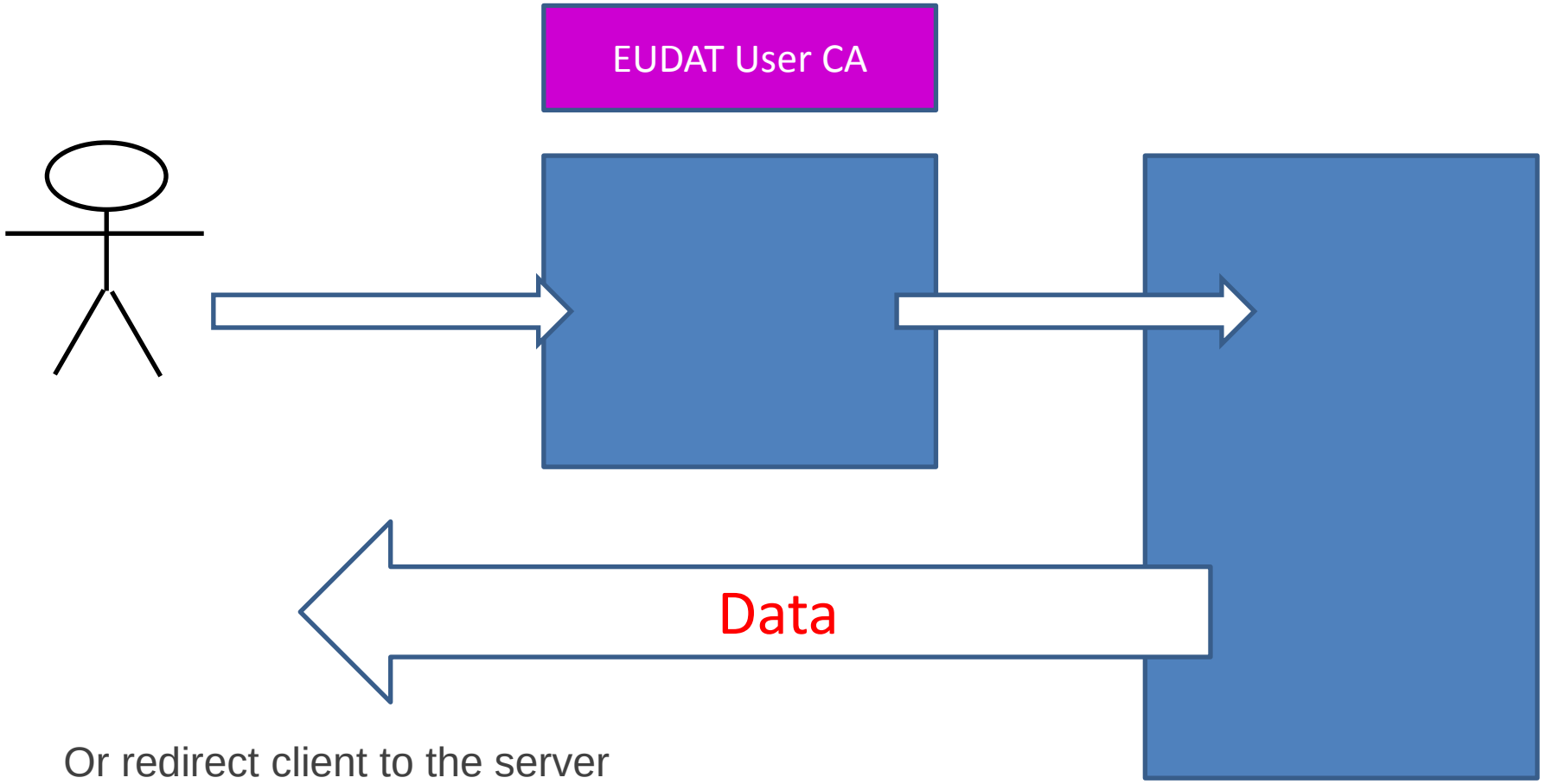
B2ACCESS
Identity & Authorisation

Accessing Data Via Portal



EUDAT

Accessing Data Via Portal



B2ACCESS
Identity & Authorisation

Current Status

- EUDAT AAI pilot implemented
- AAI integration with B2SAFE done
- Work on getting B2SHARE (repository), B2DROP (shared workspace) integrated.
- Pilots with Science Gateways of CLARIN (done), ENES (progress), EPOS (next)
- Working on making use of eduGain

