Perun AAI

Martin Kuba <makub@cesnet.cz>

Konference e-INFRA CZ 10.5.2022

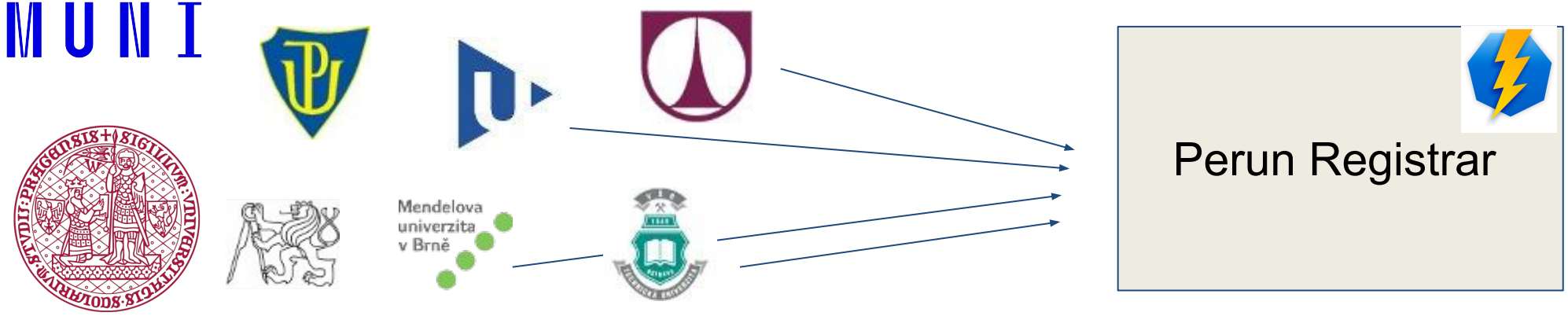
cesnet MUNI CERIT-SC VŠB TECHNICKÁ UNIVERZITA OSTRAVA | IT4INNOVATIONS NÁRODNÍ SUPERPOČÍTAČOVÉ CENTRUM

Historie spojování a Peruna

- v roce 1996 se spojila superpočítačová centra MUNI, UK a ZČU do **MetaCentra**
  - vytvořen systém Perun pro přijímání přihlášek a správu účtů na strojích MetaCentra
- v roce 2011
  - MetaCentrum vytvořilo s datovými úložišti a videokonferencemi tzv. Velkou Infrastrukturu CESNET, od 2016 **e-infrastrukturu CESNET**
  - Superpočítačové Centrum Brno se transformovalo do **CERIT Scientific Cloud**
  - systém Perun začal zajišťovat přihlášky a správu účtů e-infrastruktury CESNET i CERIT-SC
- v roce 2022
  - vzniklo jednotné AAI e-infrastruktury **e-INFRA CZ**
  - systém Perun zajišťuje přihlášky a správu účtů pro CESNET, CERIT-SC a IT4Innovations
- obdobně na bázi Peruna v roce 2016 vzniklo tzv. **ELIXIR AAI** a v 2017 **BBMRI-ERIC AAI**, v roce 2022 jsou spojovány do **Life Science Research Infrastructures AAI**

