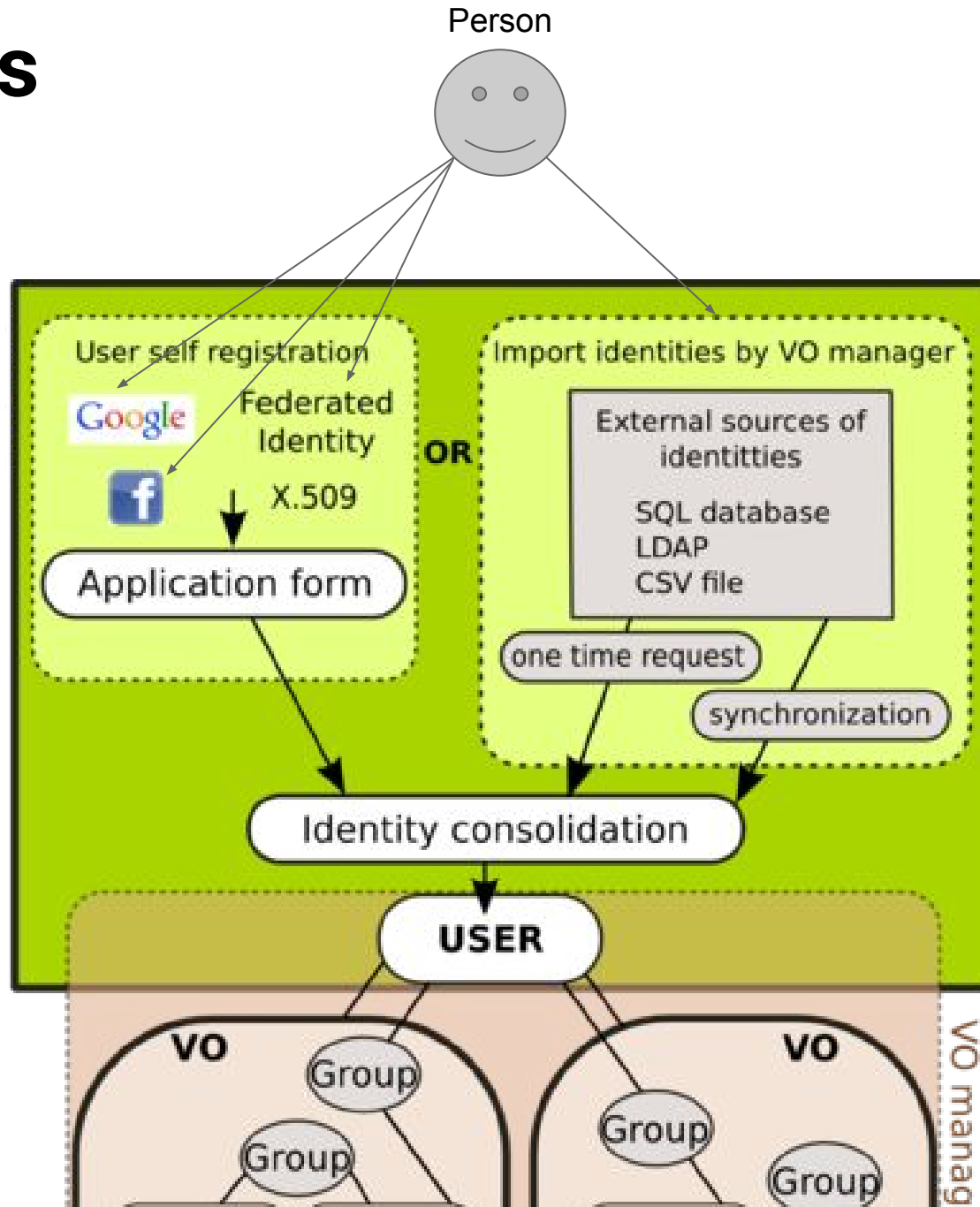




VO Administrator

Michal Procházka, Michal Šťava,
Slávek Licehammer, Pavel Zlámal

Entities





User

- Represents physical person
- Ideally every person has only one user representation in Perun
- User can be identified using various digital identities
 - social/federated identity, digital certificate, ...



