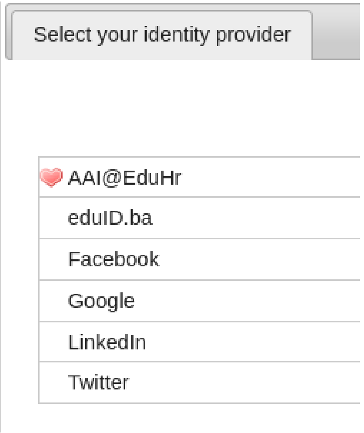
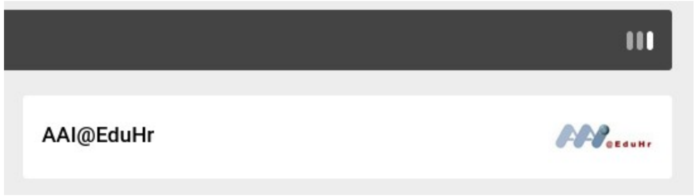
AAI@EduHr – Croatian identity federation

26.05.2023, Dubravko.Penezic@srce.hr



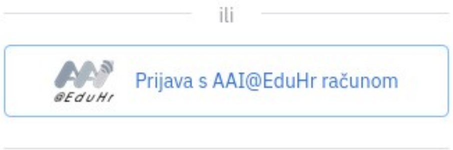
Select your identity provider

- AAI@EduHr
- eduID.ba
- Facebook
- Google
- LinkedIn
- Twitter



AAI@EduHr

@EduHr

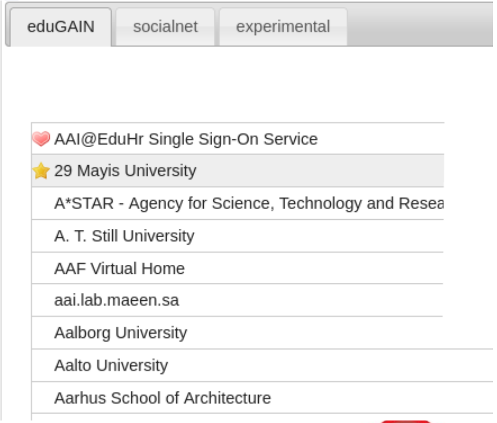


ili

Prijava s AAI@EduHr računom

Jezik podataka: Hrvatski

Prijava

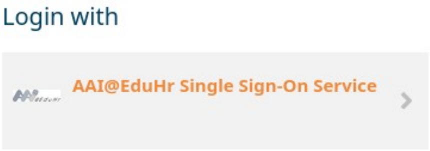


eduGAIN | socialnet | experimental

- AAI@EduHr Single Sign-On Service
- 29 Mayis University
- A*STAR - Agency for Science, Technology and Resea
- A. T. Still University
- AAF Virtual Home
- aai.lab.maeen.sa
- Aalborg University
- Aalto University
- Aarhus School of Architecture

