cesnet

Správa identit, eduID a společné pracovní skupiny

Pavel Zlámal
zlamal@cesnet.cz

4.9. 2024
VUT Brno

Úvod

Identita

- Souhrn informací, které pomáhají osobu ztotožnit
- Typicky jedna

Digitální identita

- Ekvivalent skutečné identity v digitální prostředí
- Typicky více
- Potřeba správy (z pohledu služeb)

Řízení přístupu

- **Autentizace** – ověření identity / totožnosti subjektu
- **Autorizace** – schválení/zamítnutí přístupu nebo operace

eduID.cz

- Česká akademická federace identit eduID.cz
- Vysoké školy, ústavy AV ČR, knihovny, muzea
- Cílem je poskytnout členům rámec pro vzájemné využití identit uživatelů při řízení přístupu k webovým službám.
- Federace sdružuje poskytovatele identity (IdP) a poskytovatele služeb (SP).
- CESNET v roli operátora
    - Koordinuje dění
    - Vykonává federační politiku
    - Distribuuje metadata

Výhody

- Jedno uživatelské jméno a heslo pro přístup k více aplikacím
- Princip SSO
- správci aplikací neudržují autentizační data uživatelů, ani neprovádí autentizaci
- autentizace uživatele probíhá vždy v kontextu domovské organizace
- federační infrastruktura poskytuje snadný, standardní a bezpečný způsob výměny informací o uživatelích
- Automatické propojení do interfederace eduGAIN

Omezení

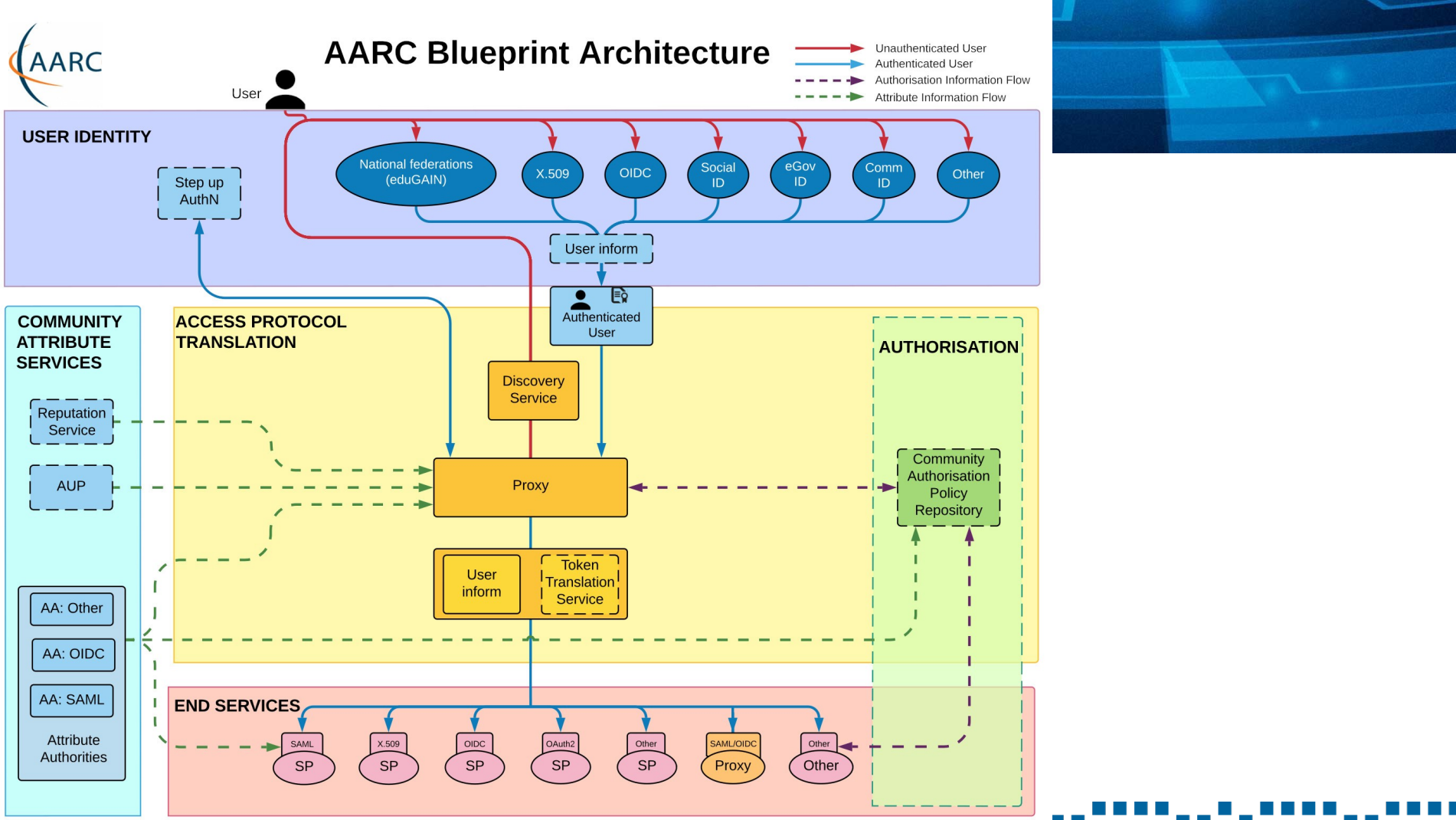
- Každá entita v principu jedná za sebe
  - Otázka vzájemné důvěry
  - Kategorie entit CoCo, Research & Scholarship
- Problém změn identifikátorů, přechod uživatele mezi organizacemi
- Provisioning pouze ve chvíli přístupu
- Neřeší problém skupin (přes více organizací / přes více služeb)

