De-provisioning - necessity even in proxy IdP/SP architecture

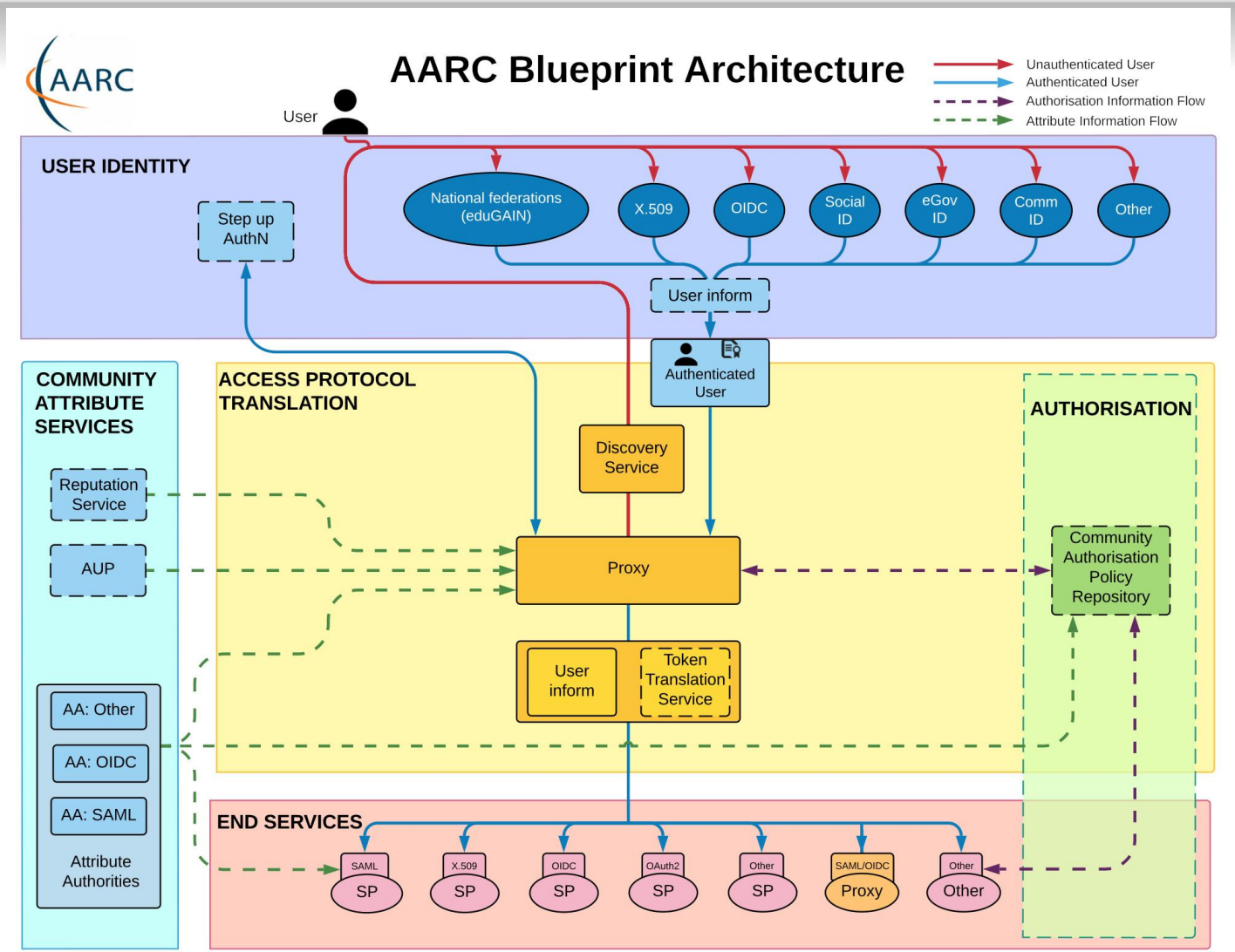
Slávek Licehammer
slavek@ics.muni.cz

cesnet

EGI Conference 2019
06. 05. 2019

UNIVERSITAS MASARYKIANA BRUNENSIS

AARC Blueprint Architecture



Proxy architecture

- Easy way to connect services
- Persistent identity for each user
- Harmonized attributes
- Authorization on proxy level
- Approval of AUP, data release, etc.

- All is done during sign in of a user

Services with extra requirements

- Some services needs to know user upfront or know when the user is no longer authorized
- Mailing list
- Cloud platforms
- Data storages
- VOMS
- Collaborative tools
- ...