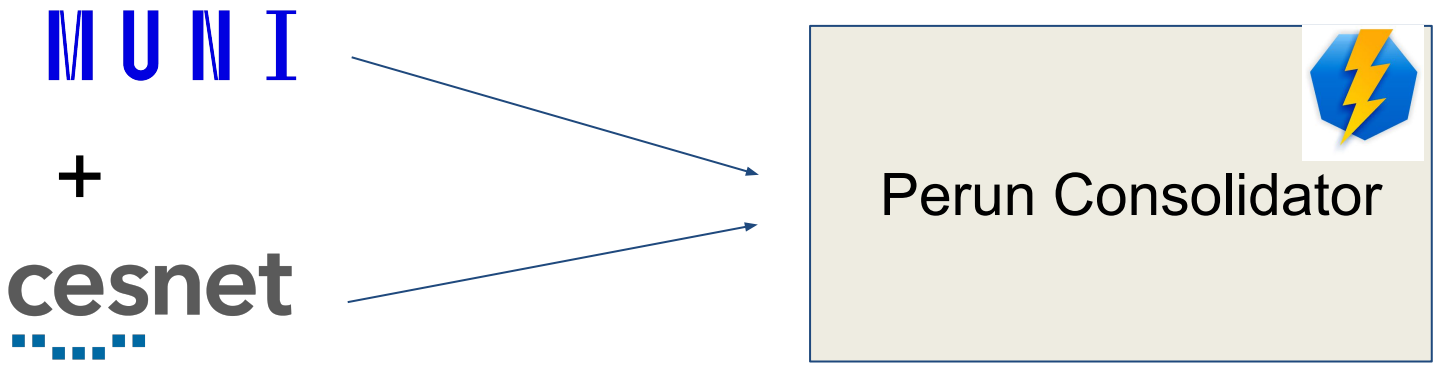
Vznik účtu v Perun AAI

- účty uživatelů v Perun AAI vznikají podáním přihlášky do nějaké virtuální organizace v komponentě zvané **Perun Registrar**
- uživatel musí nejprve prokázat svoji identitu přihlášením ve své domovské organizaci přes federaci identit **eduId.cz** (operátorem federace je CESNET) nebo **eduGAIN** (EDUcation Global Authentication INfrastructure)
- pokud jeho domovská organizace neprovozuje službu Identity Provider, lze využít přihlášení přes **Google, Facebook, Apple, ORCID, Microsoft, LinkedIn, GitHub**, které ale nezaručují skutečnou identitu uživatele



Spojování více identit do jedné

- někteří uživatelé mají více domovských organizací, např. MUNI a CESNET
- existují i alternativní způsoby přihlášení pomocí X509 certifikátů nebo jména a hesla
- více způsobů přihlášení lze spojit do jednoho uživatelského účtu v komponentě **Perun Consolidator**
- Perun eviduje kdy byl který způsob přihlášení naposledy použit a jaké atributy uživatele při tom byly získány



