Kutatási infrastruktúrák közötti átjárhatóság támogatása azonosítás és jogosultságkezelés segítségével

Mohácsi János, GÉANT igazgatósági tag
Azonosítási és jogosultsági szolgáltatás felelős, Pro-M

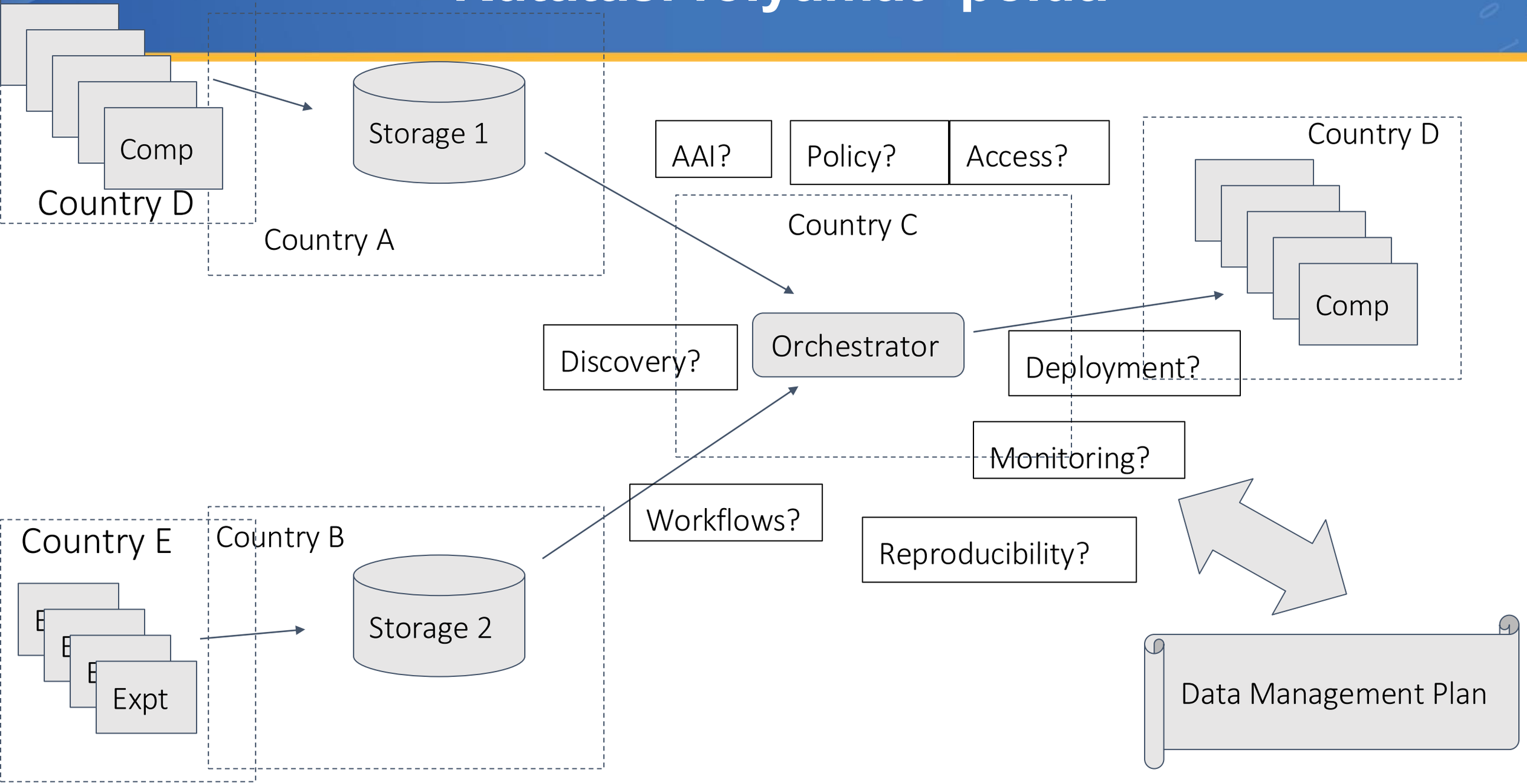
HUN-REN ARP 2025 konferencia
2025 október 8

Tartalom

- Bevezetés
- AARC Blueprint architektúra
- AARC Blueprint architektúra továbbfejlesztése
  - Esettanulmányok
  - Válaszok
- Összefoglalás

Egy föderatív világban élünk! A kutatók határokon átívelő együttműködése

Kutatási folyamat -példa



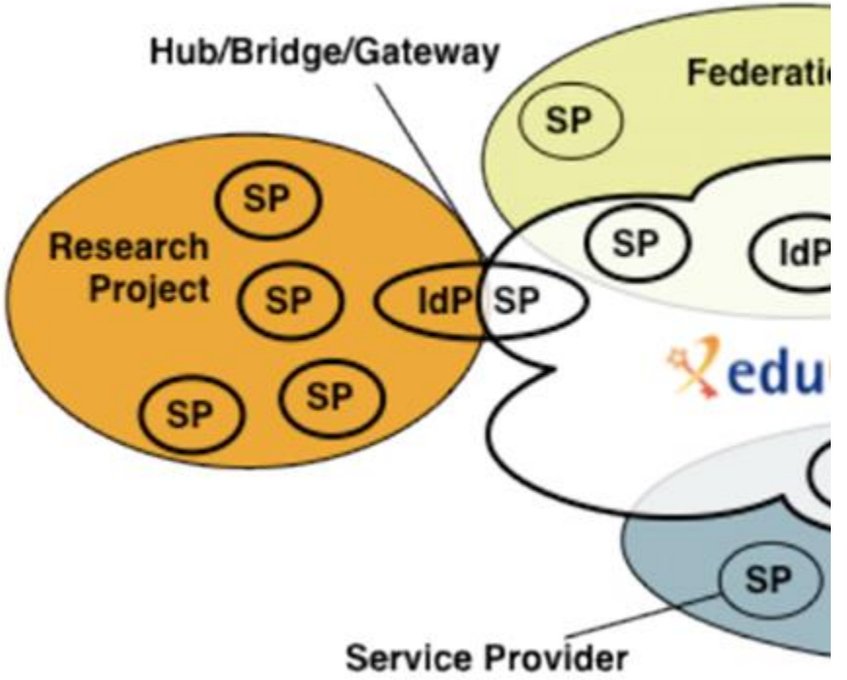
Mi az AARC BPA?

Az Authentication and Authorization For Research and Collaborations BluePrint Architecture építőelemeket tartalmaz a nemzetközi kutatási együttműködések hozzáférés-kezelési megoldásokat tervező és megvalósító szoftveresek és műszaki döntéshozók számára. Az AARC BPA technológia-független és architektúrát biztosít a AAI-t alkalmazók számára.