EUDAT

B2ACCESS
Identity & Authorisation

Community Integration

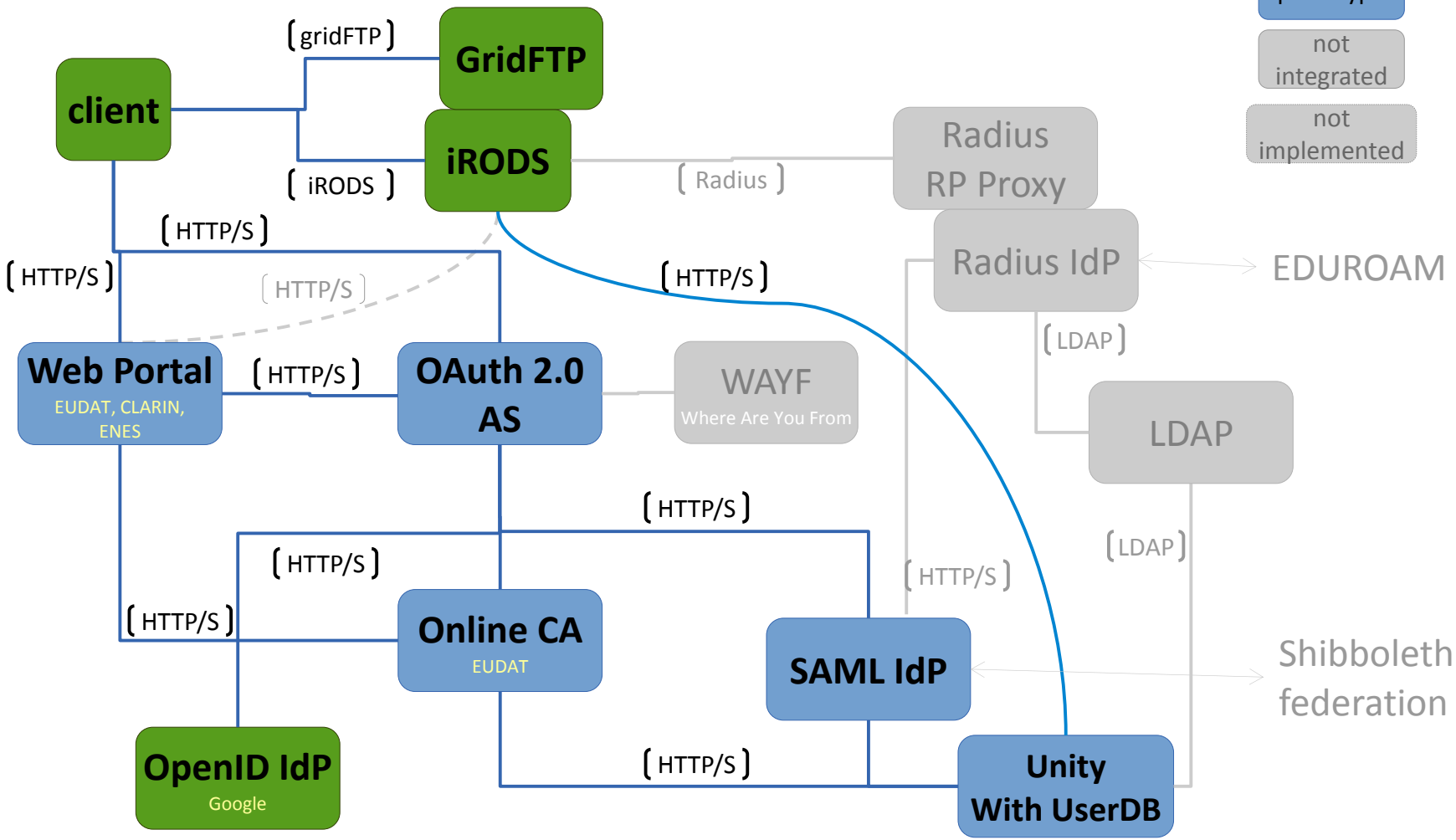
- Community integration needs efforts
  - also from the communities
- Needs *real* community identites
- Several options for integration with the EUDAT IdM based on the Unity service
  - options for portal integration
  - authentication via command-line tools supported
- EUDAT aiming to collaborate with other AAI efforts (e.g. AARC, eduGain)

EUDAT

we can explain more details …..