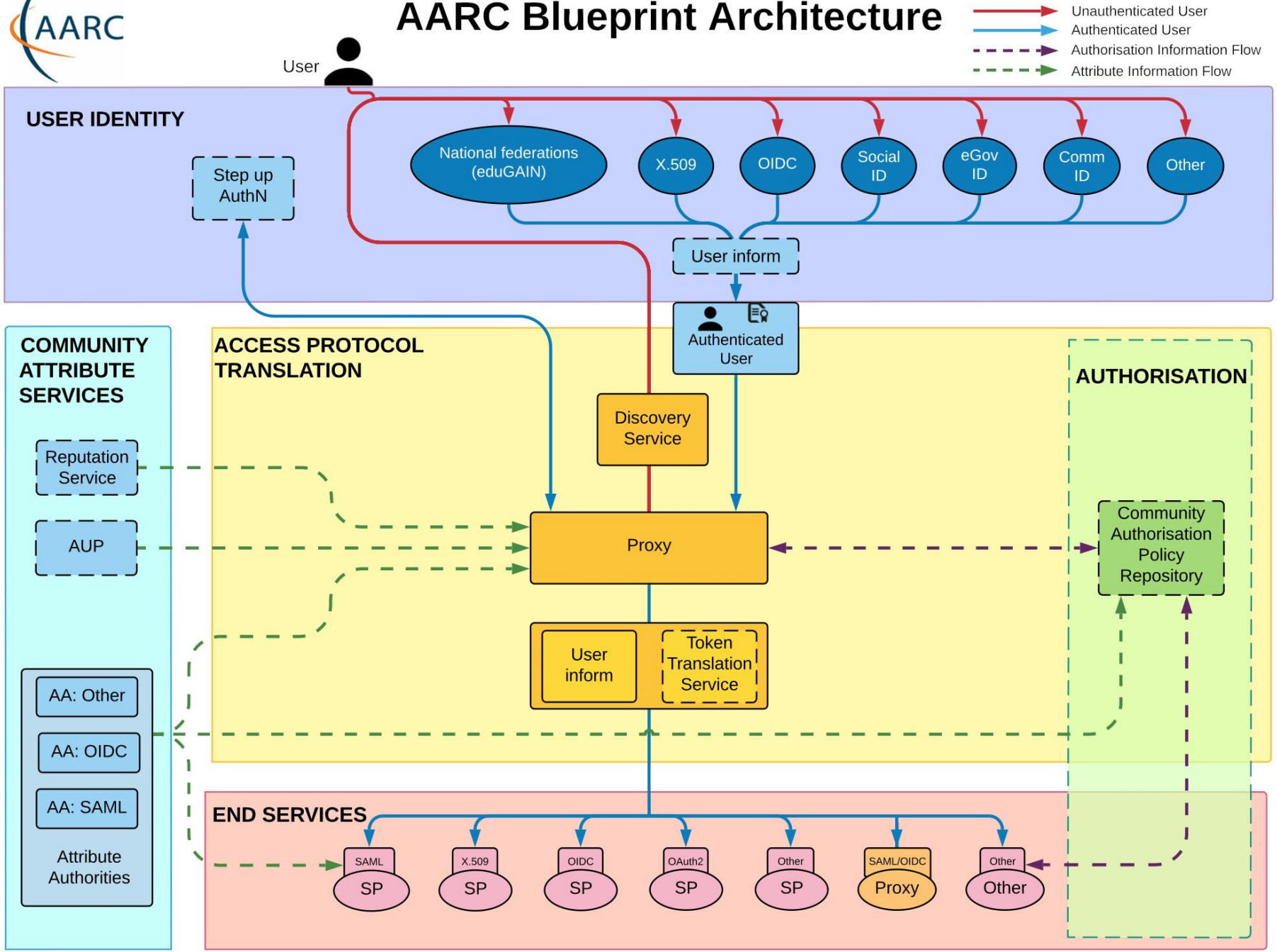
Proxy Identity Provider

- služba Identity Provider (IdP) z domovské organizace obvykle neposkytuje všechny potřebné atributy uživatele
- některé ani z principu nemůže, např. členství ve skupině tvořené uživateli z více organizací
- proto komponenta **Perun Proxy IdP** doplňuje chybějící atributy
- Proxy IdP vystupuje jako Service Provider (SP) vůči IdP domovské organizace a jako IdP vůči službám připojeným k AAI (Autentizační a Autorizační Infrastruktuře)
- kromě **autentizace** (ověření totožnosti) může Proxy IdP provádět i **autorizaci** (rozhodnutí o přístupu)
- Perun Proxy IdP podporuje protokoly **SAML a OIDC** (Security Assertion Markup Language a OpenID Connect)
- Perun Proxy IdP implementuje specifikace **GA4GH Passport** (Global Alliance for Genomics and Health) a **GA4GH AAI OpenID Connect Profile**