A tudományos klaszterek, kutatási infrastruktúrák és e-infrastruktúra-szolgáltatók az AARC Blueprint architektúrát használva implementálják az AAI rendszereket, amelyekben felhasználók és az erőforrásokhoz való hozzáférési jogokat kezelik.

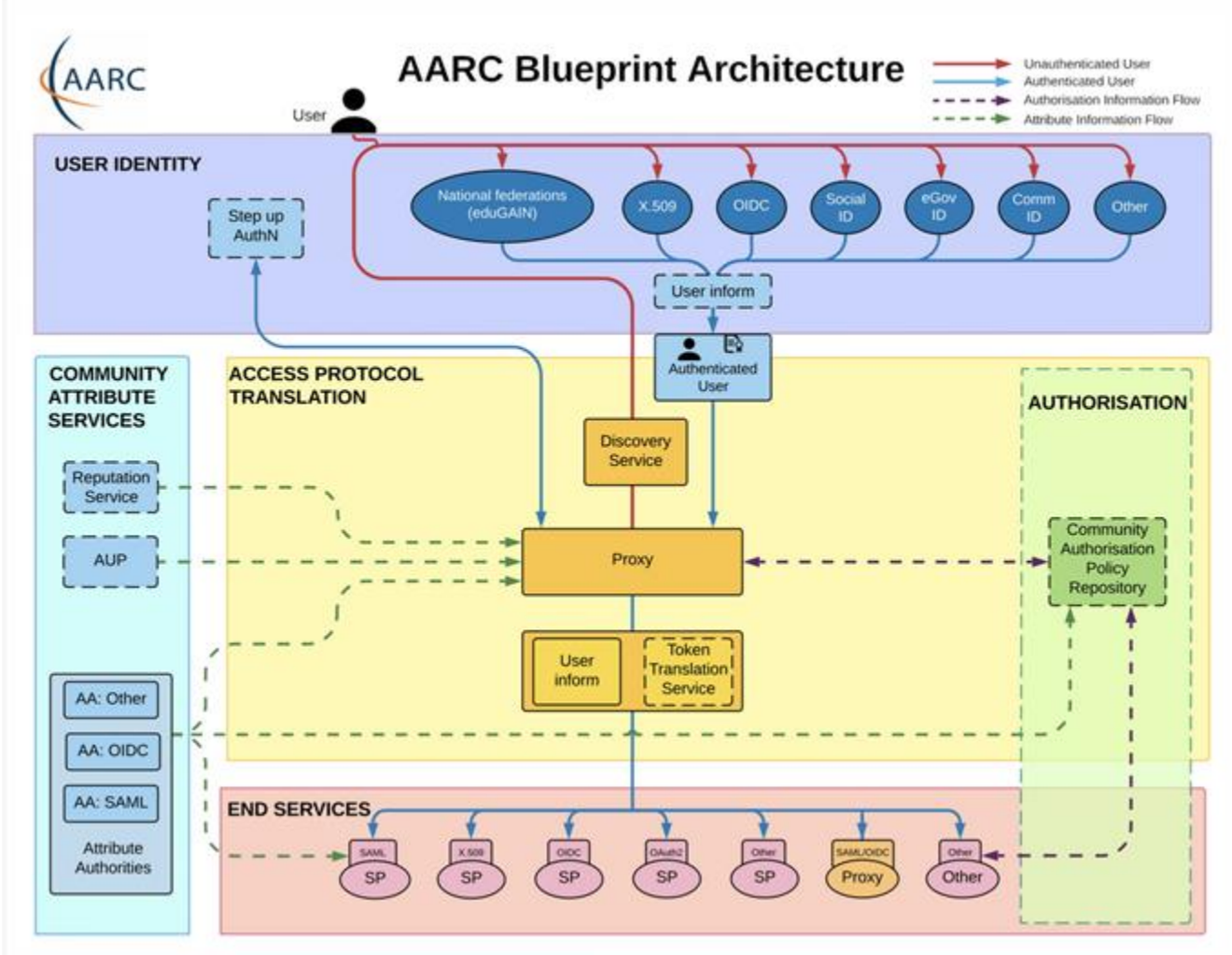
AARC BPA az eScience föderált hozzáférés kezelése érdekében

- A szolgáltatásokhoz való hozzáférés a **felhasználók saját szervezeteinek azonosítóit** használva, de **elrejtve** a több IdP, szövetség, AA technológiák **összetettségét**.
- Egy **állandó identitás** a közösség összes szolgáltatásában **a fiókok összekapcsolása** révén.
- A szolgáltatásokhoz való **hozzáférés** a felhasználóknak az **együttműködésben** betöltött **szerepe(i) alapján** .
- **webes** és **nem webes** erőforrásokra egyaránt
- A **vendégidentitási megoldások** integrálása
- Támogatás az **erősebb hitelesítésbiztosítási** mechanizmusokhoz



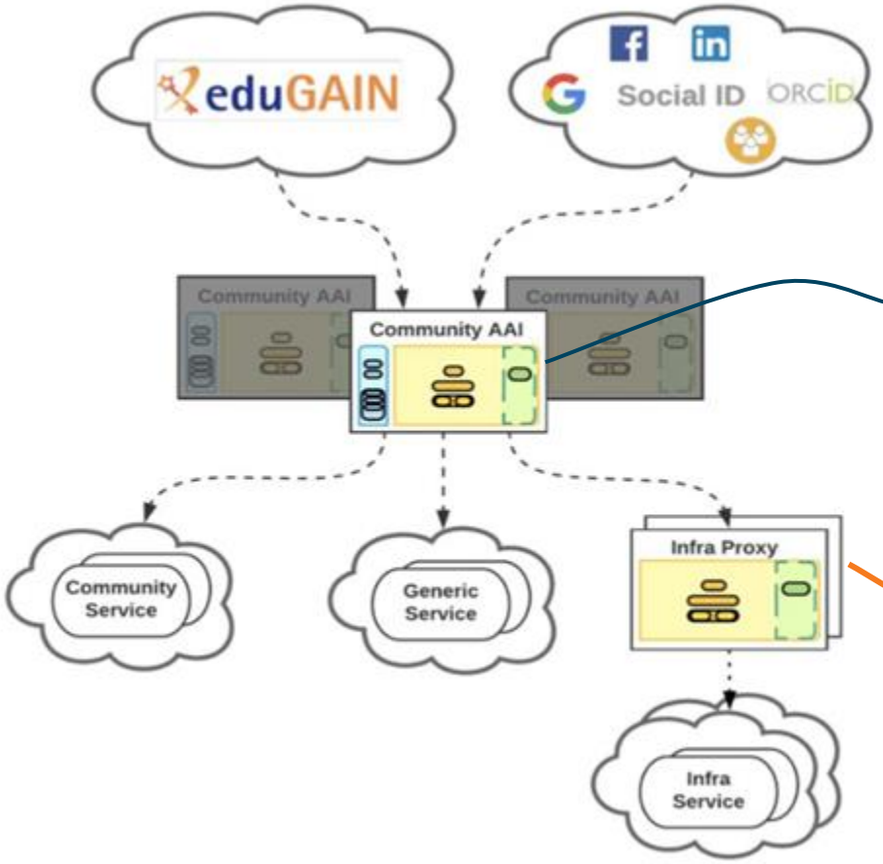
Authentication and Authorization for Research Collaboration – https://aarc-community.org/