B2ACCESS
Identity & Authorisation

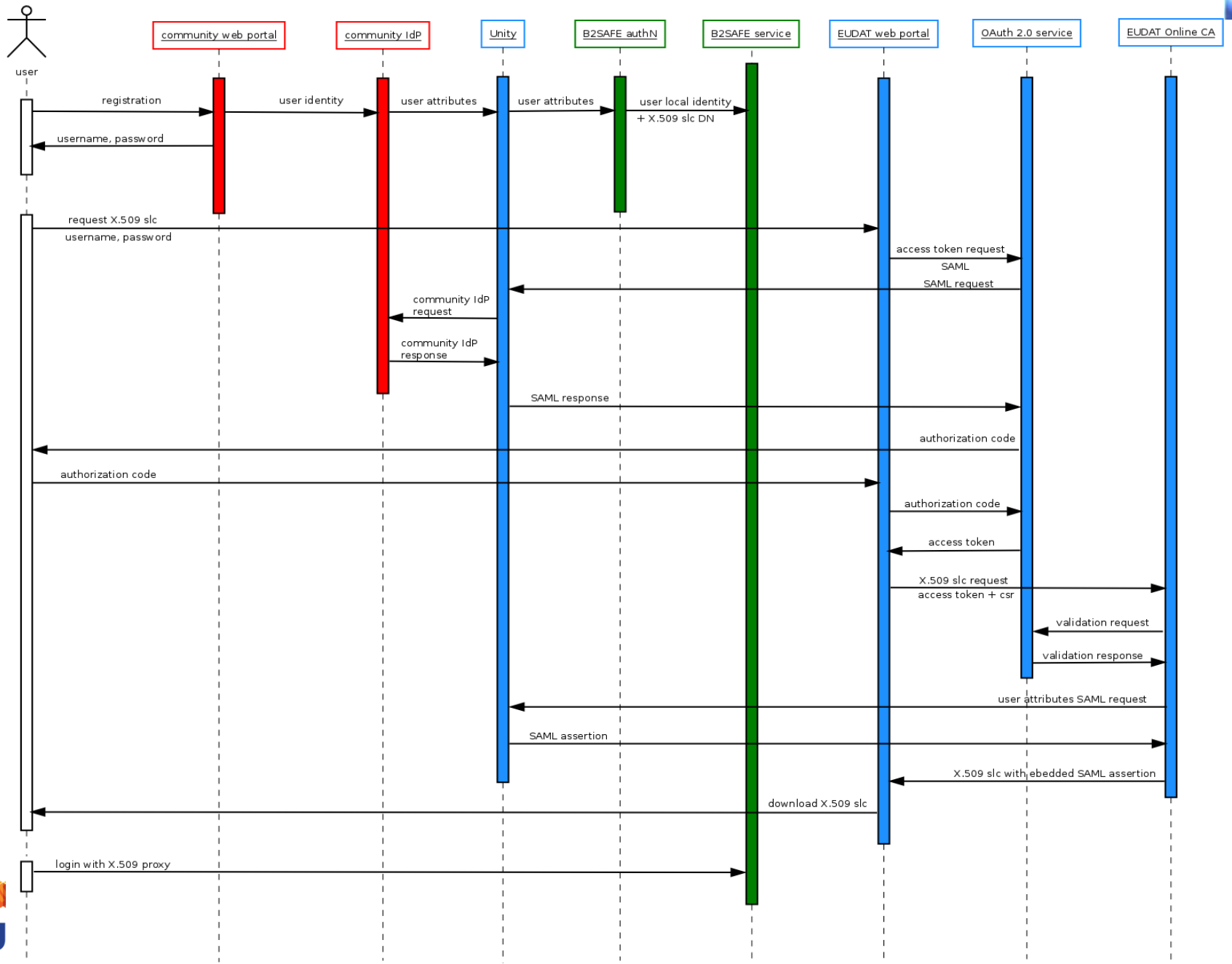
EUDAT AAI current status