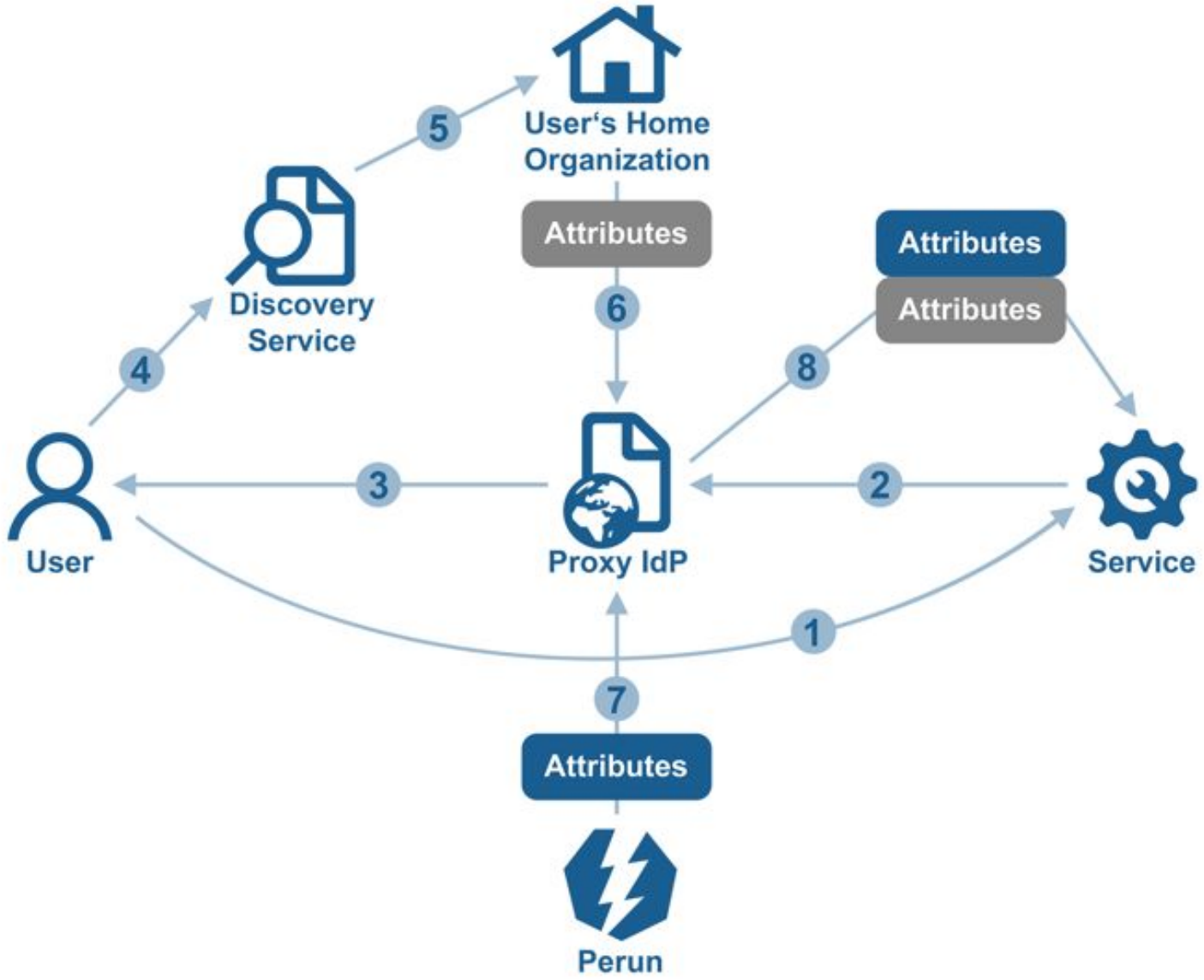
Evidence atributů a skupin uživatele

- účty zaregistrovaných uživatelů jsou evidovány v komponentě **Perun Identity Management**
- účty jsou organizovány po tzv. virtuálních organizacích (VO)
- jeden uživatel může být **členem** více VO
- člen VO může mít libovolné množství atributů (např. email, doba členství, …)
- některé atributy uživatele jsou nezávislé na VO (např. jméno, preferovaný email)
- v rámci VO existují **skupiny** uživatelů
- skupiny tvoří hierarchii, členové skupin v nich mohou být přímo nebo nepřímo přes podskupinu
- skupiny a atributy mohou být používány pro **autorizaci přístupu** k výpočetním prostředkům (např. jen členové skupiny employees mohou do vnitřní wiki)
- Perun IdM a Perun Proxy IdP dohromady tvoří AAI podle **AARC Blueprint Architecture** (Authentication and Authorisation for Research and Collaboration) https://aarc-project.eu/architecture/
- federace zajišťuje User Identity, Proxy IdP zajišťuje Access Protocol Translation, Perun IdM zajišťuje Community Attribute Services a Authorisation

