AARC Authentication and Authorisation for Research and Collaboration

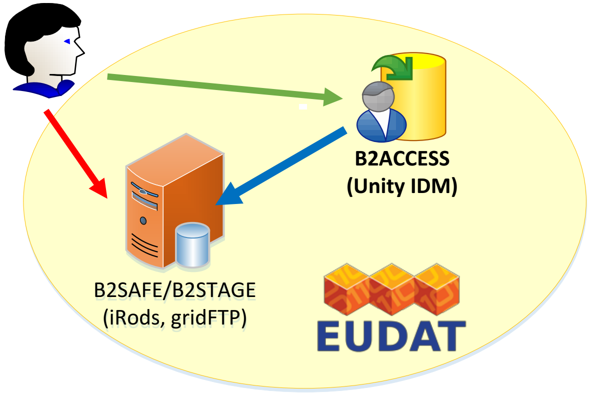
EUDAT – PRACE cross infrastructure integration pilot

scoping and approach

Michał Jankowski, Maciej Brzeźniak
AARC SA1.3
Poznan Supercomputing and Networking Center

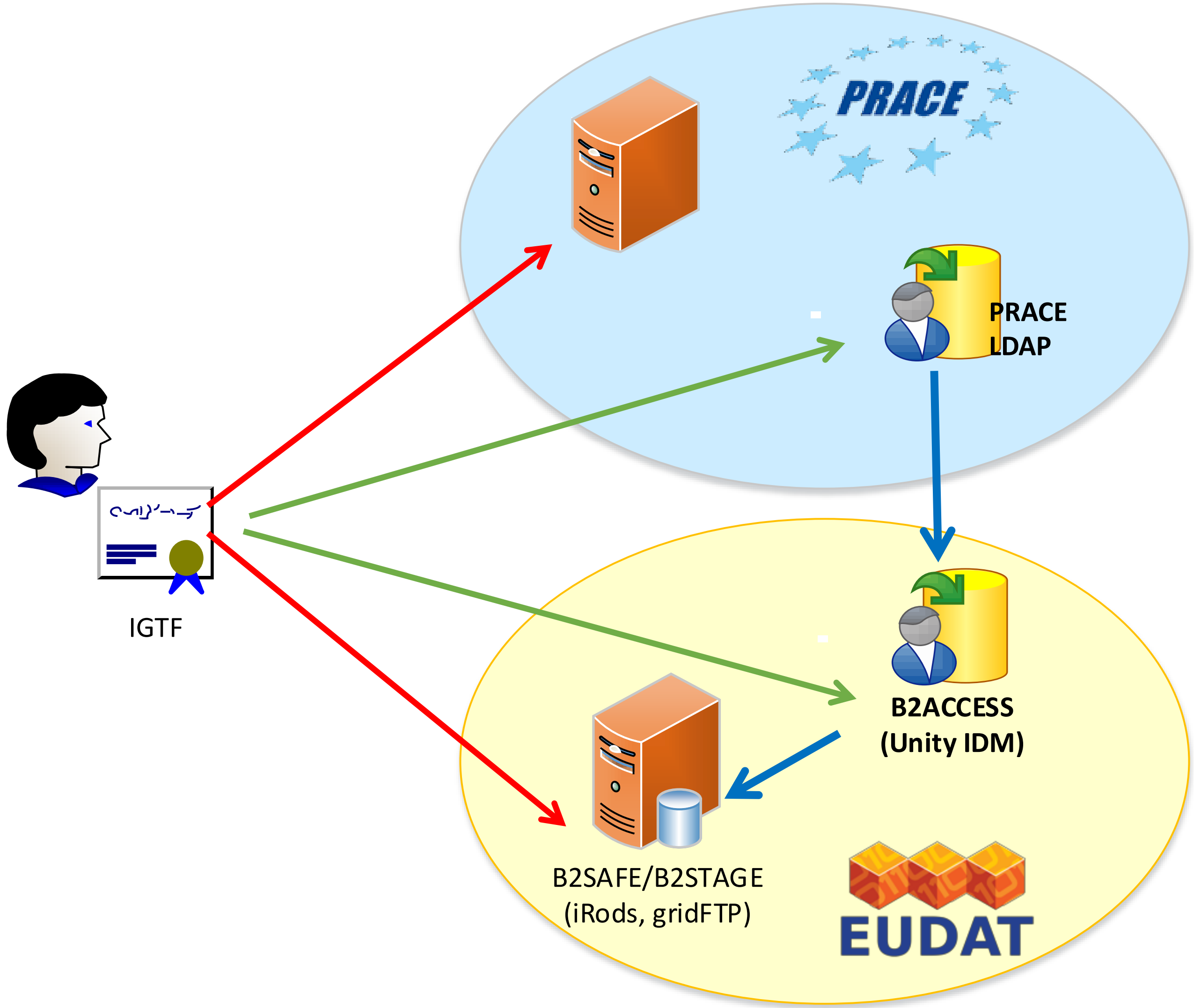
AARC General Meeting, Athens
20-22 March 2017

