AAI@EduHr – Croatian identity federation

26.05.2023, Dubravko.Penezic@srce.hr
AAI@EduHr

- Authentication and Authorisation Infrastructure of Science and higher education in Croatia
- hub-and-spoke architecture
- in production since March 1, 2006.
- web: https://www.aai.edu.hr
- e-mail: aai@srce.hr.
Statistic data

- 233 home institutions (hidden distributed identity providers)
- more than 920,000 e-identities
- service providers
  - 112 network access services (RADIUS)
  - 817 web applications (SSO)
- in the last 30 days:
  - 96M+ successful RADIUS authentications
  - 6M+ successful SSO authentications
Everything starts ...

• solving some issues in 2000.
  - directory services implementation
  - authentication of dial-in modem entries (Internet connectivity)

• solution
  - distributed architecture
  - LDAP for directory services and user database
  - RADIUS for dial-in modem authentication
We may use it also ...

• storing more information about the user and organization (hrEduOrg and hrEduPerson schema)
• eduroam (2003.)
  - early adopter
  - existing RADIUS infrastructure
• CAS (2003) for web base application (internally)
• recognize the need for SSO on the national level
So we start from ...

Dial-up access (CMU)
StuDOM
Wireless/wired access (Srce, CARNet, ...)
eduroam (http://www.eduroam.org)
UNIX/Linux PAM

(Lucent Navis) proxy radius server(s)
central LDAP server for backup

Radius server
LDAP server

Home org X  Home org Y  Home org Z

204 (167) Home orgs
= 180000 users
SW: FreeRadius & OpenLDAP

2004.
Adding mash connection ...

- on IdP AOSI WS (SOAP)
- on central servers FWS (federation WS) and HLS (home location service)
- on SP WS client for authentication and authorization
AOSI on IdP also ...

- add control of syntax and format of data
- ability to authenticate a local application
- synchronization with outer directories (AD, Azure)
- modular work-flow
Too many institutions and services ...

- Project of National AAI of Science and Higher Education (2005., Srce, MZOS, CARNET)
- AAI@EduHr Policy (2007.)
- definition of SP, IdP, and national infrastructure
- Actual version 1.3.1
- https://www.aaiedu.hr/sites/default/files/content_files/docs/AAI%40EduHr-pravilnik-ver1.3.1.pdf
IdP needs support ...

• Debian packages with all SW and configuration
• hosting IdP (small IdP)
• secondary IdP location (their own or hosted)
• A lot of presentations and P2P discussions
How we behave ...

- IdP audit (first 2011.)
- SP audit (first 2012.)
- enforce some security and organizational prerequisite
- show trends and future steps
- two parts (main and additional)
- partially automatic, partially manual
- additional bonus (NIAS)
SP needs help ...

• infrastructure Lab service
  - IdP
  - Central services

• documentation

• examples from the community, covering all major systems

• help in solving possible issues
SAML, eduGAIN

• support both from the early days
• introduce to society 2012.
• a lot of issues at beginning
• SimpleSamlPHP implementations
• benefit from eduGAIN
• work on GEANT projects
• retired our own central FWS solution
We need more ...

• monitoring services (SP and IdP), status maps
• representing usage statistic
• Virtual Organization
• authentication using social networks
• connecting to NIAS (2013.)
And more ...

- multiple instances of central IdP (solving issues and attributes translation)
  - NIAS
  - social networks and other Auth Authorities (proxy)
  - ISVU and studomat
  - EduGAIN
  - Microsoft
How to support everything ...

• digitalization and automation
• self-helping services
  - https://www.aaiedu.hr/
  - https://moj.aaiedu.hr/
  - https://status.eduroam.hr/
• help desk and ticketing system
How to support everything ...

• automated administration services
  - SP https://registar.aai.edu.hr/
  - IdP https://administracija.aai.edu.hr/
• Automated configuration creation
• Source code management (GitLab)
New things ...

• support for OIDC (2020.)
• support for 2FA (2019.)
  - multiple SMS gateways
  - multiple TOTP
  - WebAuthn/FIDO2
  - EID (X509 certificate)
Simple, but complex ...

• simple to use (users don’t see complexity)
• simple to implement
  - IdP (packages, hosting, …)
  - SP (packages, hosting, examples, …)
• very reliable services (99.999%)
• well connected (NIAS, eduGAIN, eduroam, …)
• a reliable source of user and organization data (audit)
Answer two questions ...

- we are a small team of 7 people who work with everything, including international tasks (GEANT), and support others
- we are not yet another authentication system, we are a reliable authentication system that provides reliable information about users and institutions from Croatian science and education institutions
According to the Open Access Policy, Srce ensures that all research data made by Srce is accessible and free to use by the general public, especially educational and professional information and content derived from the actions and work of Srce. This material is available under the Creative Commons License Attribution-ShareAlike 4.0 International.