Interoperabilitás - a színek



https://aarc-community.org/guidelines/

A közösségi AAI és az infrastruktúra-proxy - strukturáló elemek



Community AAI (Közösségi AAI)

A közösségi AAI célja, hogy egyszerűsítse a kutatók hozzáférését a szolgáltatásokhoz, mind a saját infrastruktúrájuk által nyújtott szolgáltatásokhoz, mind a más közösségekkel megosztott infrastruktúrák által nyújtott szolgáltatásokhoz.

Infrastructure Proxy (infrastruktúra-proxy)

Az infrastruktúra proxy lehetővé teszi a nagyszámú erőforrással rendelkező infrastruktúrák számára, hogy azokat **egyetlen integrációs ponton** keresztül biztosítsák, ahol az infrastruktúra központilag karbantarthatja az összes **vonatkozó szabályzatot és üzleti logikát**, hogy ezeket az erőforrásokat **több közösség számára is elérhetővé tegye**.

AARC Technical Revision to Enhance Effectiveness

AARC TREE Project dióhéjban

Kezdés: March 2024
Időtartam: 24 M
22 Partner (Köztük KIFÜ/Pro-M)
2,5 M Euro

Az AARC3 globális tevékenység
- **Minden** érdekelt bevonása

Megkérdezett infrasrtruktúrák és visszajelzések

Research Infrastructure	Type
SURF/SRAM	National e-Infrastructure
EUDAT	Research Infrastructure
HIFIS	National e-Infrastructure
EISCAT	Research Infrastructure
CINECA	National HPC
FENIX	HPC
SeaDataNet	Research Infrastructure
NFDI	National e-Infrastructure
Juelich	National HPC
CERN (WLCG)	e-Infrastructure
Elixir	Research Infrastructure
Photonic and Neutron	National e-Infrastructure

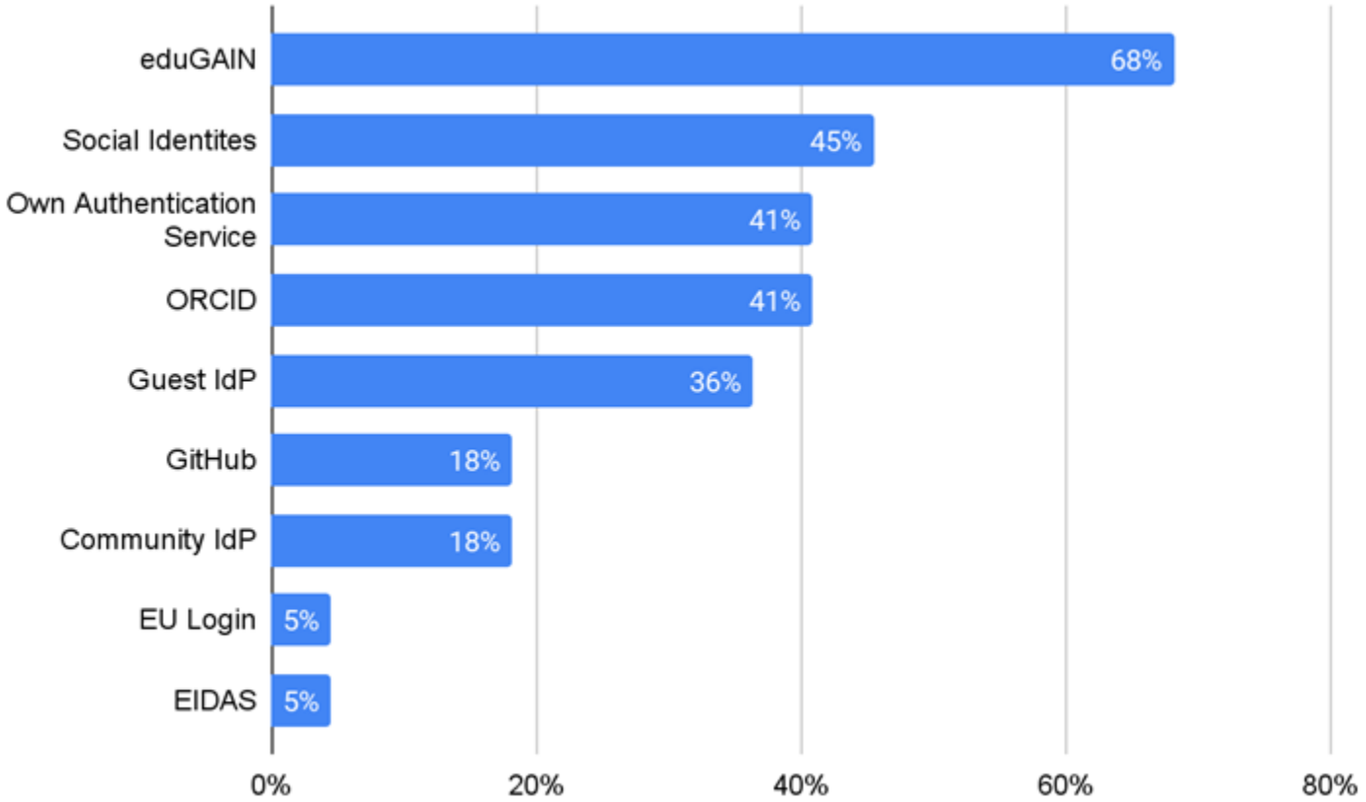
Research Infrastructure	Type
ELI	Research Infrastructure
EGI	E-infrastructure
SKA	Research Infrastructure
GÉANT	E-infrastructure
ESCAPE	Research Infrastructure
Komondor HPC	National HPC
Instruct ERIC	Research Infrastructure
Puhuri/LUMI	HPC
Arts and Humanities/Dariah	Research Infrastructure
DAFNI (STFC)	Research Infrastructure
NIKHEF	Research Infrastructure

- Architektúra, Policy és Validációs AARC TREE munkacsoport
- AEGIS
- EOSC AAI munkacsoport