EUDAT so far scenario



- The user registers in B2ACCESS (and accesses it) using different types of credentials (SAML IdP, social ID, local username/password, X.509 (long living cert signed by IGTF approved CA)
- B2ACCESS admin adds the user to relevant group
- B2ACCESS issues X.509 short living cert signed by its internal CA
    - This cert will not be accepted by PRACE!
- The couple of scripts running on the resource (B2STAGE/B2SAFE service) periodically get users from B2ACCESS, provision accounts and map users to these accounts.
    - The mapping is based on DN generated by B2ACCESS –not appropriate for PRACE!
- The user accesses the resource using the EUDAT certificate

Scenario



1. PRACE LDAP -> B2ACCESS synchronisation
2. B2ACCESS -> B2STAGE synchronisation
3. Access to web based EUDAT services

PRACE LDAP -> B2ACCESS synchronization

- Cron script:
  - Collect selected users from PRACE LDAP (deisaUserProfile set to “EUDAT”)
  - For each collected PRACE user:
    - Create Unity entity with x500 name identity equal to PRACE user DN (if not already exist)
    - Add the entity to PRACE Unity group (if not already added)
  - For each Unity entity in PRACE group:
    - Remove the entity from this group if it is not within collected PRACE users

B2ACCESS – B2STAGE/B2SAFE integration - modification to the current mechanism

- Cron script:
  - Maps B2ACCESS groups to iRods users
  - Maps DN from IGTF certificate exactly as DN from certificate issued by B2ACCESS

```
/C=DE/L=Juelich/O=FZJ/OU=JSC/CN=a7f7c4b5-7005-4af6-b346-b87f6e8ba442/CN=226
/C=PL/O=GRID/O=PSNC/CN=Michal Jankowski
```

- Limitations:
  - Multiple users per account
  - Non up to date authorization information
  - Not very scalable

