National Czech Programme | eosc

AAI and the Service Support System

Eliška Blažková, Lucie Hošková

Co-funded by the European Union

MINISTRY OF EDUCATION, YOUTH AND SPORTS

cesnet

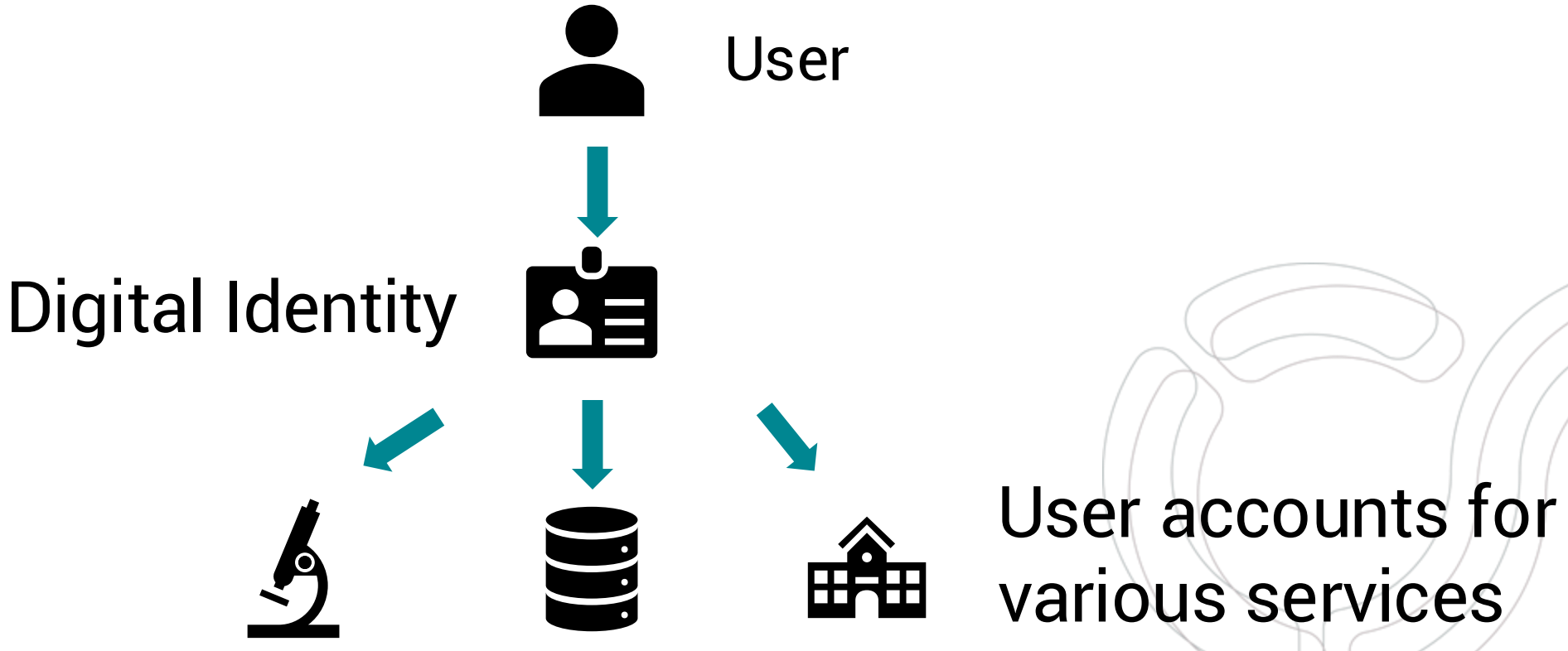
NRP project registration number

CZ.02.01.01/00/23_014/0008787

What is AAI?

- **"Authentication and Authorization Infrastructure"**
  - Login and access rights management across organizations
- **Benefits of using AAI:**
  - **Ease of use**
    - One account for one person across different services
  - **Comfort**
    - Only need to confirm login occasionally, instead of logging into each service every time
  - **Control**
    - Different levels of access for different groups of users

How Does It Work?



