SWITCH edu-ID / Microsoft integration concept & demo

Christoph Graf
Christoph.graf@switch.ch
edu-ID Update Event, 27.6.2018, Berne
AAI-enabling only «half-way» done:
- often implemented for shared Web-Resources
- usually not implemented for LDAP/AD-integrated local resources

Why does this matter?...
University

AD/LDAP connected services: 
→ edu-ID ready?
Now, we look into this…
With AD connected services in focus

AAI/edu-ID enabled service: 
Ready for external authentication 
→ edu-ID ready
Typical service types

Microsoft cloud services
• O365 (web, fat client)
• Azure

«modern» on-prem services
• With federated login (AAI, ADFS)

«legacy» on-prem services
• Basic
• NTLM
• Kerberos
• Own userstore

AAD = Azure AD
edu-ID auth
To be assessed

Cloud only
Demo

Hybrid case
Demo

n.a.
Scenario A: Cloud only

• SWITCH (productive environment):
  – Already adopted edu-ID
  – Own tenant with O365 licenced
  – No local AD, only AAD (Azure AD)

• Demo use case
  – SWITCH employee logs into O365 with edu-ID (Demo 1)
Scenario B: Hybrid case

• Uni Demo (demo set-up):
  – Already adopted edu-ID
  – Own tenant with O365 licenced
  – Populated local AD, synced with AAD Connect (no credentials in AAD)

• Demo use cases:
  – Uni Demo staff or student log into O365 with edu-ID
    (Web & Fat Client: Demo 2)
  – Uni Demo staff or student access on-prem «legacy» service (Demo 3)
Demo 1: O365 for SWITCH employees

0. User provisioning with scripts to AAD

Azure AD

Admin

Office 365

2. Home realm discovery (WAYF)

3. Authentication

4. Service access (authenticated)

Microsoft Cloud

SWITCH edu-ID (production federation)

Organisation SWITCH (edu-ID adopted)

User

1. Access attempt (unauthenticated)
Demo 2: O365 for Uni Demo

1. Access attempt (unauthenticated)
2. Home realm discovery (WAYF)
3. Authentication
4. Service access (authenticated)

© 2018 SWITCH | 8
Demo 3: «legacy» on-prem service (Kerberos)

Organisation Uni Demo (edu-ID adopted)

User

Service access

Local authentication

«legacy» on-prem service

Office 365

Microsoft Cloud

SWITCH edu-ID (test federation)

© 2018 SWITCH |
SWITCH edu-ID/MS integration concept

Your **service login**
- Longlived, cross-organisational, user-centric, SSO…
- Use it, whenever this window appears (and only then)
- Requirements:
  - Organisation performed edu-ID-adoption
  - AAD: Custom-domain with edu-ID authentication configuration

When relevant:

Your local **machine login**
- Issued by your organisation (typ. together with machine)
- SWITCH edu-ID will offer windows integrated authentication (SPNEGO provided by edu-ID) for domain-joined clients
Summary

• Access to Microsoft cloud services (O365, Azure) for your organisation (tenant) with SWITCH edu-ID
• Harmonized login experience (AAI, Azure and Azure-connected services)
• Integrating the SAML and Azure «worlds» into the SWITCH edu-ID ecosystem
• Seamless SSO (with windows integrated login)
• SWITCH has built expertise (workshops, consultant, trainings)
Next steps

• Validation of integration concept with specialists from our community
  – If interested to contribute, please contact eduid@switch.ch

• Integration of AD-connected service will be added to future edu-id planning projects
  – and reassessed, where needed