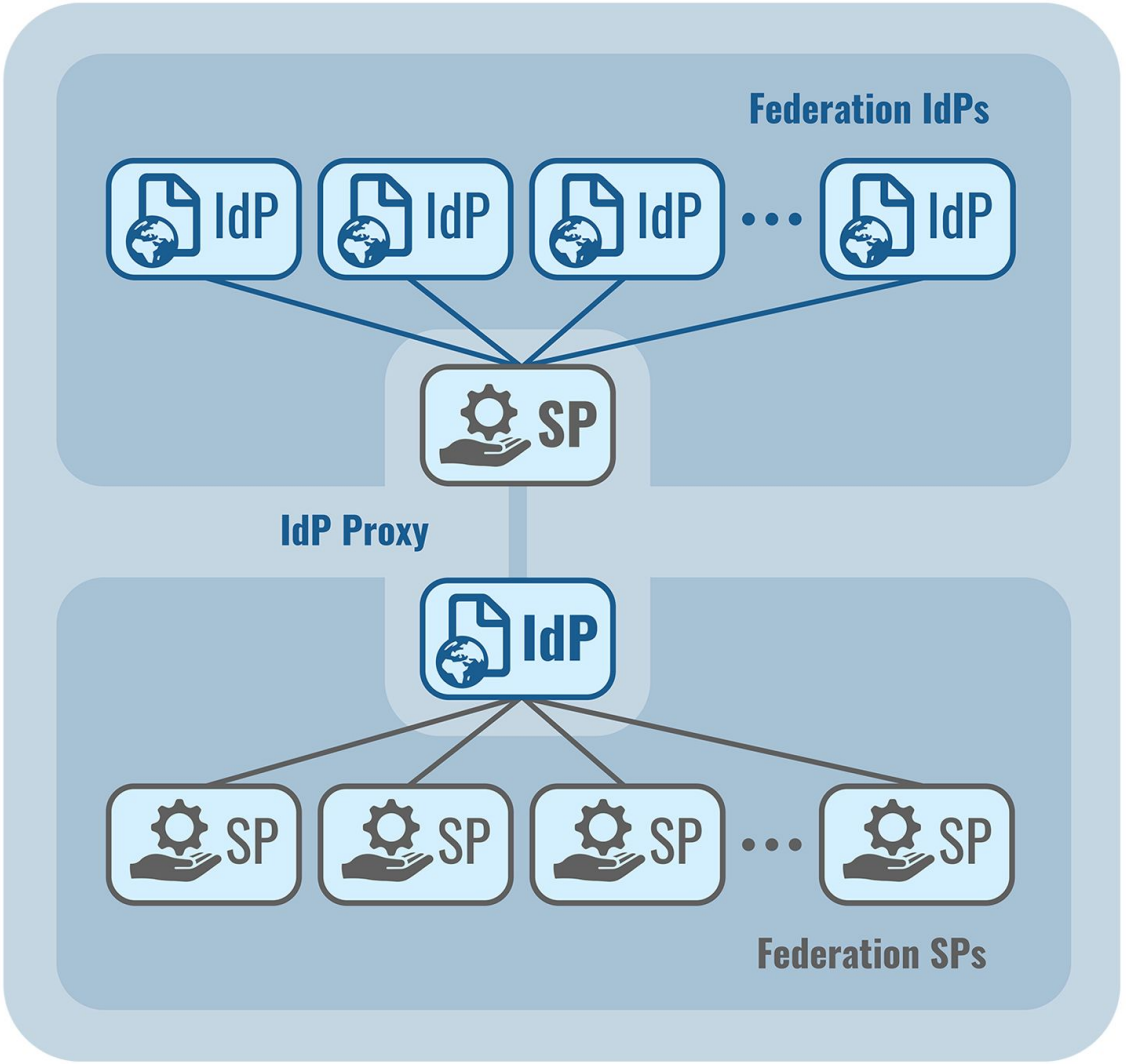
Efficient AAI for research communities using the IdP/SP Proxy

EGI Conference 2020
3. 11. 2020
Slávek Licehammer
slavek@ics.muni.cz


Federation IdPs
IdP
IdP
IdP
IdP
SP
IdP Proxy
IdP
SP
SP
SP
SP
Federation SPs

Standard features of proxy based infrastructure

- Protocol translation (SAML2, OIDC, …)
- Attributes harmonization
- Single persistent identifier for each user
- User registration
- Maintaining user profile
- Account linking

Potential

- Proxy architecture offers greater potential
- Single point where user have to go
  - Possible interception of the authentication flow

- CESNET and Masaryk university implemented additional proxy features
- Part of Perun ecosystem
- Used in several deployments
  - ELIXIR AAI
  - BBMRI AAI
  - Czech national e-infrastructure
  - ...

Features

Automatic account validity extension

- Account expiration is needed for various reasons
  - GDPR
  - Statistics
- Manual account renewal is burden for users
- Automatic renewal for active users
- Done on proxy, each time user signs in
- Can be conditional (e.g. based on affiliation)
- Can be combined with manual renewal process for non-active users
  - Expiration & notifications

Delegated authorization

- Typically SP/RP manages authorization based on attributes
- Proxy can do it instead - **delegated authorization**
  - No need to implement (coarse-grained) authorization on the service
- Based on data from underlying IdM system
- Proxy can offer next step for user if access in denied
  - Link to documentation
  - Redirection
  - Offer request for access (web form with optional approval process)
- Improved (and consistent) user experience

Acceptable Usage Policy management

- How to approve new versions of AUP?
- AUP can be on VO level or on SP/RP level
  - Multiple SP/RP can have same AUP
- Proxy can detect which AUP needs to be approved
  - Based on VO, accessed SP/RP, already approved AUPs
- Services don’t have to handle AUPs on their own
- Potential for AUP approval revocation

Multi-factor authentication

- Main user-case is accessing sensitive data or services
- Services can request multi-factor authentication
- User can choose multi-factor authentication everywhere
- Proxy request multi-factor authentication from home IdP
- If home IdP in not able to do multi-factor, Proxy can do it itself
- It’s possible to have a session (last use) of multifactor
    - User comfort vs. security

Identity provider enforcement requested by services

- SP/RP can request specific IdP or limit IdP in some way
  - e.g. do not allow social IdPs
- Proxy limits IdP selection in the discovery service
- Even if there is a single sign-on session in the proxy, new IdP is enforced
- Not very user-friendly in general
- Useful for very specific SP/RP (e.g. those with strict autheN requirements)

Manually assigned affiliations

- Obtaining affiliation information from IdPs might be problematic
- Community can managed affiliation for their members manually
- Designated “managers” per affiliation value
- Managers have to be trusted
  - Only usable in limited scope
- Can be enhanced with expirations and renewal processes
- Very useful feature for dealing with missing attributes form IdPs

Conclusion

- Many features can be done centrally on proxy instead of on each SP/RP
  - Useful for building infrastructure
  - Saving cost by doing development only in one place
  - Better user experience
- Intercepting user authentication flows
  - Approvals, registrations, showing important informations, …
  - Updating stored data
- Huge potential for proxy-based infrastructure for the future

Thank you for attention

EGI Conference 2020
3. 11. 2020
Slávek Licehammer
slavek@ics.muni.cz