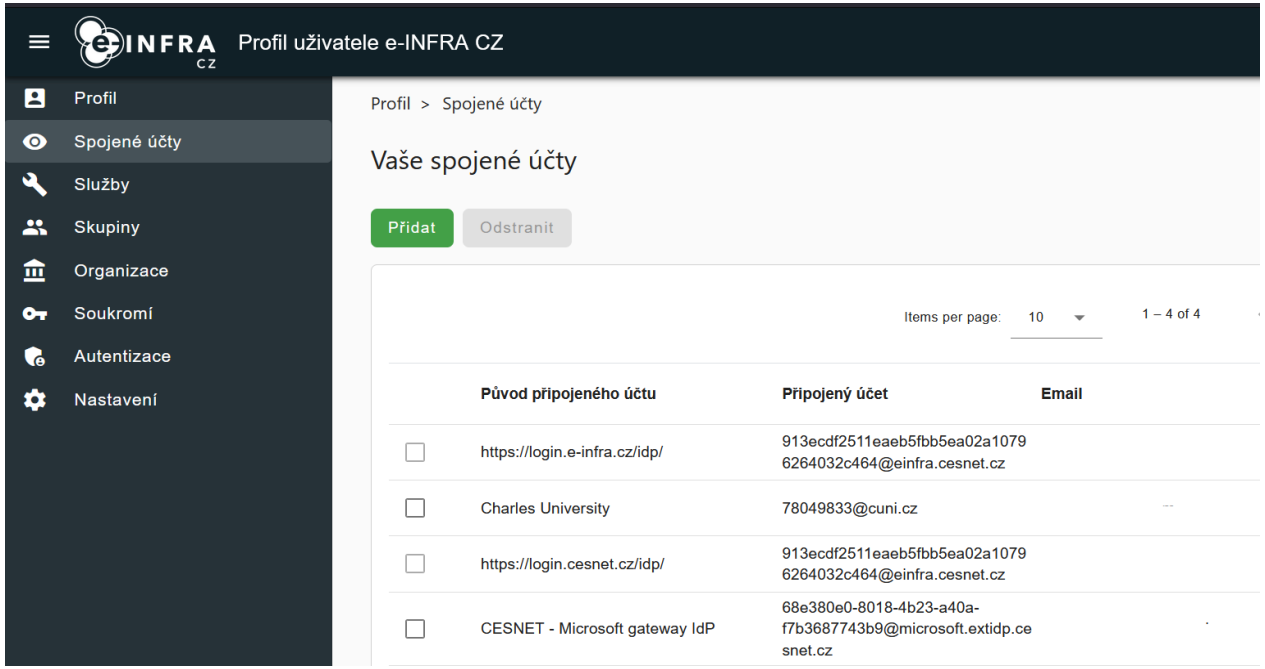
AAI in NRP

- Ability to **access all EOSC services via e-INFRA login** – including data repositories created using the **National Repository Platform**
- It is **MANDATORY** for repositories to be connected to e-INFRA AAI
- e-INFRA login operates using eduID which is part of eduGAIN
  - Identifiers for international federation of academic and research organizations
  - **You don't have to have eduID from Czech institution to be able to log in**

e-INFRA CZ Profile

e-INFRA CZ User Profile

- Personal profile where researchers can manage their e-INFRA user account
- Setting up and managing your digital identities



How to log in to e-INFRA?

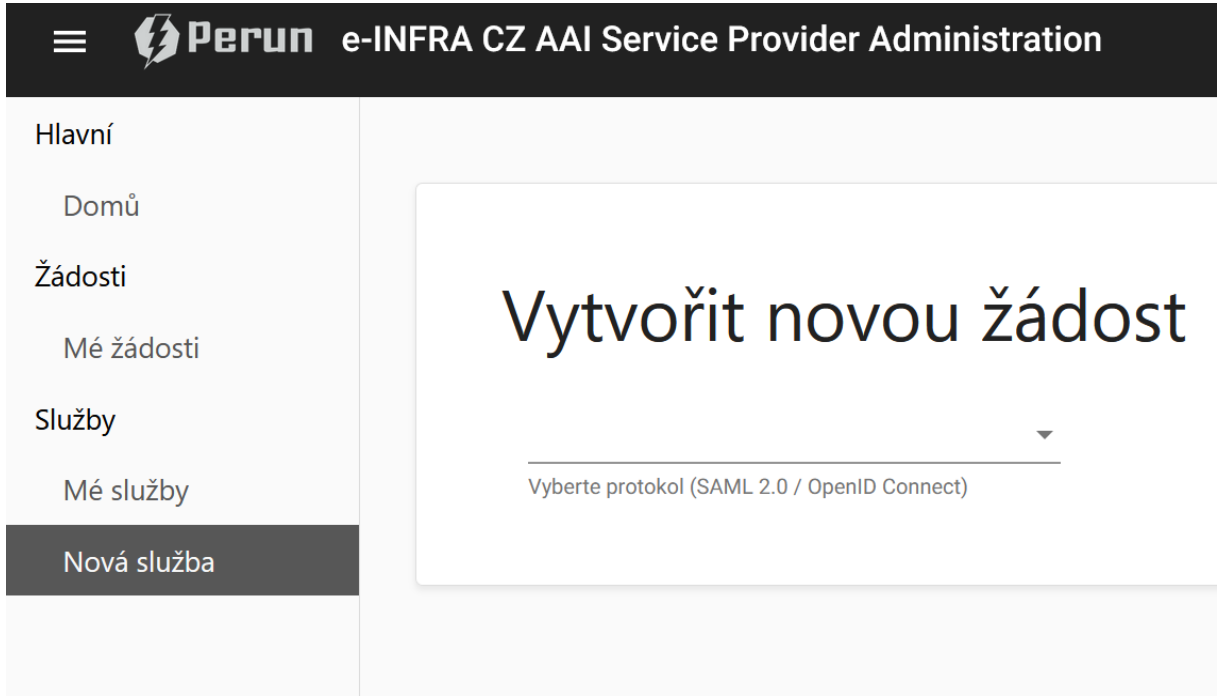
- **Academic / reseach organisation credentials**
- **Through external services**
  - It is possible to **connect your personal e-INFRA ID to** your accounts from **external services** (e.g. GitHub, ORCID) through Perun
  - These can then be used for login to e-INFRA