Autentizační a autorizační infrastruktura (AAI)

- Služba poskytující podporu uživatelům i ostatním službám
- Perun AAI – společný vývoj CESNET / Masarykova Univerzita
- Cílí na vědecko-výzkumné e-infrastruktury
- Postaveno podle AARC Blueprint Architecture

AAI podle AARC Blueprint Architecture

- Výzkumný projekt AARC (Authentication and Authorization for Research Communities) stanovil v roce 2015 vhodnou architekturu AAI
- Centrální místo s tzv. **Proxy IdP**
  - Vůči IdP vystupuje jako SP
  - Vůči SP vystupuje jako IdP
  - Poskytuje další služby jako
    - správa skupin uživatelů
    - správa dalších atributů uživatele (jiných než poskytovaných IdP)
    - volitelná multi-faktorová autentizace
    - volitelná autorizace před odesláním uživatele na SP
    - správa vyjádření souhlasu uživatele s různými politikami/pravidly (GDPR atp.)
    - překlad mezi protokoly, např. mezi SAML a OIDC


AARC Blueprint Architecture
Unauthenticated User
Authenticated User
Authorisation Information Flow
Attribute Information Flow
User
USER IDENTITY
Step up AuthN
National federations (eduGAIN)
X.509
OIDC
Social ID
eGov ID
Comm ID
Other
User inform
Authenticated User
COMMUNITY ATTRIBUTE SERVICES
ACCESS PROTOCOL TRANSLATION
AUTHORISATION
Discovery Service
Reputation Service
AUP
Proxy
Community Authorisation Policy Repository
User inform
Token Translation Service
AA: Other
AA: OIDC
AA: SAML
Attribute Authorities
END SERVICES
SAML SP
X.509 SP
OIDC SP
OAuth2 SP
Other SP
SAML/OIDC Proxy
Other Other

Výhody použití AAI

- Řeší problém kde evidovat skupiny uživatelů z různých organizací
  - Možnost registrace uživatele do skupiny
  - Expirace členství, žádosti o prodloužení
  - Přímý export skupiny do služeb
- Uživatelům poskytuje jednotný účet pro přístup ke všem službám
- Řízení přístupu ke všem službám
- Přehled o využití služeb, auditing

Perun AAI

Perun AAI je nasazena ve více instancích jako služba pro:

- e-infrastruktury CESNET a e-INFRA CZ
- LifeScience AAI - evropské biologické infrastruktury
  - ELIXIR - European life sciences infrastructure
  - BBMRI - Biobanking and BioMolecular Research Infrastructure
  - GDI - Genomics Data Infrastructure
- platformu MyAcademicID / Erasmus+
- MyAccessId - AAI pro evropská superpočítačová centra
- EGI - European Grid Infrastructure
- další e-infrastruktury SURF, UmbrellaID, FENIX, eduTEAMS

Shrnutí

- eduId.cz je základ
  - Poskytuje důvěryhodné identity
  - Poskytuje společný rámec/standard
- AAI
  - Poskytuje možnost spravovat skupiny uživatelů přes více služeb a organizací
  - Umožňuje spravovat více identit uživatele
  - Poskytuje další služby (MFA, další atributy do služeb)

cesnet

DĚKUJI ZA POZORNOST

DOTAZY?