AARC Blueprint Architecture



Architektura Perun AAI



Perun Identity Management

- u služeb s webovým uživatelským rozhraním lze provádět autorizaci přístupu v okamžiku přihlášení uživatele na Proxy IdP
- u služeb bez webového rozhraní je potřeba dodávat aktuální autorizační informace na službu (tzv. provisioning a deprovisioning)
- např. na výpočetních strojích MetaCentra musí existovat soubory /etc/passwd a /etc/group obsahující aktuální uživatele a jejich skupiny
- tyto soubory vytváří a udržuje komponenta **Perun Engine**
- existují desítky hotových tzv. služeb generujících konfigurační soubory a/nebo provádějící nastavení konkrétního software
- nastavení probíhá obvykle přes protokol ssh, nebo zasláním souboru nějakým jiným komunikačním protokolem (HTTP, SMB, LDAP, …)
- v opačném směru může Perun Identity Management synchronizovat údaje o uživatelích z jiných systémů, např. personálního

Životní cyklus uživatele

- uživatelský účet v Perun AAI vzniká akceptováním podané přihlášky (automaticky nebo ručním schválením)
- přihlášky mohou být do VO nebo do konkrétních skupin
- po vzniku nastavena expirace členství ve VO podle pravidel dané VO (např. po jednom roce od vzniku, na konci určitého kalendářního měsíce, atp.)
- členství ve VO je možné prodlužovat podáním tvz. žádosti o prodloužení
- žádost o prodloužení je konfigurovatelný formulář podobně jako prvotní přihláška
- výzvy k prodloužení členství ve VO jsou rozesílány podle pravidel dané VO
- pro prodloužení je potřeba přihlášení přes domovskou organizaci
- bez prodloužení po datu expirace členství ve VO zaniká

Uživatelské rozhraní Perun AAI

- pro správce https://perun.e-infra.cz/
  - správa VO
  - správa skupin
  - správa facilities a resources (spravované výpočetní prostředky)
- pro samosprávu uživatelského účtu https://profile.e-infra.cz/
  - preferovaný jazyk, časová zóna
  - spojené identity
  - hesla, ssh klíče
  - preferovaný shell, diskové kvóty, …

Evidence publikací

- pro potřeby MetaCentra Perun obsahuje komponentu pro **evidenci publikací**
- MetaCentrum dává uživatelům s více publikacemi přednost při spouštění úloh (zvyšuje jim tzv. fairshare)
- nově implementované webové rozhraní na https://publications.e-infra.cz/

Nasazení Perun AAI

- e-infrastruktura CESNET
- e-INFRA CZ
- LifeScience RI + ELIXIR
- biobanking infrastruktura BBMRI (bude migrováno do Lifescience RI)
- ERASMUS / MyAcademicID
- MyAccessID - FENIX, PUHURI, LUMI
- UmbrellaId - European Large Neutron and Photon Facilities
- GÉANT
- GÉANT eduTEAMS
- nizozemský SURF Research Access Management
- CEITEC
- bez Perun Registrar a Proxy IdP - MUNI a VŠUP

Shrnutí komponent systému Perun AAI

- Perun Registrar - přihlášky a žádosti o prodloužení
- Perun Consolidator - spojování více identit do jednoho účtu
- Perun Identity Management - synchronizace, správa účtů a atributů
- Perun Engine - provisioning, deprovisioning
- Perun Proxy IdP - autentizace, autorizace, poskytování atributů
- UI
  - administrativní
  - profil uživatele
  - evidence publikací

Děkuji za pozornost

Napište nám na perun@cesnet.cz nebo navštivte https://perun-aai.org