B2ACCESS – B2STAGE/B2SAFE integration - new mechanism

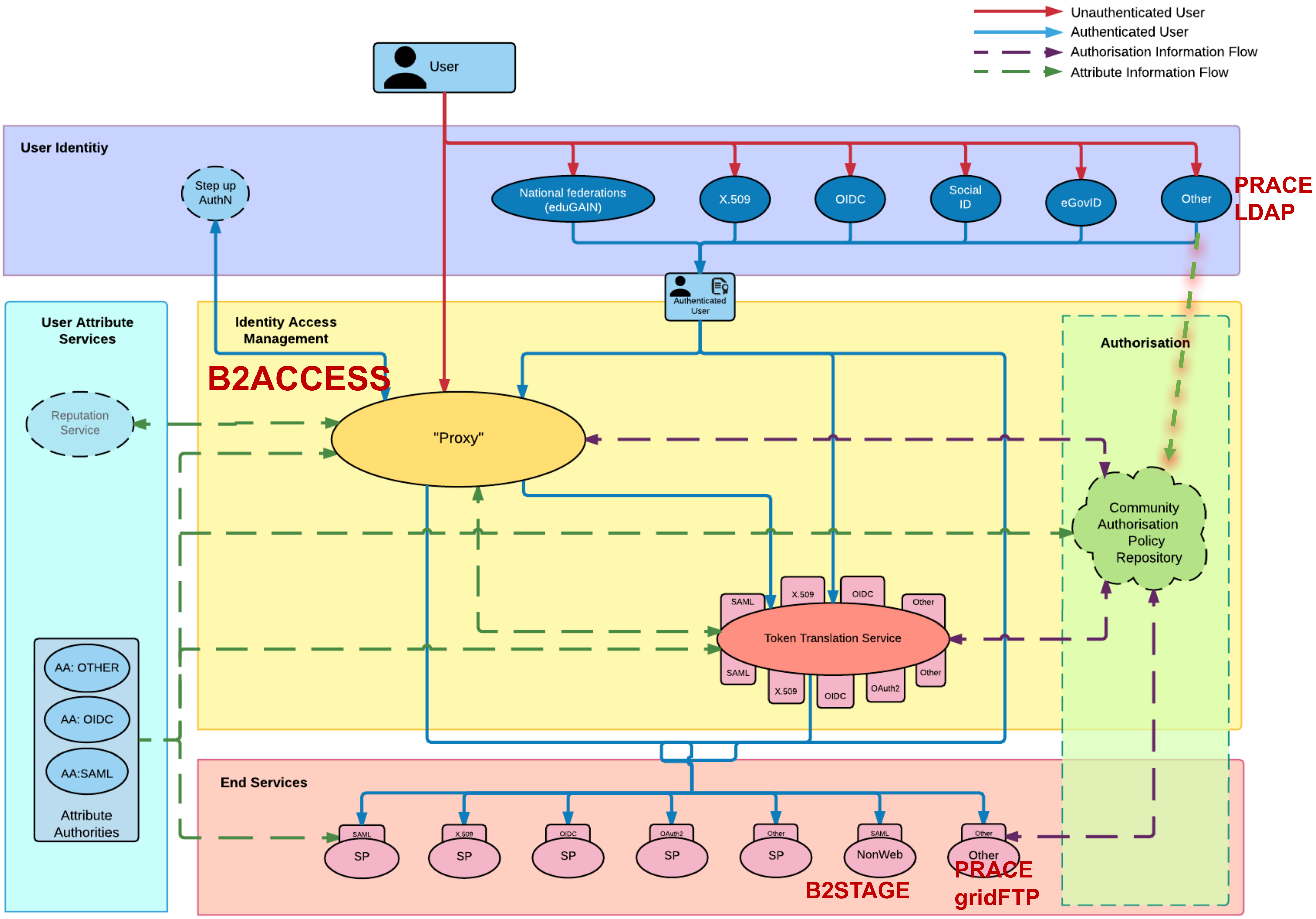
- Online user check using `gridmap_iRODS_callout` prior the mapping is done:
  - Get user (entity) info and groups from Unity
  - Provision local account
  - Associate/disassociate the local user with local groups according to group map configuration.
- This approach is not inline with some local policies
- It is preferred by PRACE
- PRACE group (project) -> single iRods user mapping is minimum required
- Both mechanisms may coexist providing careful configuration

Status and further work

- PRACE LDAP -> B2ACCESS script
  - Being evaluated by EUDAT
  - Group synchronisation will be added
- B2ACCESS -> B2STAGE ”old” mechanism
  - Ready for evaluation
- B2ACCESS -> B2STAGE ”new” mechanism
  - Proof of concept

- The work is intended to be put in production

AARC Blueprint Architecture



Deliverable DSA1.4:
Pilots to improve access to R&E relevant resources

- CILogon -like
- LDAP Facade
- SSH key management using COmanage and OpenConext
- SSH key provisioning for VMs using WATTS
- EUDAT-PRACE
- EUDAT-EGI (web and non-web)
- Federated access to ORCID
- LibreOffice/OwnCloud

- Elixir TTS with CILogon
- BBMRI AAI

Thank you

Any Questions?

AARC

https://aarc-project.eu

The work leading to these results has received funding from the European Union’s Horizon 2020 research and innovation programme under Grant Agreement No. 653965 (AARC).