23 Interviewed infrastructures

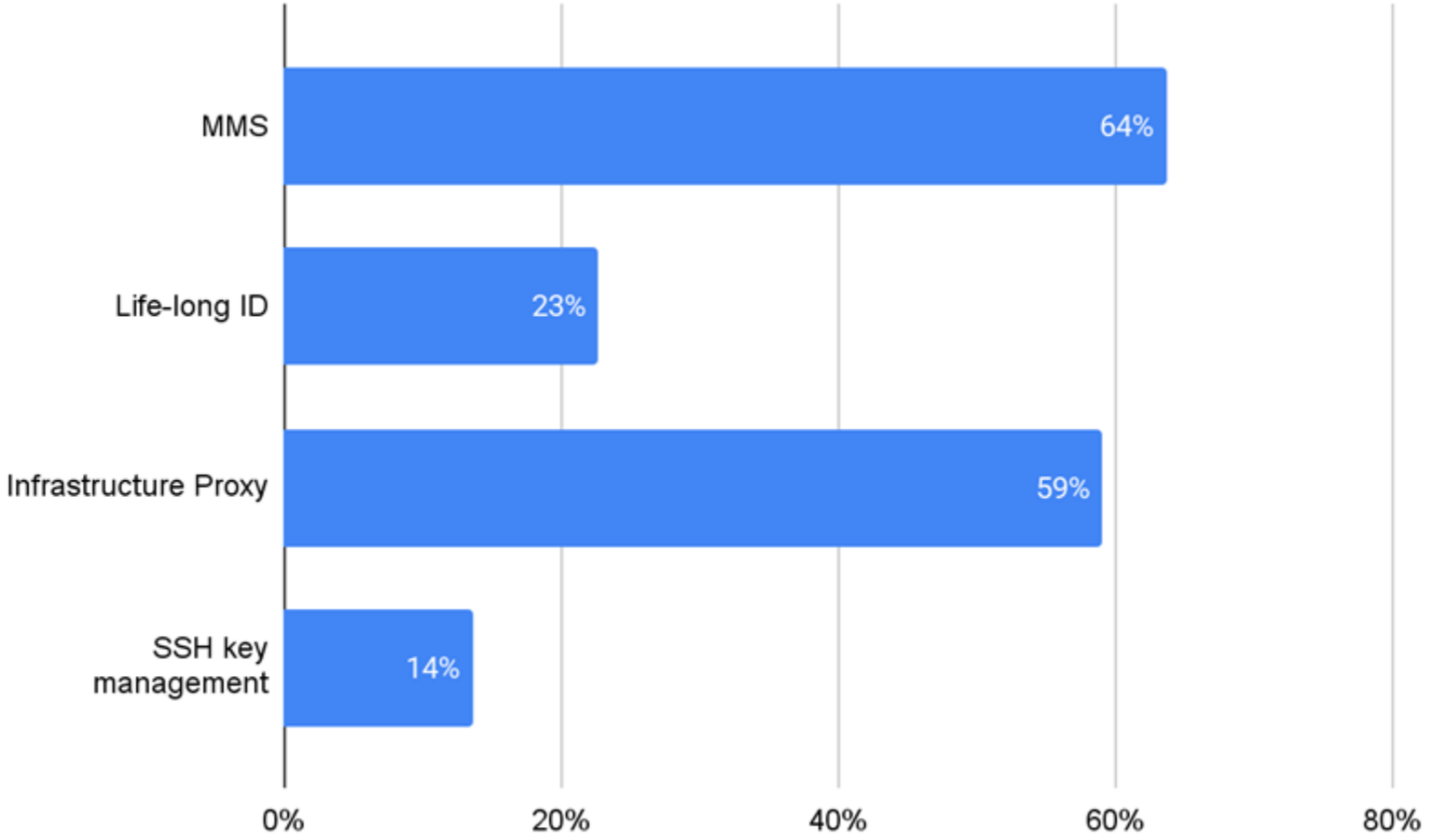
AARC TREE felmérés – alkalmazott AAI források

- A legtöbb infrastruktúra elsődleges hitelesítési forrásként az **eduGAIN**-en keresztül elérhető akadémiai szövetségi azonosításokat használja
- Sok esetben támogatják a **nem akadémiai azonosítókat** is (például Google, Facebook, GitHub, Microsoft) és a **vendégazonosító szolgáltatókat**.
- Az **ORCID** a kutatók körében széles körben elterjedt hitelesítési megoldás – de nem elég,
- egyes infrastruktúrák – történeti okokból, zárt felhasználói közösségek miatt, vagy a helyi azonosítási folyamatokba vetett nagyobb bizalom okán – **saját identitáskezelési rendszereik**re is támaszkodnak.
- A **MyAccessID** szolgáltatáson keresztül elérhető az **EU Login** és az **eIDAS** alapú hitelesítés is, lehetőséget biztosítva azon infrastruktúrák számára, amelyek az **Európai Bizottság által támogatott azonosítási megoldásokat** kívánják alkalmazni.

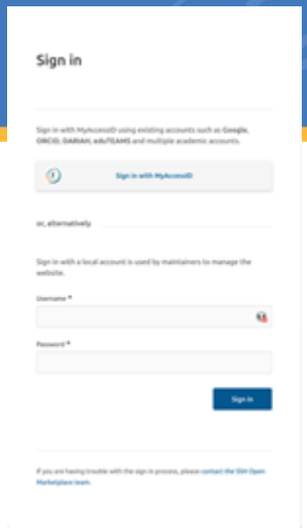


AARC TREE –speciális AAI-funkciók

- Számos infrastruktúra **infrastruktúra-proxyt** működtet a **AARC BPA-nak megfelelő** architektúra részeként, míg egyes – az ellenőrzés és irányítás megtartása érdekében – akkor is saját proxy fenntartását választják ha **e-infrastruktúra szolgáltatások** vesznek igénybe.
- A **tagságkezelő szolgáltatások (Membership Management Services, MMS)** széles körben alkalmazottak az **authorizációhoz kapcsolódó információk kezelésé**
- Egyes infrastruktúrák **élethosszig tartó identitásmegoldásokat** valósítanak meg annak érdekében hogy a felhasználók a foglalkoztat viszonyuk megváltozása ellenére i hozzáférjenek a szolgáltatásokhoz
- Több infrastruktúra **speciális SSH-kulcskezelő megoldásokat** haszná mivel szolgáltatásaikhoz elsősorba **parancssoros felületen keresztül** férnek hozzá.



Néhány konkrét esettanulmány



1. SSH Open Marketplace AAI Switchover (2024) – régi rendszer nem támogatott

- Kulcs követelmények:
  - social logins támogatása (Google, ORCID, etc.) tartalékként
  - Felhasználói fiókok migrációja (Előző hozzáférések megőrzése) → fiókok egyesítése
- Megoldás: MyAccessID (GEANT)

2. **EISCAT Data Portal**

- Rendkívül nagy adatmennyiség(100 Tb/s 60 000 vevőtől) – redukció (néhány PB/év).
- Megbízható hozzáférés és megosztás biztosítása a kutatók számára portálon és API-kon keresztül
- Hitelesítés és jogosultságkezelés: Biztonságos felhasználókezelés - metaadatok nyílt böngészése, adatokhoz és feldolgozásokhoz való hozzáférés korlátozás a tagság és intézményalapján.

