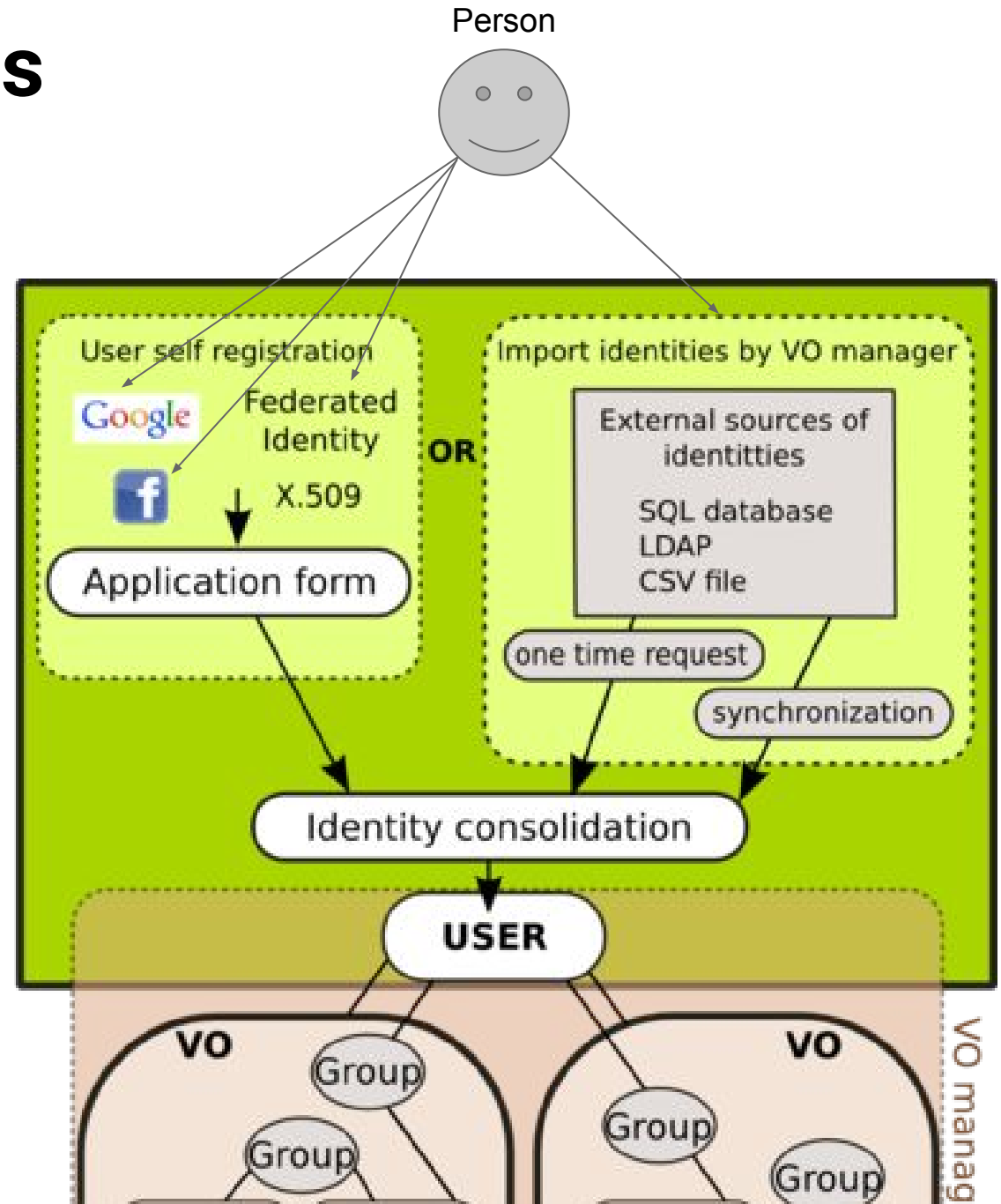
Perun

VO Administrator

Michal Procházka, Michal Šťava,
Slávek Licehammer, Pavel Zlámal

Entities


Person
User self registration
Google
Federated Identity
X.509
Application form
OR
Import identities by VO manager
External sources of identitties
SQL database
LDAP
CSV file
one time request
synchronization
Identity consolidation
USER
VO
Group
Group
VO
Group
Group
VO manag