- The **same principle applies when works for multiple institutions**. They can be connected through Perun and your e-INFRA ID will know they both belong to one identity – you.

Perun AAI - Identity and Access Management (IAM)

e-INFRA CZ Service Provider Administration dashboard

- For a repository administrators
- Managing user groups
- Sending out invites
- Configuring the repository



Repository in NRP and the AAI – What are the conditions?

If you want to use NRP services and infrastructure for hosting your repository, you need to adhere to the Conditions for Creating New and Modifying Existing Domain Repositories.

Expected Responsibilities of the Repository Administrator	Establishing and implementing roles and permissions within user communities in the repository instance, e.g. common depositor, curator, approver. Linking these roles to groups of people in e-INFRA CZ AAI. Setting and implementing additional rules to control access to data for user groups, e.g. sharing specific data with selected users only.
Expected Responsibilities of the Repository Administrator	Integration of the repository instance with user authentication via e-INFRA CZ AAI, preferably using the OIDC protocol. Definition and implementation of roles and permissions within user communities in the repository instance, e.g., regular contributor, curator, approver. Linking these roles to user groups in e-INFRA CZ AAI. Configuration and implementation of additional access control rules for user groups, e.g. sharing specific data only with selected users. Definition and implementation of the user lifecycle in the repository, including the removal of inactive users.

Before You Begin

1) Read through the AAI terms and conditions.
2) Decide, who is going to be **the lead AAI coordinator for your repository** and **who is going to be helping with the more IT related side of things**.
3) Familiarize yourself with the AAI terminology and architecture in NRP.

1st step

Contact the repository systems specialists

- Tell us about your wish to implement the AAI in your repository.
- We will give you a **set of six basic administrative questions** to prepare while we facilitate meeting with the Perun AAI team.
  - repository name, repository platform, name of the lead technical coordinator etc.

2nd step

Set up the OpenID Connect (OIDC) in your repository

- OIDC is a **token-based security protocol for authentication between services**. It is an extension of OAuth 2.0
- This is the main way Perun authenticates users.

Request the creation of new service aka facility (your repository)

- Done by **filling in a form** in the e-INFRA CZ AAI Service Provider Administrator.
- Once the AAI team processes your request, they will connect to your OIDC and give you the space and time to iron out any issues.

3rd step

Give the AAI team the information about how you want to control the access to repository accounts

- Do you want to give **different users different access roles**?
- Do you want to review each new user before giving them the access to the repository account or **can it be automated** and if so, what are the criteria to allow the automatic account aproval?

Now everything is set up and ready to be used!

Service Support System

- **Repositories in NRP must provide their users with L1 support**
  - L2 and L3 support is provided by the NRP infrastructure
- Basically, each repository must have a dedicated "helpline" that the users can easily access if they ran into any problems while using the repository.
  - It is up to individual repositories how they will manage this support, but **CESNET can provide them with a RT system**.

Service Support System – L2 and L3

What if a problem is too complicated for the repository administrator to handle?

- CESNET will be providing a **central Service desk**, which you will be able to turn to once your repository is running and you encounter any bigger problems (like AAI suddenly not working, the whole repository is down), or if you will have any additional **questions about the NRP services**.

Service Support System – L2 and L3

- The Service desk will forward your query to dedicated experts that can advise you with your problem – be it AAI, questions about licenses, or questions about data stewards.
- **The system is still WIP,** but some of those mentioned groups are already up and taking questions.
- **During the process of creating your repository, always turn first to the repository systems specialists**, who will be able to forward your questions to the most suitable person.

National Czech Programme

eosc

Q & A

Co-funded by the European Union

MINISTRY OF EDUCATION, YOUTH AND SPORTS

Emerging Data Curator Community

- living (EOSC-CZ supported) Data Stewards Community
  - www.eosc.cz/en/communities/data-stewards
  - sharing know-how and experience
  - helping each other with day-to day data steward chores
  - domain-specific training (supported by EOSC-CZ)
  - in-person meetings (summer school and others)
- **datasteward.cz** Discord server is a core part of the network
  - We are considering setting up an online place for data curators and data administrators

Repository Administrators & Data Curators Community - preliminary Qs