3. **Élettudományok (Life Science - EOSC ENTRUST)**

- Érzékeny adatok (pl. egészségügyi adatok) nemzeti hatóságok ellenőrzése alatt állnak → szigorú követelmények az azonosság hitelesítésére.
- Az eIDAS használata nehézségekbe ütközik a nemzeti jogszabályok miatt → a MyAccessID megoldást kínálhat erre. - Mi a helyzet a nem EU-s kutatókkal vagy kereskedelmi partnerekkel?
- Az elemzéseket megbízható kutatási környezetekben (Trusted Research Environments, TRE) kell futtatni → szigorú hozzáférés-ellenőrzés
- Nem „hagyományos” föderált hitelesítés vagy jogosultságkezelés, ugyanakkor szükség van szövetségi identitásra a felhasználók és projektek számára.
- A felhasználónak előzetesen engedélyezettnek kell lennie az összes érintett TRE-ben, hogy az elemzés minden környezetben lefuthasson anélkül, hogy manuálisan kellene regisztrálni, hozzáférést kérni és elindítani az elemzést külön-külön.

AARC TREE felmérés - interjúk során azonosított további probléma területek

Technikai:

- Csoportokhoz kapcsolódó információk cseréje a szolgáltatások között
- Interoperabilitás – távoli token-ellenőrzés (remote token introspection)
- OpenID-föderáció
- Nem webalapú hozzáférés
- Föderált SSH-hozzáférés
- Összetettebb csoportmodell
- Élethosszig tartó felhasználói azonosítók
- Felhasználók törlése (deprovisioning) a GDPR-előírásoknak megfelelően
- eID alapú bejelentkezés
- Proxyhalmozás elkerülése felhasználói élmény szempontjából
- Fejlettebb jogosultságkezelés

Legjobb gyakorlatok és oktatás:

- Útmutatókra és szabályzatokra vonatkozó workshop
- Identity linking
- Útmutatók és szabályzatok technikai, üzleti szereplők számára - érthető formába
- Mi az EOSC AAI? – Interoperabilitás az EOSC-szolgáltatásokkal
- Felhasználói élmény (UX) proxyhalmozás esetén
- Többlépcsős hitelesítés (MFA)
- Biztonsági szint (Level of Assurance, LoA)
- Attribútumkiadás (attribute release)
- Vendégazonosító-szolgáltatók és ipari felhasználók támogatása
- Csoportkezelés (Group Management)
- Legjobb gyakorlatok a felhasználói szerepkörök kezelésében

Helyzetkép:

- Tesztelt és használt szoftverek

AARC BPA fejlesztése az OIDC támogatásához

SAML -> OIDC

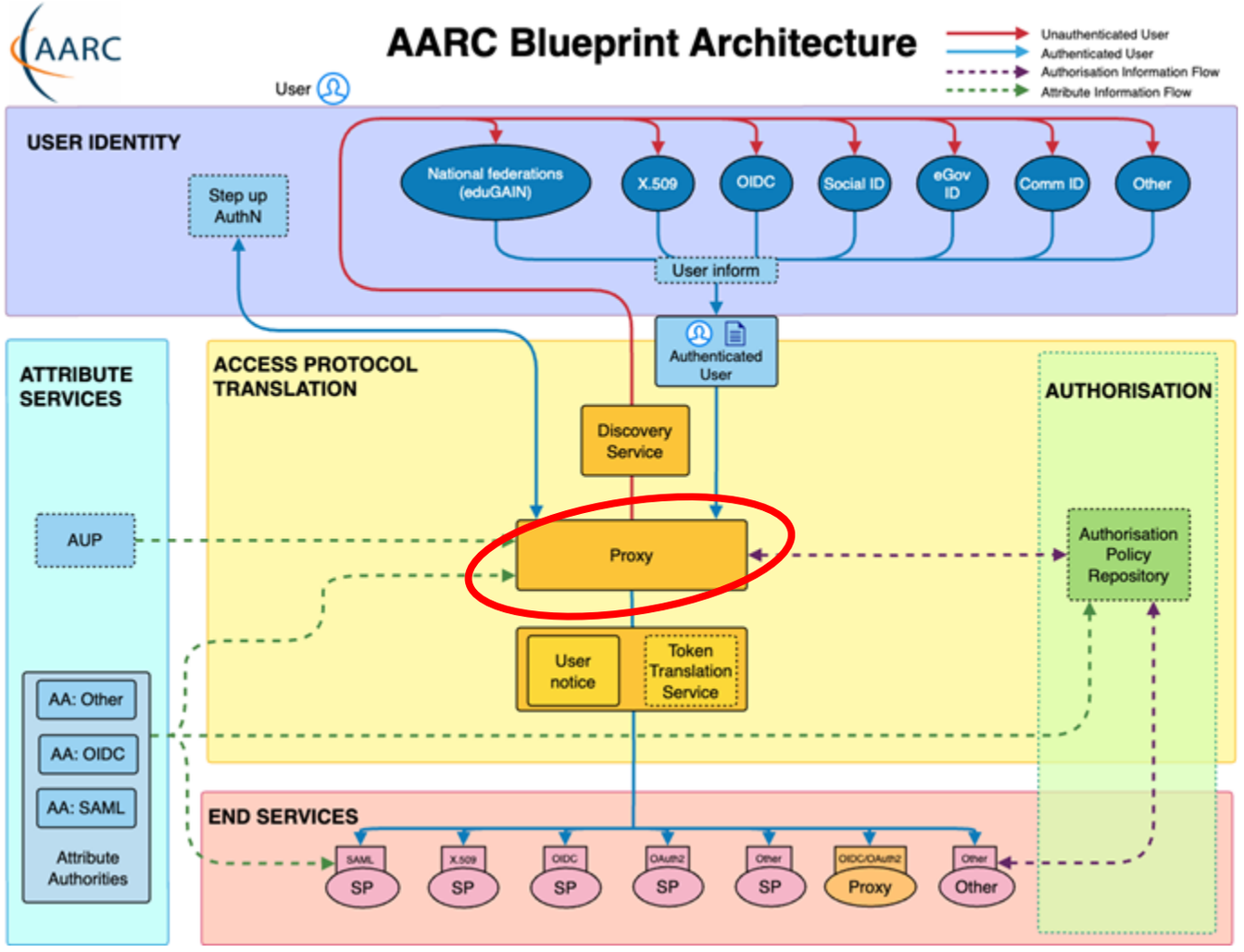
- eduGAIN ma: 83 nemzeti föderáció, mintegy 10 000 azonosításszolgáltató és szolgáltatás
- A föderáció SAML 2.0-ra és XML metaadat-aggregációra épül
- Azonban… a SAML-t a modern weben már régies technológiának számít
- A legtöbb szolgáltatás ma már az OpenID Connect-et részesíti előnyben

Miért OIDC?