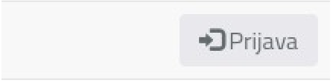
eduTEAMS

srce
Sveučilište u Zagrebu
Sveučilišni računski centar

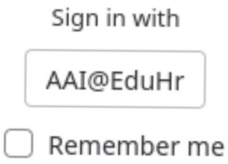


Login with

AAI@EduHr Single Sign-On Service



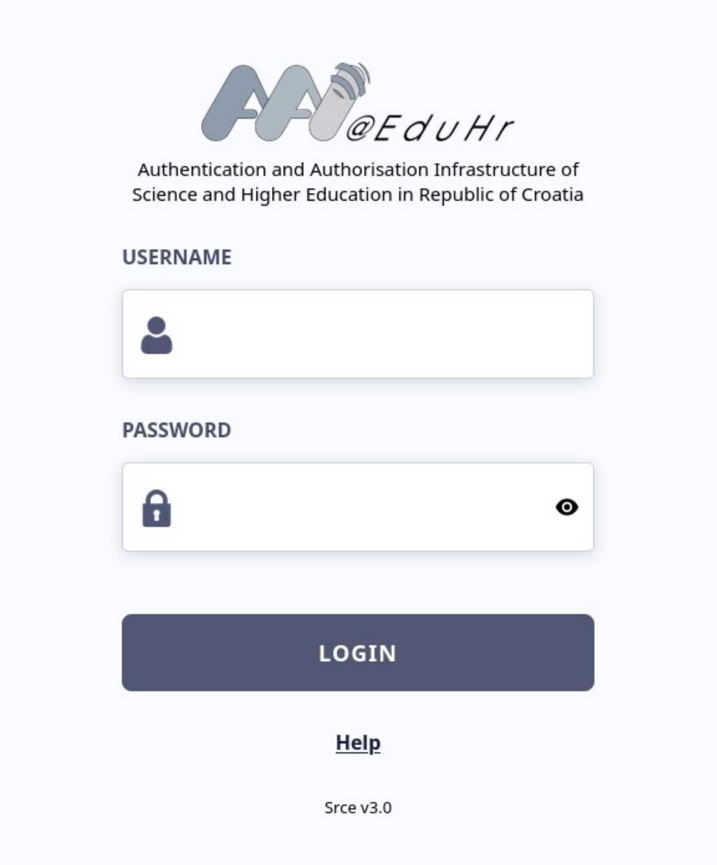
Prijava



Sign in with

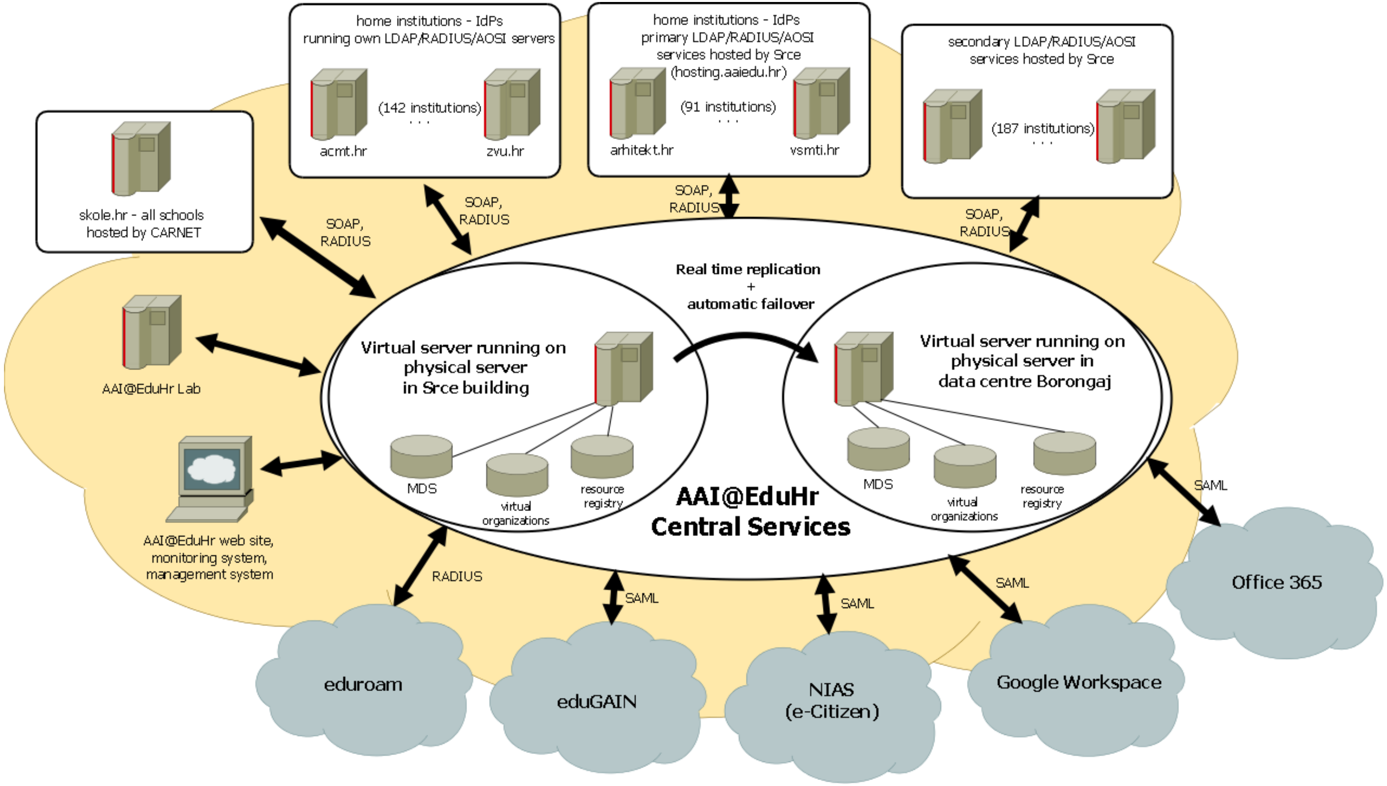
AAI@EduHr

□ Remember me



Authentication and Authorisation Infrastructure of Science and Higher Education in Republic of Croatia

Srce v3.0



home institutions - IdPs
running own LDAP/RADIUS/AOSI servers
(142 institutions)
acmt.hr
zvu.hr

home institutions - IdPs
primary LDAP/RADIUS/AOSI
services hosted by Srce
(hosting.aaiedu.hr)
(91 institutions)
arhitekt.hr
vsmti.hr