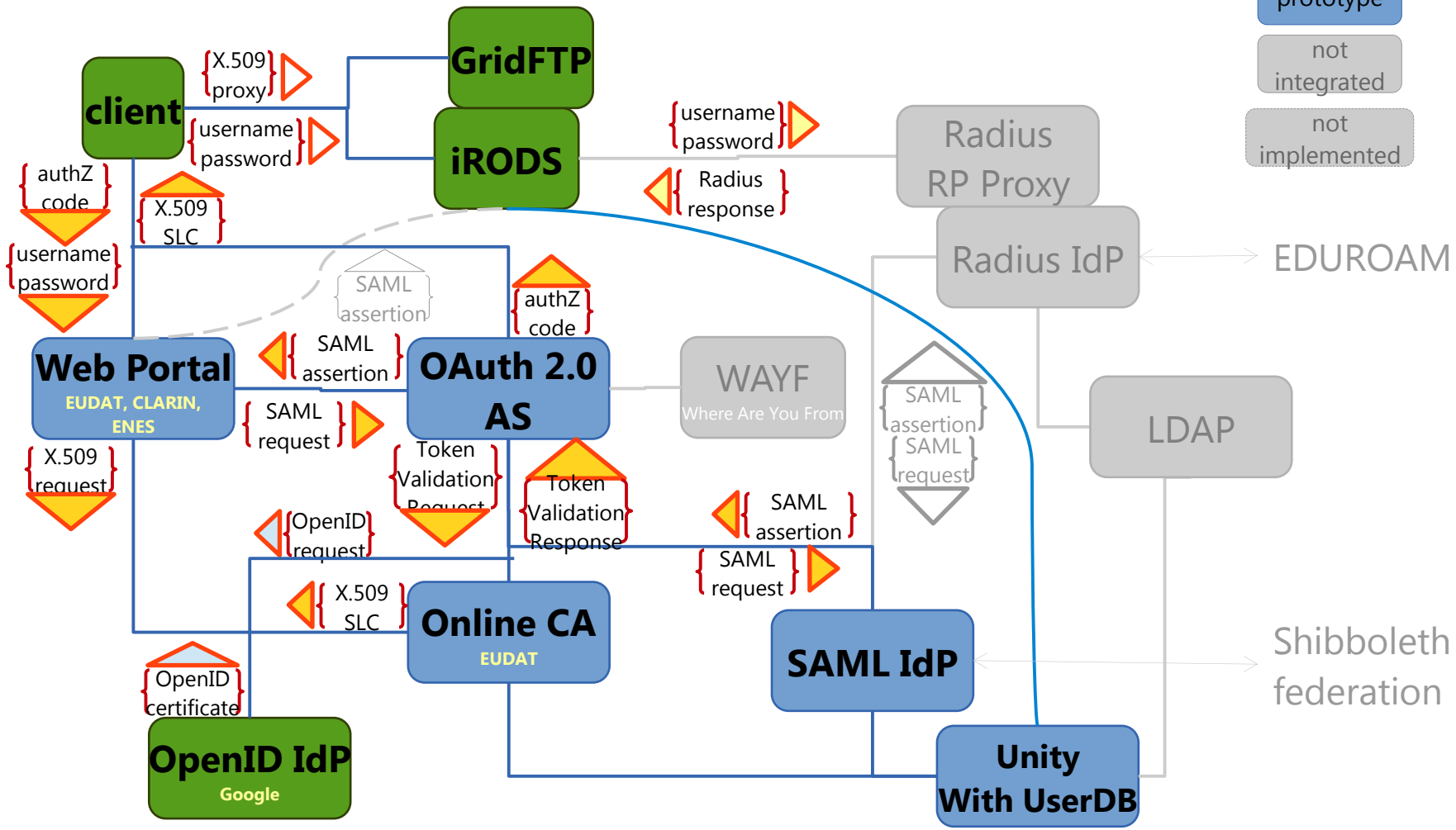
EUDAT

B2ACCESS
Identity & Authorisation