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

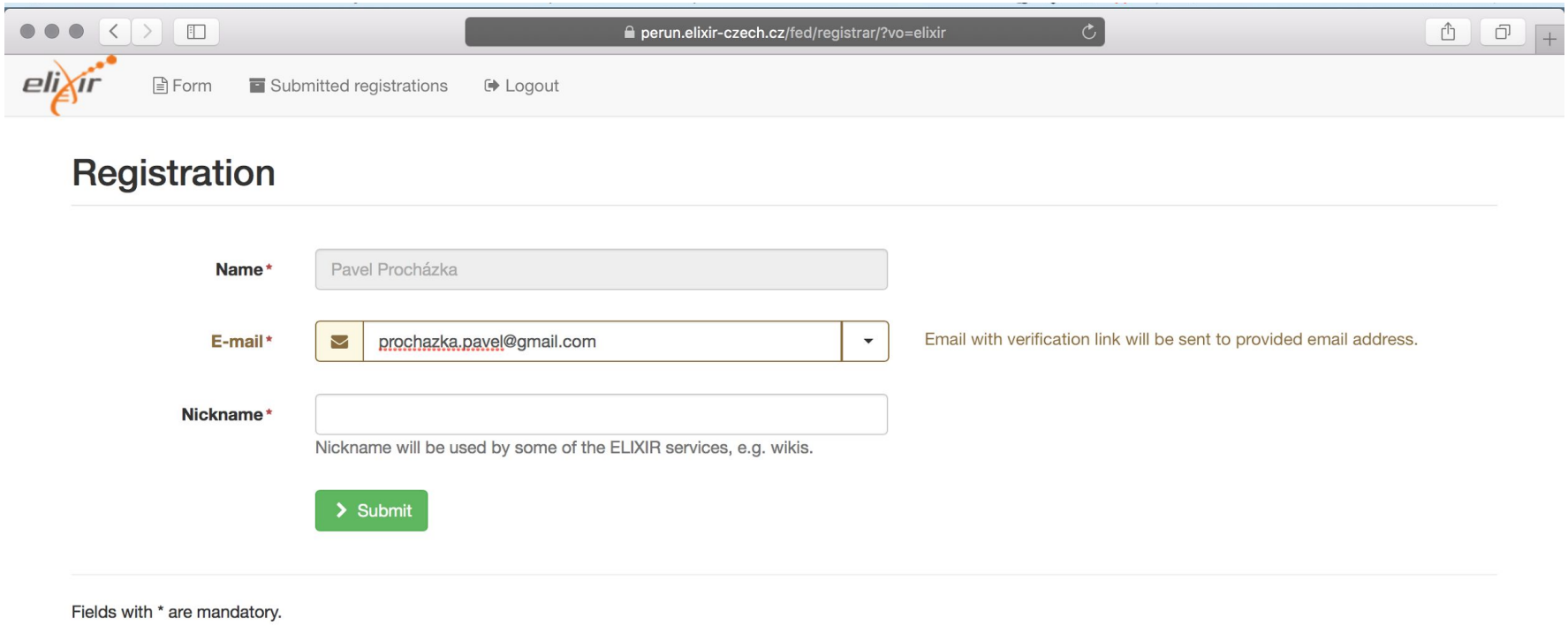
- Import from existing identity management system
  - direct connection to the external system

