IdP auditing in AAI@EduHr

Miroslav Milinović

University Computing Centre,
University of Zagreb, Zagreb, Croatia

<miro@srce.hr>

TF-EMC2

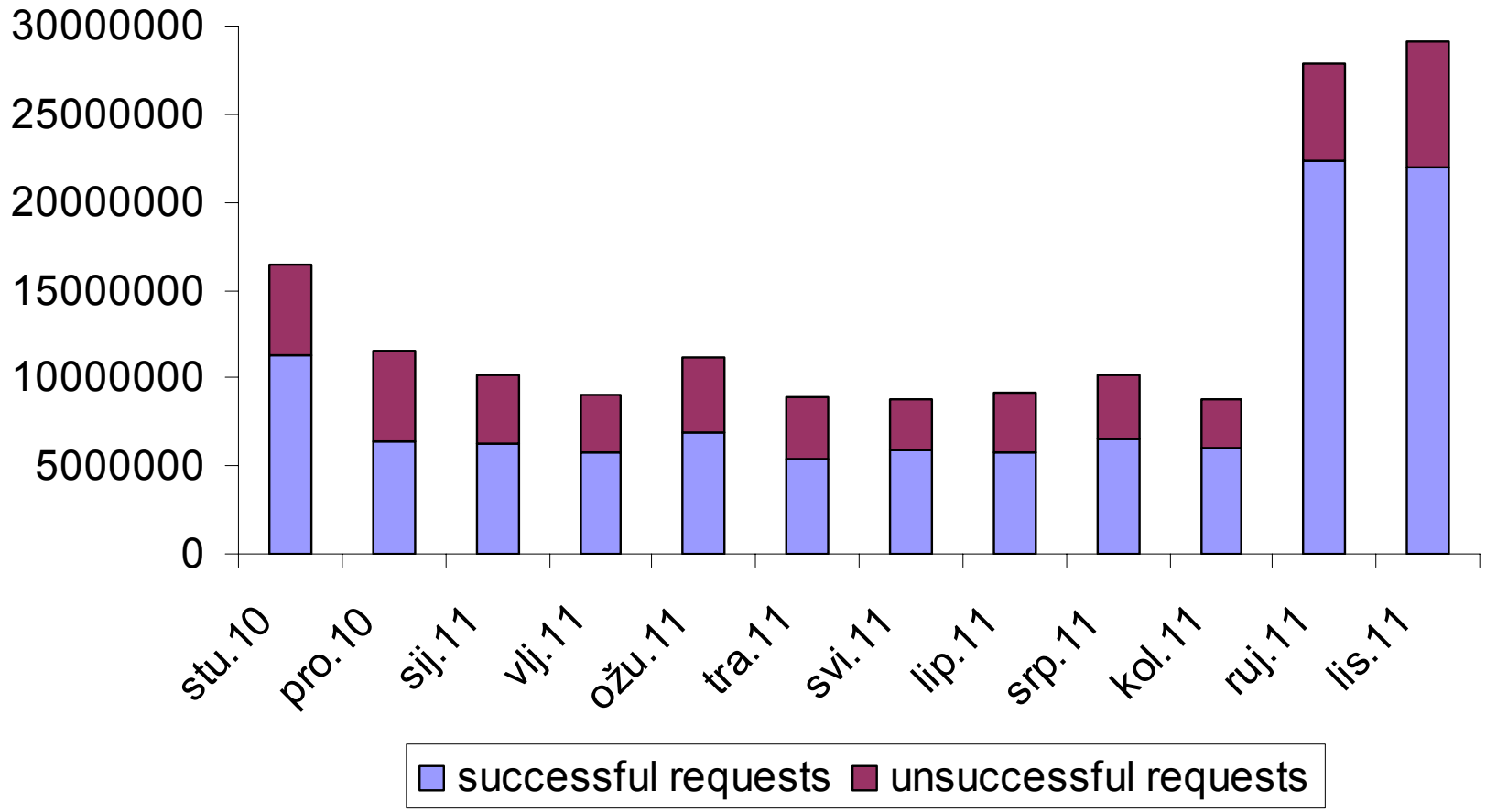
Bologna, Italy, November 2011

srce

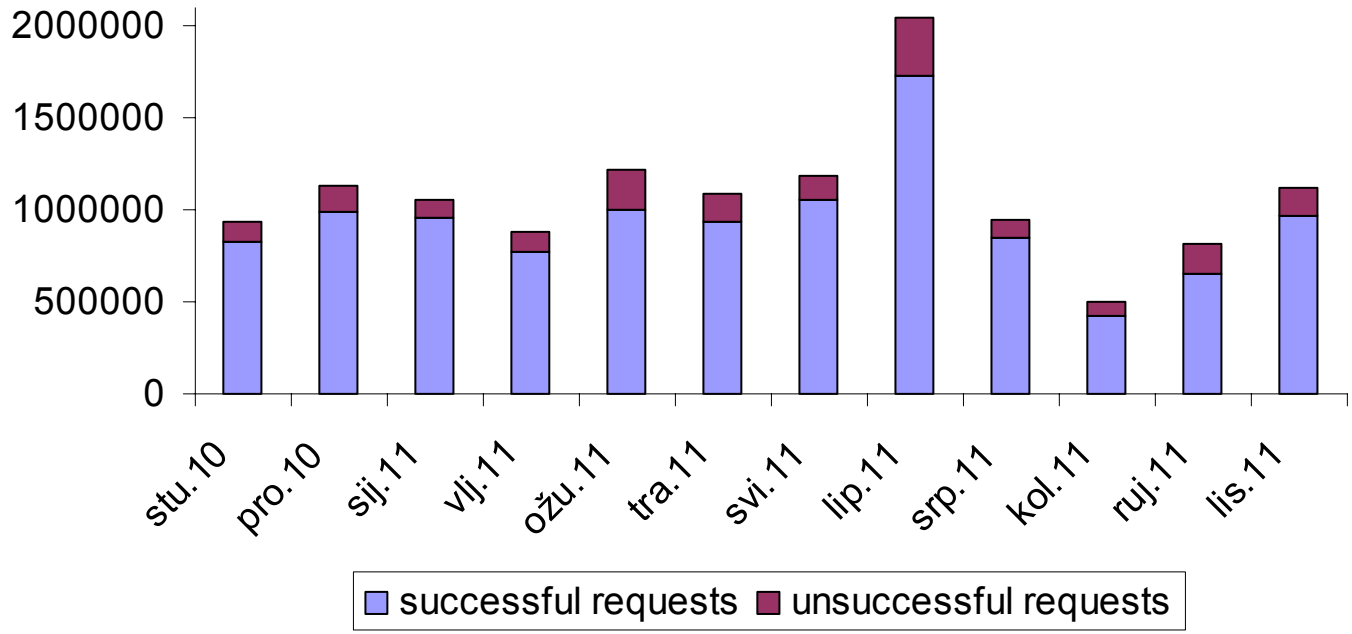
AAI@EduHr landscape

- In production since 1.3.2006.
- Hub & spoke with central services (sso/login, RADIUS proxy, MDS)
  - RADIUS
  - SAML (2.0)
  - home-grown-SOAP for legacy apps
- 220 + 1 (catch-all for schools) + 1 (home-for-homeless) IdPs
- + 650.000 identities
- + 230 SPs (from network access to Web & apps.)
- “member” of eduroam & eduGAIN