secondary LDAP/RADIUS/AOSI
services hosted by Srce
(187 institutions)

skole.hr - all schools
hosted by CARNET

AAI@EduHr Lab

AAI@EduHr web site,
monitoring system,
management system

SOAP,
RADIUS

Real time replication
+
automatic failover

Virtual server running on
physical server
in Srce building

Virtual server running on
physical server in
data centre Borongaj

MDS
virtual
organizations
resource
registry

AAI@EduHr
Central Services

RADIUS
SAML

eduroam
eduGAIN
NIAS
(e-Citizen)
Google Workspace
Office 365

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.aaiedu.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

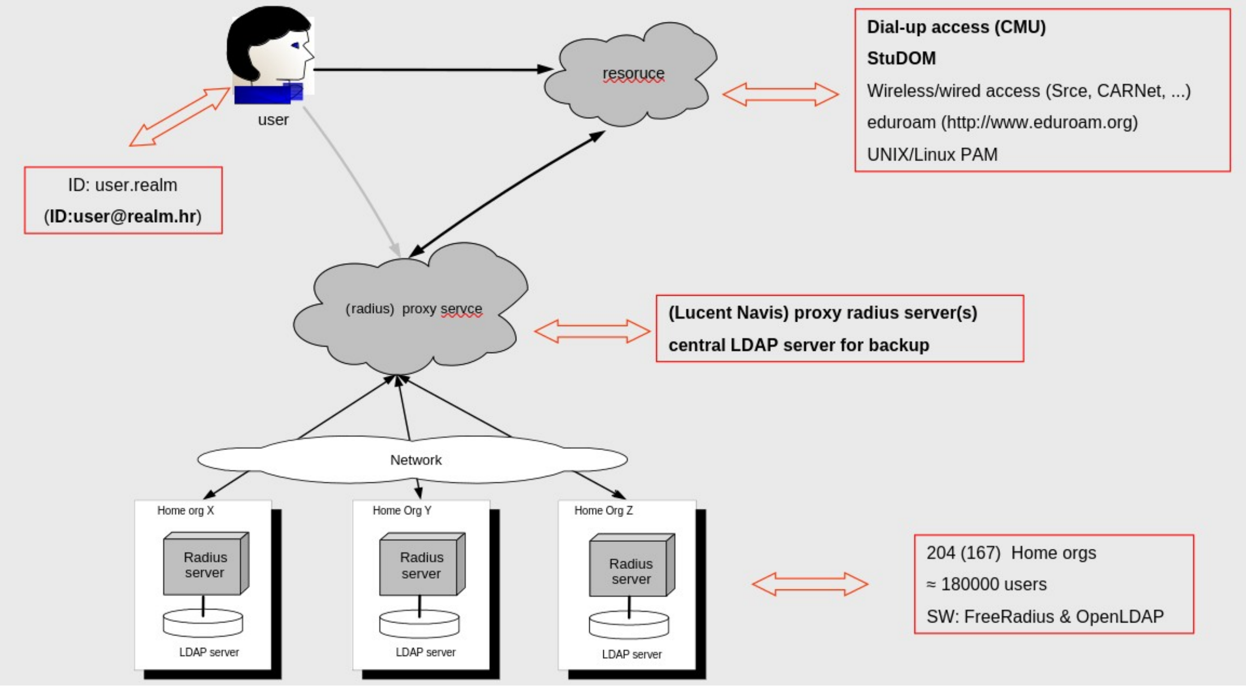
Everything starts ...