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



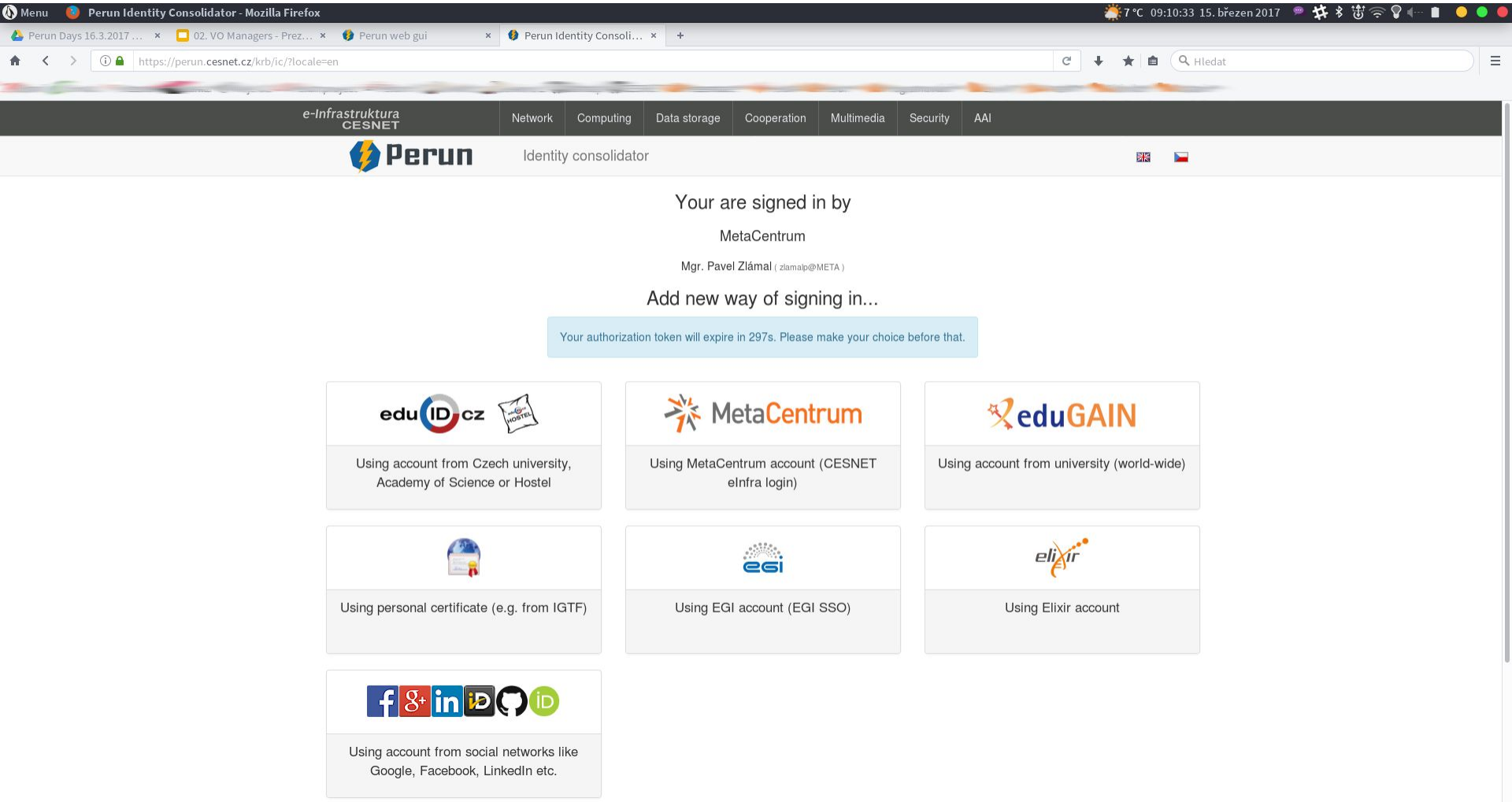
Import

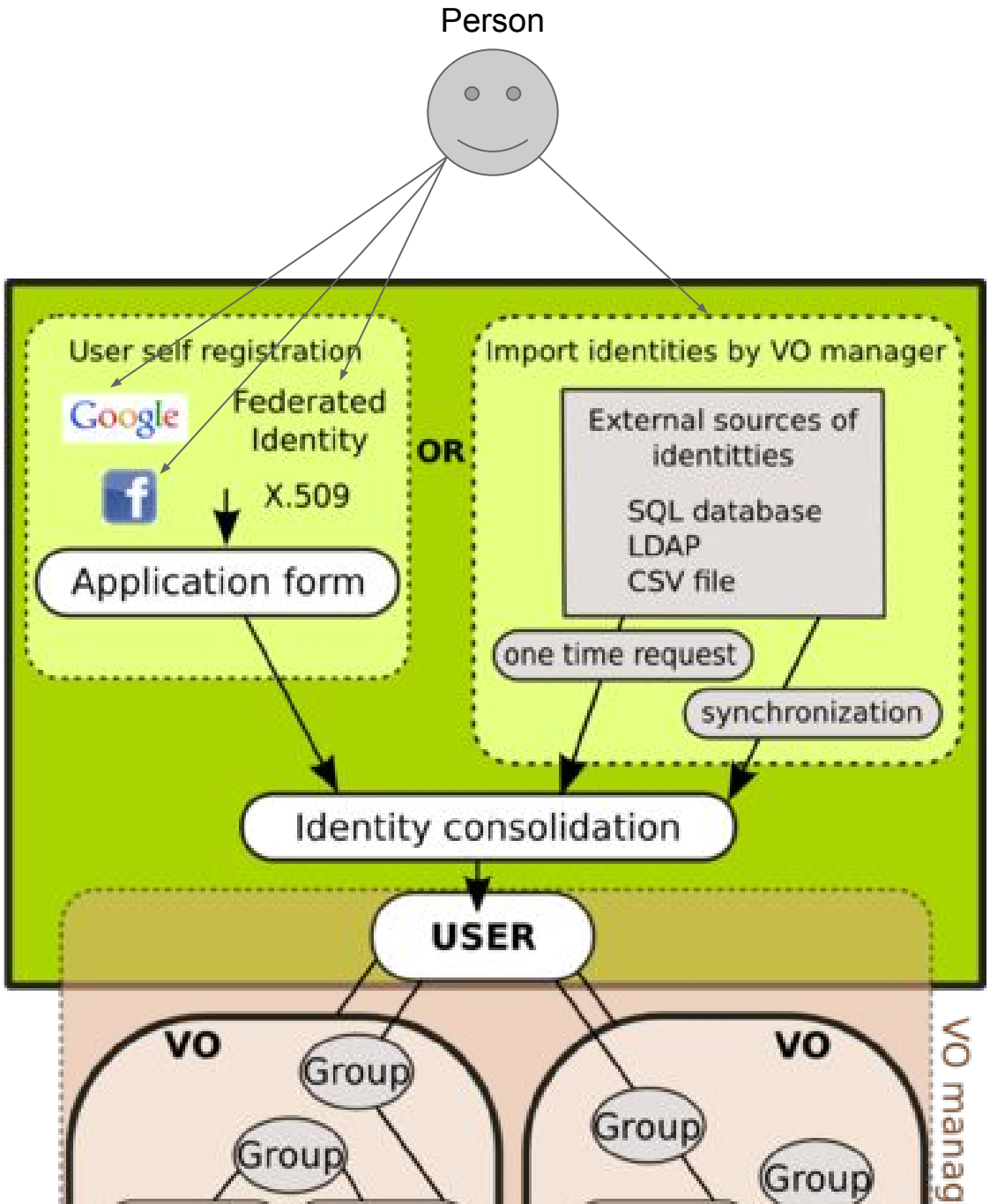
- Users import from existing identity management system (external source)
- Periodic vs. one time
- Mapping rules between Perun and external source
- Various protocols supported
  - LDAP, SQL, XML, CSV, AD, ...

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




Person
User self registration
Google
Federated Identity
X.509
Application form
OR
Import identities by VO manager
External sources of identitties
SQL database
LDAP
CSV file
one time request
synchronization
Identity consolidation
USER
VO
Group
Group
VO
Group
Group
VO manag

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