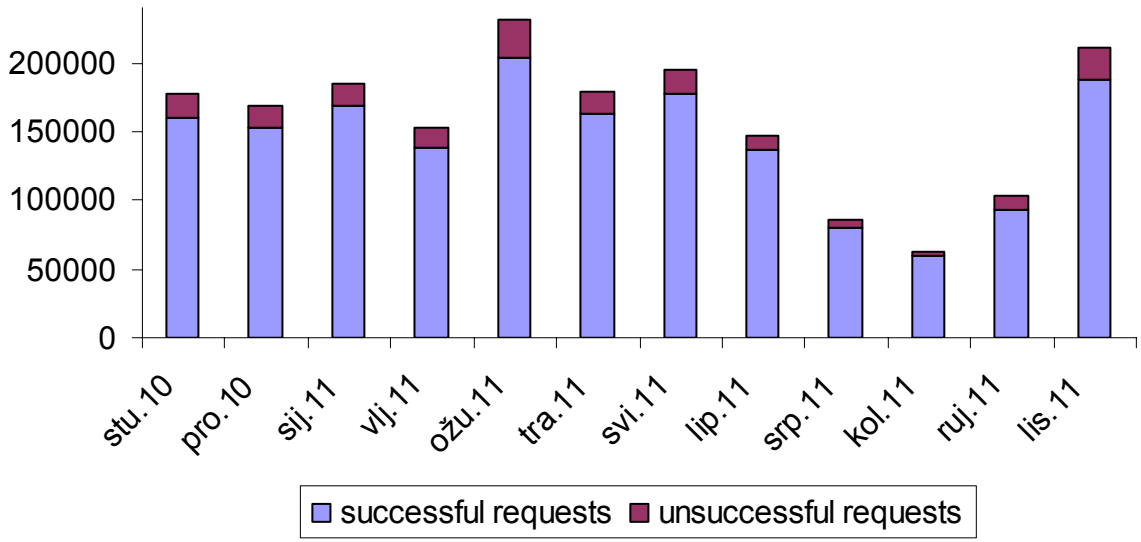
RADIUS traffic



FWS traffic


2000000
1500000
1000000
500000
0
stu.10
pro.10
sij.11
vlj.11
ožu.11
tra.11
svi.11
lip.11
srp.11
kol.11
ruj.11
lis.11
successful requests
unsuccessful requests

SSO traffic


200000
150000
100000
50000
0
stu.10
pro.10
sij.11
vlj.11
ožu.11
tra.11
svi.11
lip.11
srp.11
kol.11
ruj.11
lis.11
successful requests
unsuccessful requests

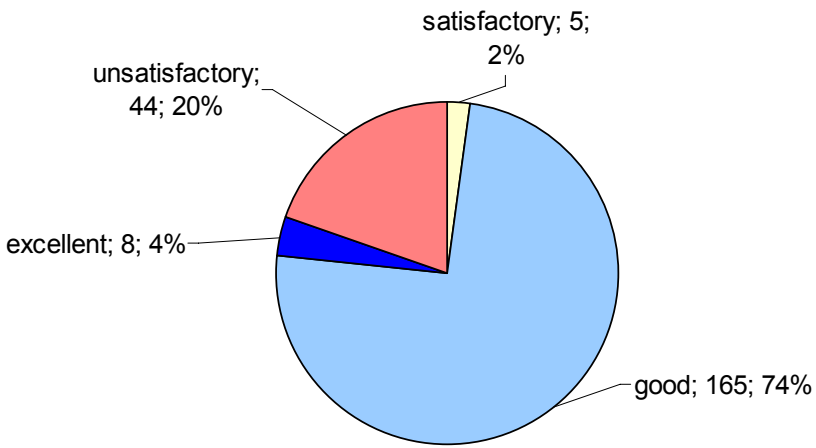
Auditing project

- enhance and maintain trust in IdPs and SPs
- auditing service:
  - documented and tested in 2010
  - covers both IdPs and SPs
  - auditing is carried out by the:
    - federation coordinator (Srce)
    - IdPs/SPs (self-audit)
  - includes both manual checkups and use of special tools
  - 2 types of requirements: MUST & SHOULD
  - 3 levels of compliance:
    - Satisfactory – all MUSTs
    - Good – all MUSTs + (at lest) 50% of SHOULDs
    - Excellent – all requirements

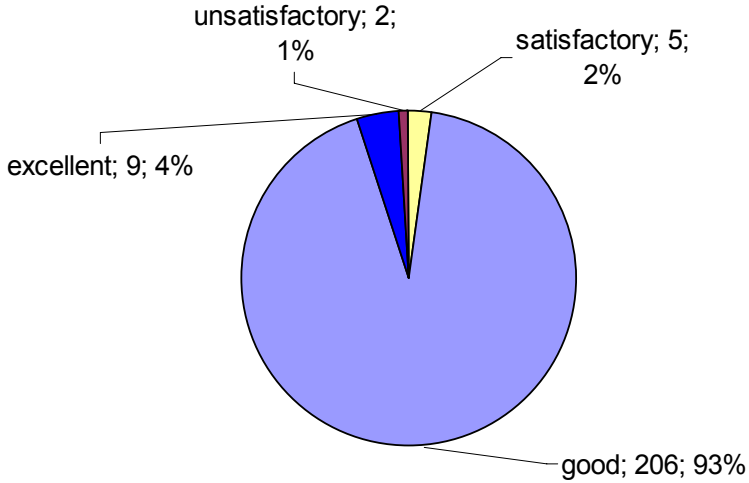
Auditing IdPs (2011)

- Total of 30 requirements (cover organisational aspects, information quality/completeness and technical correctness)
  - 18 MUSTs
  - 12 SHOULDs
- Tools used:
  - LDAP directory analyzer – tool developed by Srce
  - web site for IdP self-audit
  - central monitoring service
- Carried out between March 1 and April 18 with extra time for those who failed (from May 2 to July 8)