Az OIDC támogatja a modern igényeket:

- Egyszeri bejelentkezés (Single Sign-On, SSO) webes és mobilalkalmazásokhoz
- API-hozzáférés tokenekkel (hozzáférési és frissítési tokenek)
- Gép–gép közötti munkafolyamatok (ügyfélhitelesítési adatok, azaz client credentials)
- JSON webtokenek (JWT) a biztonságos állításokhoz (claim)

AARC BPA evolúciója az OIDC támogatáshoz

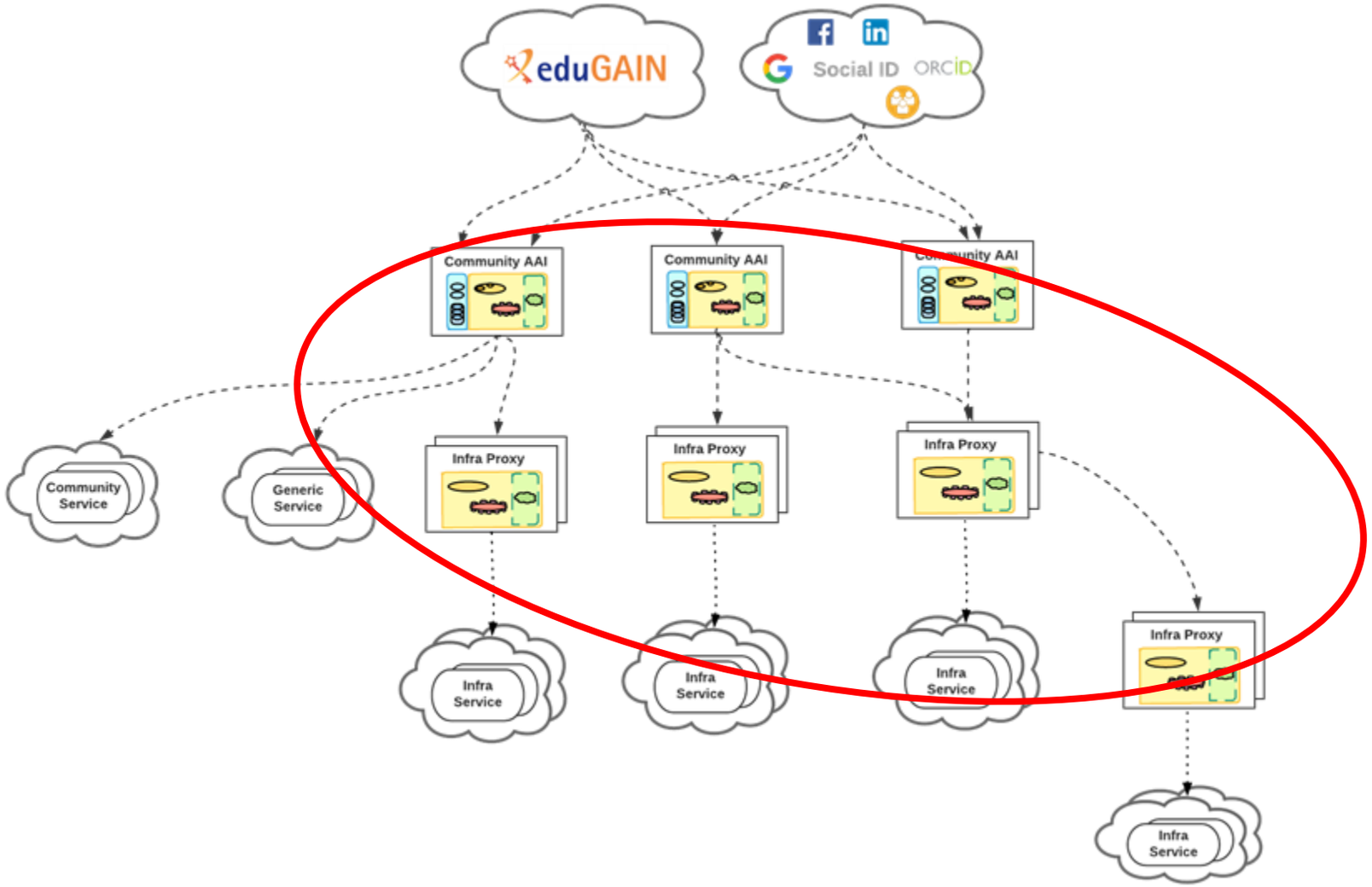


"All computer problems can be solved with a proxy"