Provisioning & deprovisioning

- Method to deliver user information to services
  - Access rights
  - Authorization informations (groups, roles)
  - User attributes (name, e-mail, …)
- Triggered without direct user interaction
- Services react accordingly
  - Creating accounts
  - Updating local user information
  - Disabling or deleting account

Benefits of (de-)provisioning

- Database of access rights for all users and services
- Database of which data released to services
  - GDPR
- Deprovisioning can be used to disable account when it have been compromised
- Provision access tokens for non-web access
  - SSH keys

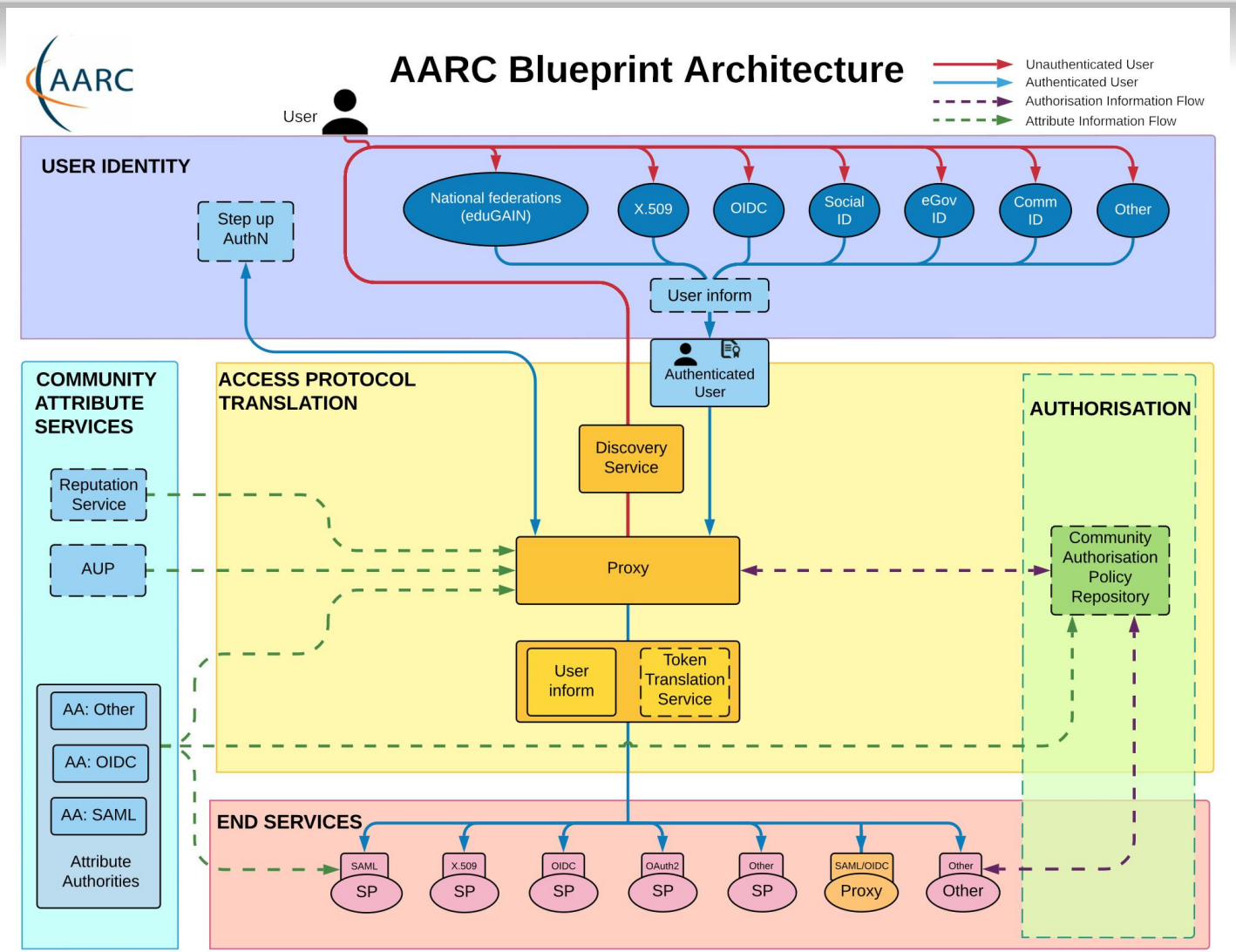
Implementation

- Transfer model
  - Periodic pull
  - Push model
- Transferred dataset
  - Changeset only
    - Need to ensure consistency
  - Full state
    - May have performance issues
- Protocols
  - LDAP, VOOT, SCIM, JSON, XML, OIDC, ...

Identity and access management

- Identity and access management
  - source for (de-)provisioned data
- Support for user life-cycle
  - Registration / import, expiration, renewal
  - Support also on service side
- Support for access management
  - Group, entitlements, capabilities management
  - Configurable provisioning to services

AARC Blueprint Architecture



Perun

- Identity and access management
- (De-)provisioning engine
- Open-source (https://perun-aai.org)
- Major deployment: ELIXIR, EGI, GÉANT
- EGI instance integrated with EGI Check-in
- (De-)provisioning connectors available for many services
  - Easy to develop new connectors

Summary

- Provisioning and deprovisioning notify services about changes in user attributes or state
- Deprovisioning is crucial for services with persistent user resources
- Can be handled with external identity and access management system
- Is aligned with AARC Blueprint Architecture

Thank you for attention

Slávek Licehammer
slavek@ics.muni.cz

cesnet

UNIVERSITAS MASARYKIANA BRUNENSIS