Auditing IdPs - results (2011)

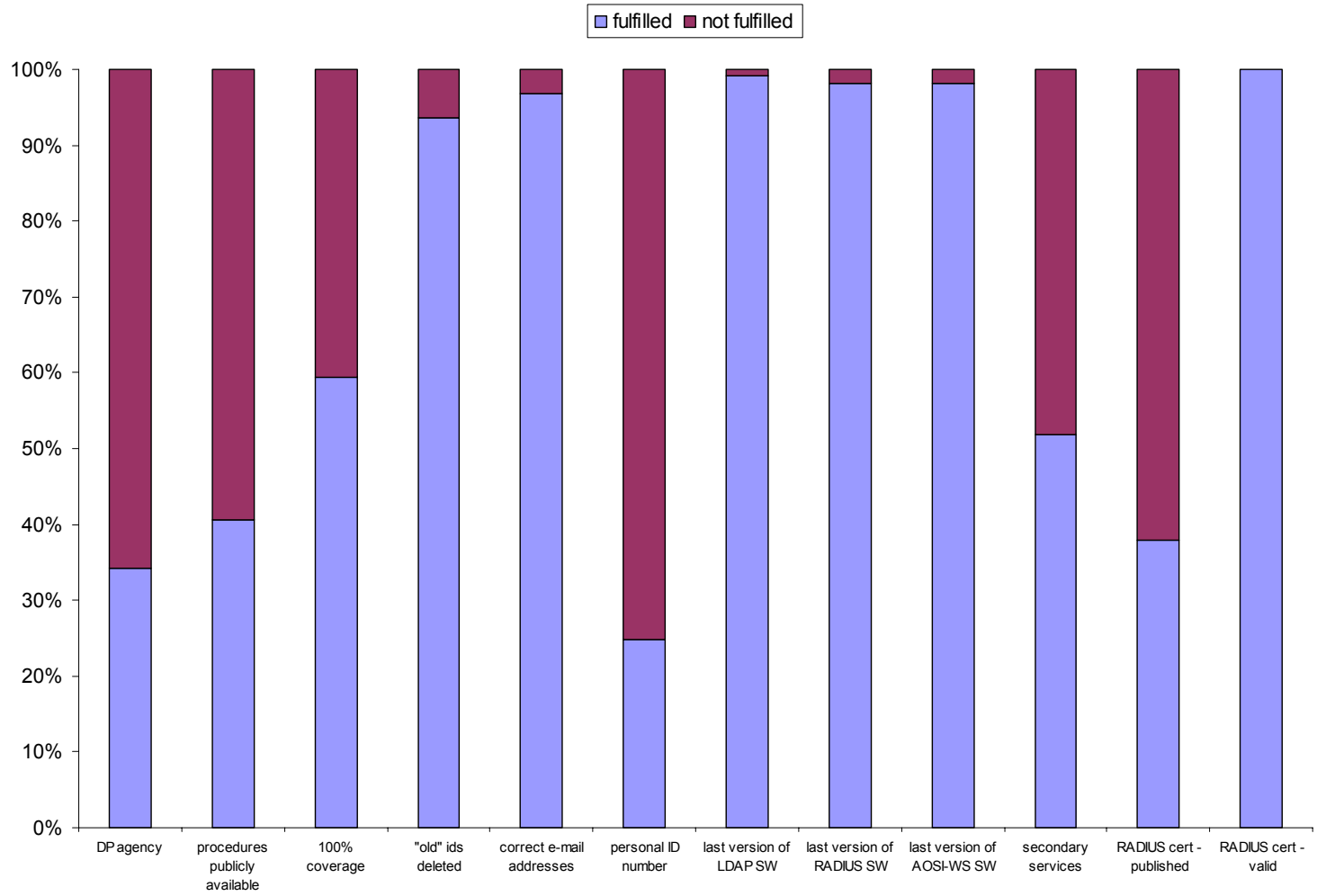


On April 18



On July 8

Requirements marked as SHOULD



Conclusion

- Lessons learned:
  - time consuming
  - positive effect (raise awareness, ...)
- Plans:
  - repeat IdP auditing regularly (once a year)
  - start SP auditing (in 2012)
  - develop special scheme for auditing newcommers
  - ajust requirements / methods before each auditing
  - align with formal LoAs