Integrating O365 with SWITCH edu-ID

SWITCH

Thomas Bärecke
thomas.baerecke@switch.ch
15.05.2019, Berne
Process: O365 for edu-ID adopted organization

0. User provisioning with scripts to AAD

1. Access attempt (unauthenticated)

2. Home realm discovery (WAYF)

3. Authentication

4. Service access (authenticated)

Azure AD

Office 365

Microsoft Cloud

Organisation SWITCH (edu-ID adopted)

User

SWITCH edu-ID (production federation)
Demo

• Demo in browser
Enabling federated login
(for every AAD custom domain separately)

Via PowerShell:

Connect-MsolService

$dom = "unidemo.ch"
$fedBrandName = "Demo University"
$url = "https://login.unidemo.test.eduid.ch/idp/profile/SAML2/POST/SSO"
$uri = "https://aai-login.uni-demo.ch/idp/shibboleth"
$logoutUrl = "https://login.test.eduid.ch/idp/profile/Logout"
$certData = [system.convert]::tobase64string($cert.rawdata)

User provisioning

Synchronisation methods SWITCH edu-ID

• Pull via Attribute Provider API (Attribute Aggregator)
• Push via Affiliation API

Attributes

• extAzureADImmutableID
• userPrincipalname
extAzureADImmutableId

Organizations with Active Directory & AAD Connect
• Equals the sourceAnchor of AAD Connect
• By Default AD user value of ms-DS-ConsistencyGuid (base64 encoded)

Other organizations
• May be generated for each user by guid-tool or other processes
• Stored in organization’s IdM
• Synchronized with Azure AD attribute ImmutableId
userPrincipalName

Organizations with (On-Prem) Active Directory
• Directly taken from AD attribute of the same name

Other organizations
• Depending on the organization’s IdM system, the user’s organizational e-mail address or a separate value for a userPrincipalName attribute as defined by Microsoft

In all cases
• Synchronized to userPrincipalName of Azure AD tenant
Working for a better digital world