Virtual Organization (VO)

- Basic entity for users categorization
- Special type of a group
- Defined membership rules
- Defined purpose
- At least one VO administrator
- Entity which can have an agreement with service providers



Resource

- Representation of end-service in a VO
 - VO specific configuration of service
 - Configurable from both sides



Member

- Representation of user in VO
- Must obey VO membership rules
- Usually has limited lifetime
- One user can be member in several VOs



Group

- Categorization entity inside the VO
- Provides delegation support
- Basic entity used for access control
- Group arithmetic



User lifecycle

1. Registration/import
2. Membership in VO
3. Membership in Groups
4. Access to the services
5. Membership renewal
6. Suspension/membership expiration



How to become a user

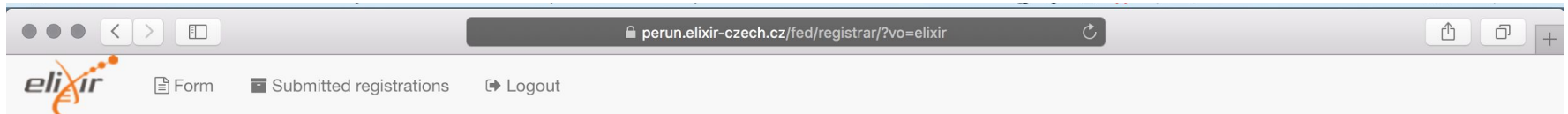
- Possess existing external identity supported by Perun
 - federated identity, social identity, digital certificate, ...
 - user's enrollment
- Import from existing identity management system
 - direct connection to the external system



Enrollment management

- Every VO or Group can define its own application form
 - request various information from the users
 - data can be filled from trusted source
- Initial vs. extension application form
- Automatic vs. manual approval
 - Redirections
- Text and notification customization
- Multilingual support

Example of registration form



Registration

Name*

Pavel Procházka

E-mail*

 prochazka.pavel@gmail.com

Email with verification link will be sent to provided email address.

Nickname*

Nickname will be used by some of the ELIXIR services, e.g. wikis.

> Submit

Fields with * are mandatory.



Import

- Users import from existing identity management system (external source)
- Periodic vs. one time
- Mapping rules between Perun and external source
- Various protocols supported
 - LDAP, SQL, XML, CSV, AD, ...



Account linking

- User can possess more identities
- Perun is able to link/unlink those identities
 - Heuristic search
- User can access Perun and its components with any of linked identity
- Identities can be transferred to end services

Account linking example


Perun Identity Consolidator - Mozilla Firefox

Perun Days 16.3.2017 ... 02. VO Managers - Prez... Perun web gui Perun Identity Consoli... +