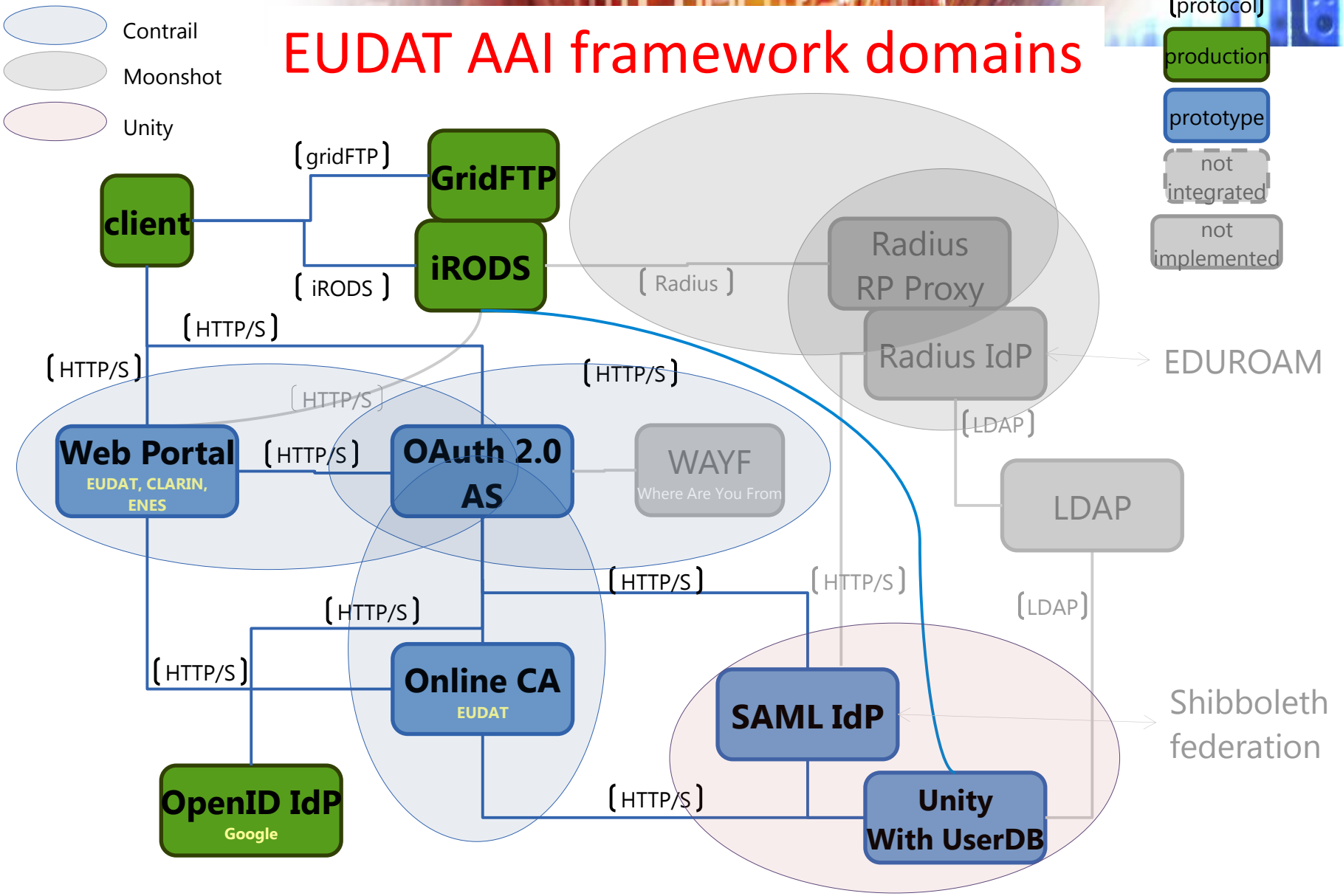
EUDAT AAI sequence diagram



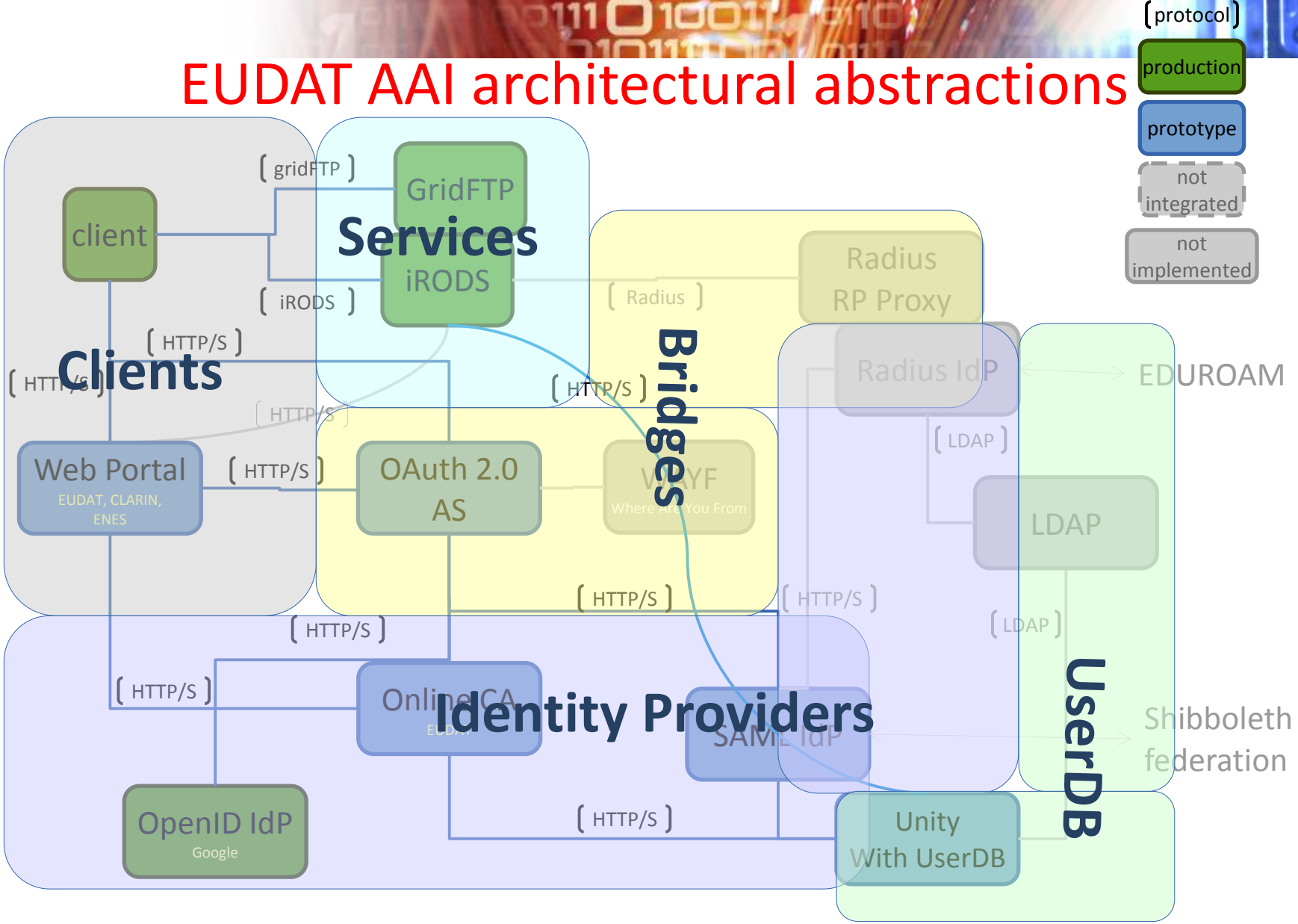
EUDAT AAI user credential flow



EUDAT AAI framework domains



EUDAT AAI architectural abstractions



EUDAT