- Anonymous IT Guru

AARC BPA evolúciója az OIDC támogatáshoz

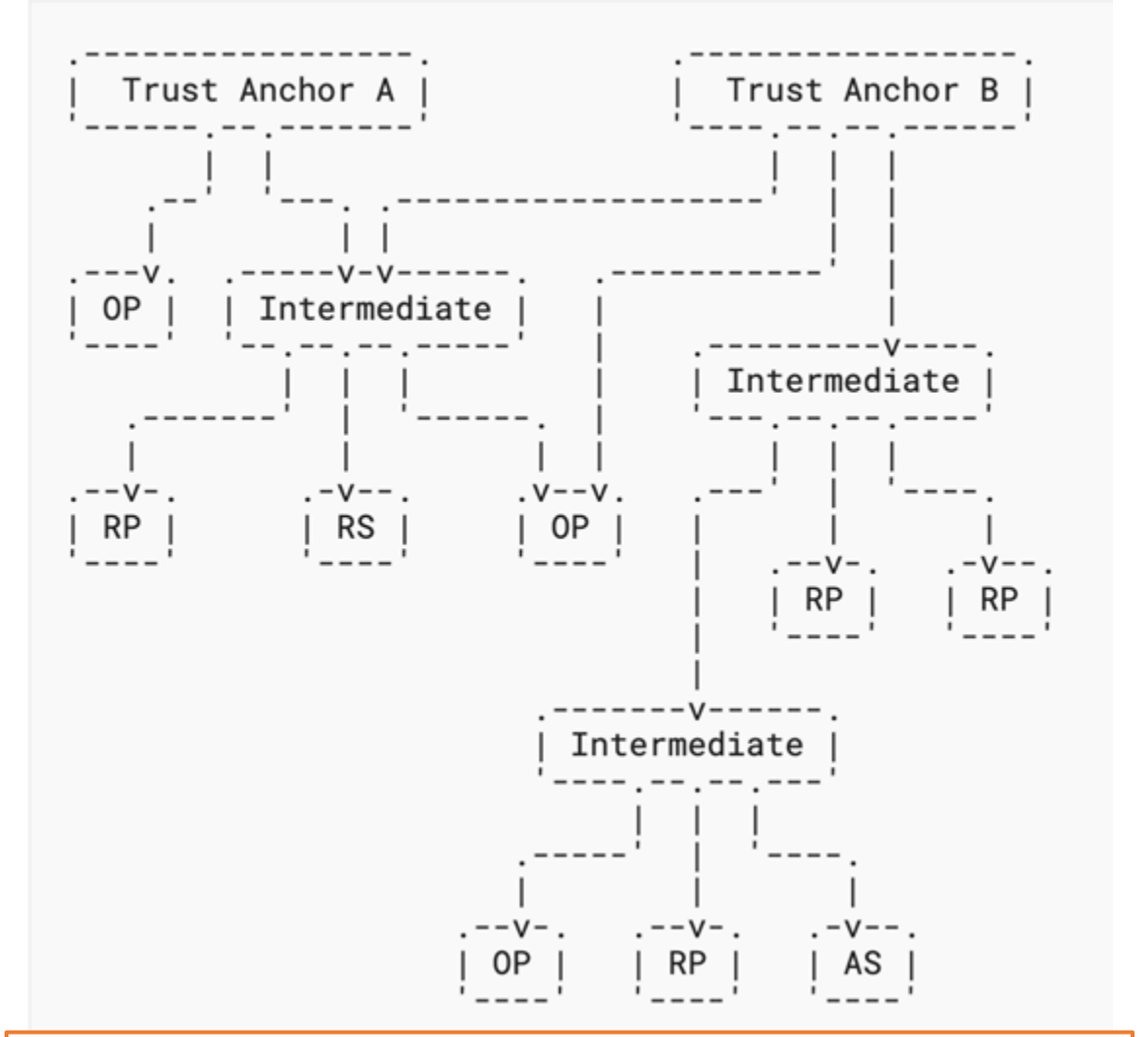
Mi történik, ha több proxy-hoz szükséges kapcsolódni?



AARC BPA evolúciója az OIDC támogatáshoz

OpenID Federation (OID-Fed) a megoldás

- Kiérlelt specifikáció (draft) – A specifikáció a 43-as revíziót érte el, és stabilnak tekinthető
- A kutatási és oktatási közösség által elfogadott – A kutatási és oktatási (R&E) föderációk jövőbeli bizalmi keretrendszereként tekintenek rá
  - Javaslat, hogy legyen R&E Wallet ökoszisztéma bizalmi alapja
- A bizalom skálázhatóságára tervezve – Támogatja a dinamikus bizalmi kapcsolatokat, a skálázhatóságot és az interoperabilitást a hagyományos föderációs modelleken túl



https://openid.net/specs/openid-federation-1_0.html

AARC BPA evolúciója az OIDC támogatáshoz

Ugyanazt a nyelvet beszéljük

- Harmonizált identitás-attribútumkészlet
- Biztosítja, hogy az azonosítók, tagságok, csoportok és bizalmi szintek egységesen legyenek értelmezve
- Közös szókészlet az OIDC tokenek interoperábilis használatához

AARC-G056

+

Tokenek ellenőrzése a Proxy-k között

- Szabványos módszer a proxyk számára a tokenek érvényességének ellenőrzésére
- Többproxy-s környezet támogatása
- Biztosítja, hogy a tokenek az eredeti kibocsátó tartományon túl is megbízhatók legyenek

AARC-G052

+

Bizalom Skálázása

- OpenID Federation keretrendszerre éül
- Támogatja az egyszerű és a részletes bizalmi modelleket egyaránt
- Lehetővé teszi, hogy a proxyk kétoldalú megállapodások nélkül is megbízzanak egymásban