https://perun.cesnet.cz/krb/ic/?locale=en

e-Infrastruktura CESNET

Network Computing Data storage Cooperation Multimedia Security AAI








 Identity consolidator

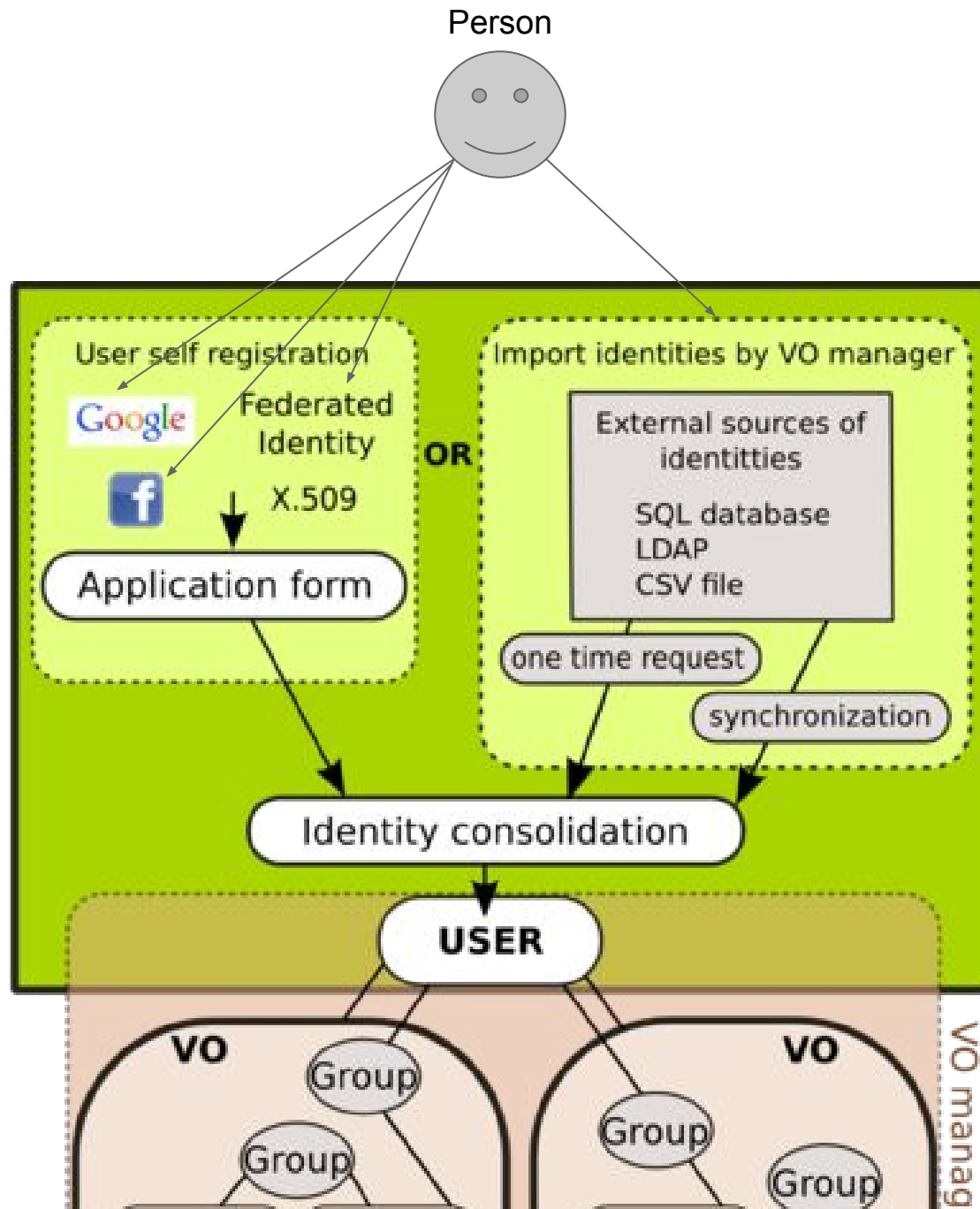
7 °C 09:10:33 15. březen 2017

Your are signed in by
MetaCentrum
Mgr. Pavel Zlámal (zlamalp@META)

Add new way of signing in...

Your authorization token will expire in 297s. Please make your choice before that.

 Using account from Czech university, Academy of Science or Hostel	 Using MetaCentrum account (CESNET eInfra login)	 Using account from university (world-wide)
 Using personal certificate (e.g. from IGTF)	 Using EGI account (EGI SSO)	 Using Elixir account
 Using account from social networks like Google, Facebook, LinkedIn etc.		





User's roles

- Perun admin
 - God
- VO admin
 - manages whole VO including Group and all associated entities
- Group admin
 - manages group membership
- User
 - self-management



Result

- Automation of user management processes
 - Service configuration is mostly static
 - Automatic synchronization of users in groups
 - Enrollment management

Live Demo

- Create a VO
- Invite member by an e-mail
- Add member from external source
- Create a group
- Add member to the group
- Account linking