- 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 ...



ID: user.realm

(**ID:user@realm.hr**)

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

204 (167) Home orgs

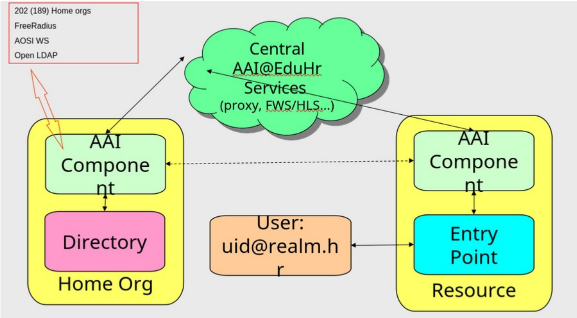
≈ 180000 users

SW: FreeRadius & OpenLDAP

2004.

Adding mash connection ...

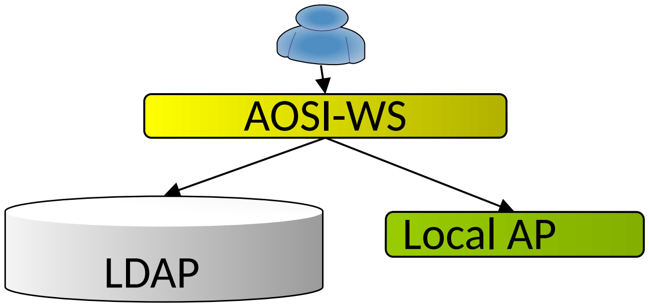
- on IdP AOSI WS (SOAP)
- on central servers FWS (federation WS) and HLS (home location service)
- on SP WS client for authentication and authorization

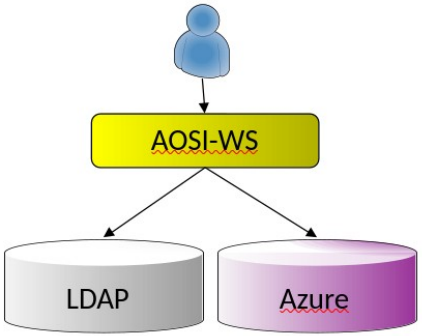


2005.

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

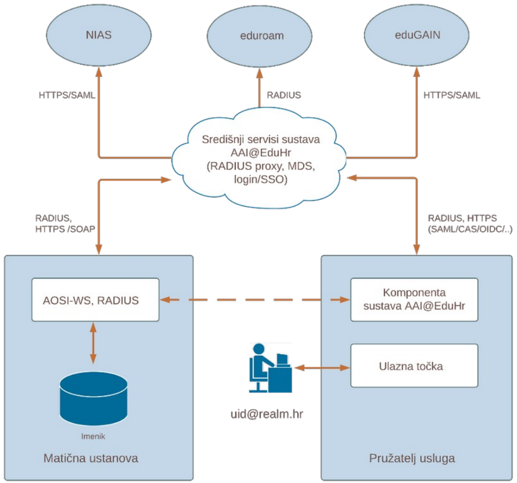
How to support everything ...

- automated administration services
  - SP https://registar.aaiedu.hr/
  - IdP https://administracija.aaiedu.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

Any questions or comments?

https://www.aaiedu.hr

aai@srce.hr

srce
University of Zagreb
University Computing Centre

www.srce.unizg.hr/en

creativecommons.org/licenses/by-sa/4.0/deed.en

www.srce.unizg.hr/oa-and-oer

cc BY SA

srce
otvoreni pristup