AARC-G100

+

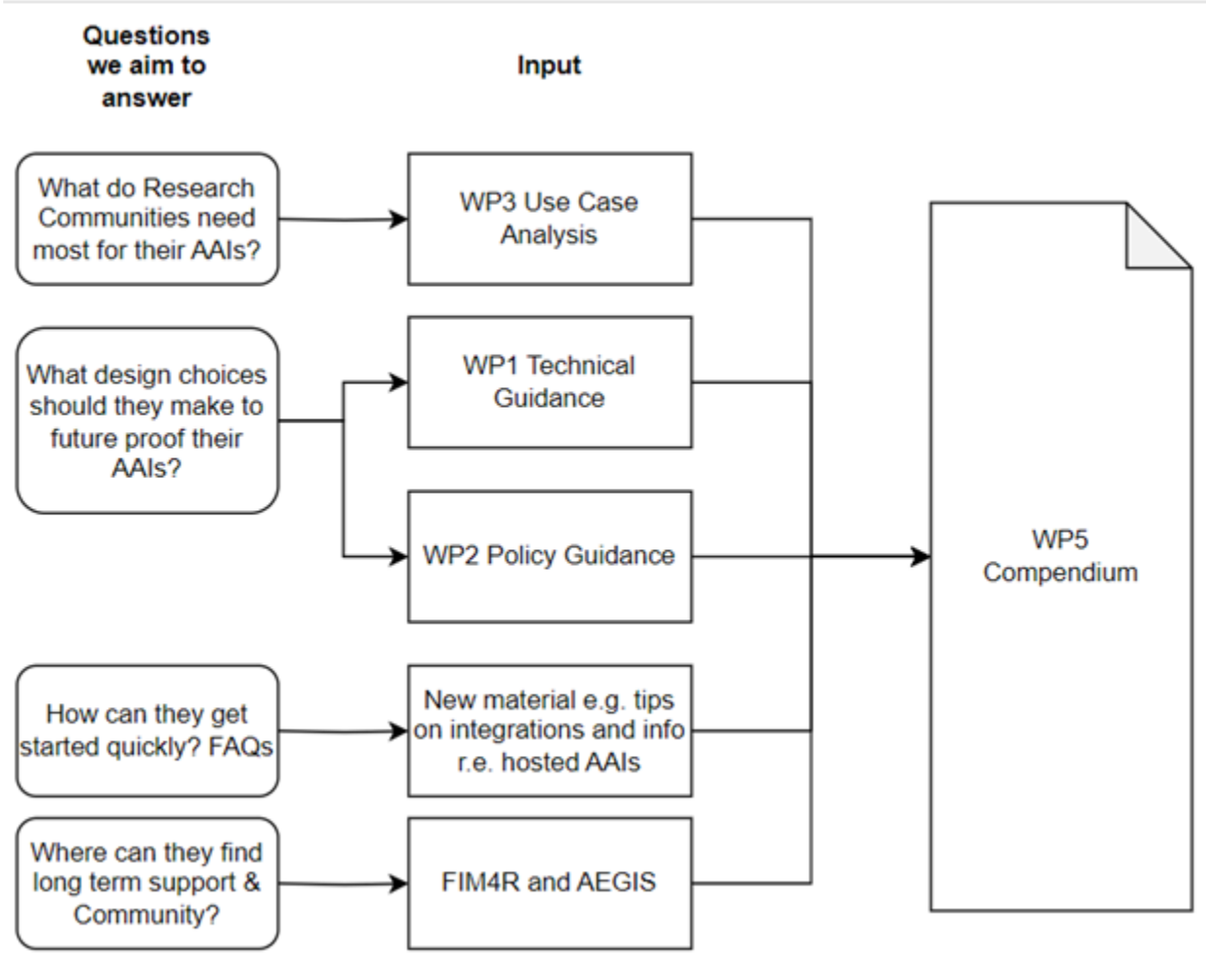
Tokenek élettartamnak harmonizálása

- Alap, min és max élettartamok (access and refresh token)
- Használhatóság (hosszabb munkamenetek, kevesebb bejelentkezés) és biztonság (a kockázatok korlátozása kompromittálódás) egyensúlya
- Biztosítja az infrastruktúrák közötti konzisztenciát a többproxy-s környezetekben

AARC-G081

AARC Compendium – AARC TREE 1. eredménye

- Web dokumentum (Wiki)
- Kutatói közösségek és technikai támogatóik megtalálhatják a szükséges útmutatást
- A szakzsargon használatának lehető legnagyobb mértékű kerülése
- Minél több gyakorlati segítség biztosítása, például döntési folyamatábra arról, hogy érdemes-e saját AAI-t üzemeltetni, vagy inkább hosztolt megoldást választani
- Válaszok a jelenlegi gyakori kérdésekre, például hogyan lehet integrálódni az EOSC-hoz, illetve mely iránymutatásokat érdemes követni a hosszú távú kompatibilitás maximalizálása érdekében
- Kiemelt figyelem a kisebb közösségek (10–100 fő) támogatására



AARC Közösség – nyitva áll mindenki számára

AARC Engagement Group for Infrastructures

The forum of e/r-Infras that operate an AARC BPA complaint AAI.
It's a closed group on purpose as we want to get feedback from the hands on group.
They approve the AARC guidelines.

Technical WG

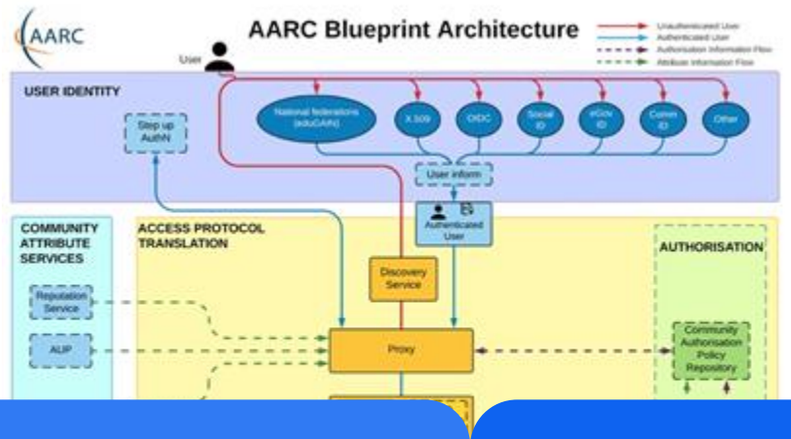
- Where technical guidelines are discussed
- Anybody can join the discussion: **https://lists.geant.org/sympa/info/aarc-architecture**

Policy WG

- Supported by EnCo and IGTF
- Anybody can join the discussion: **policy@aarc-community.org** https://lists.geant.org/sympa/info/aarc-na3

AARC Blueprint Architecture ‘BPA2025’!

AARC BPA 2019

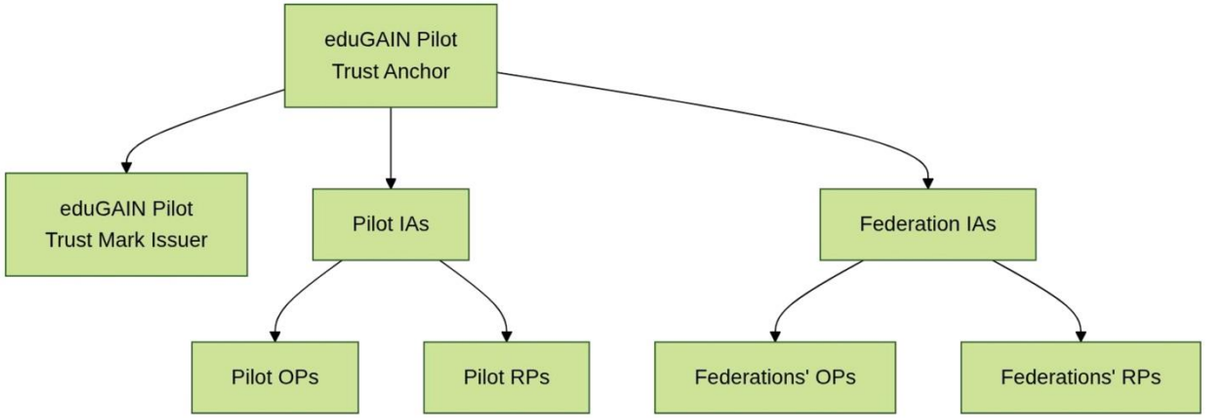


OpenID Federations + AuthZ for Federated Resources + Decentralised Identities & Wallets

AARC BPA 2025

AARC BPA Magyarországon

- Pro-M (Magyar NREN) részt vesz a AARC BPA továbbfejlesztésében és eduGAIN OpenID Federation Technological Profile definíciójában
- Pro-M (eduid.hu) bekapcsolódott a GÉANT (páneurópai kutatási infrastruktúra) tagjaként a OIDC-Fed pilotba
- GÉANT és Pro-M szolgáltatásai AARC BPA kompatibilisek és azon dolgozunk, hogy továbbiakban is az legyen
- Pro-M résztvevője a HUN-REN magyar EOSC Node kezdeményezésnek



Összefoglalás - Kérdések?

- Az AARC BPA szolgál referenciamodellként az azonosítási és jogosultságkezelési infrastruktúra (AAI) számára kutatási szolgáltatásokban, valamint ezen túl az Erasmus+ programban és az egyetemi szövetségek esetében is.
- GÉANT és Pro-M ezekkel kompatibilis azonosítási és jogosultságkezelési infrastruktúrát biztosít.

Mohácsi János
mohacsi.janos@pro-m.hu