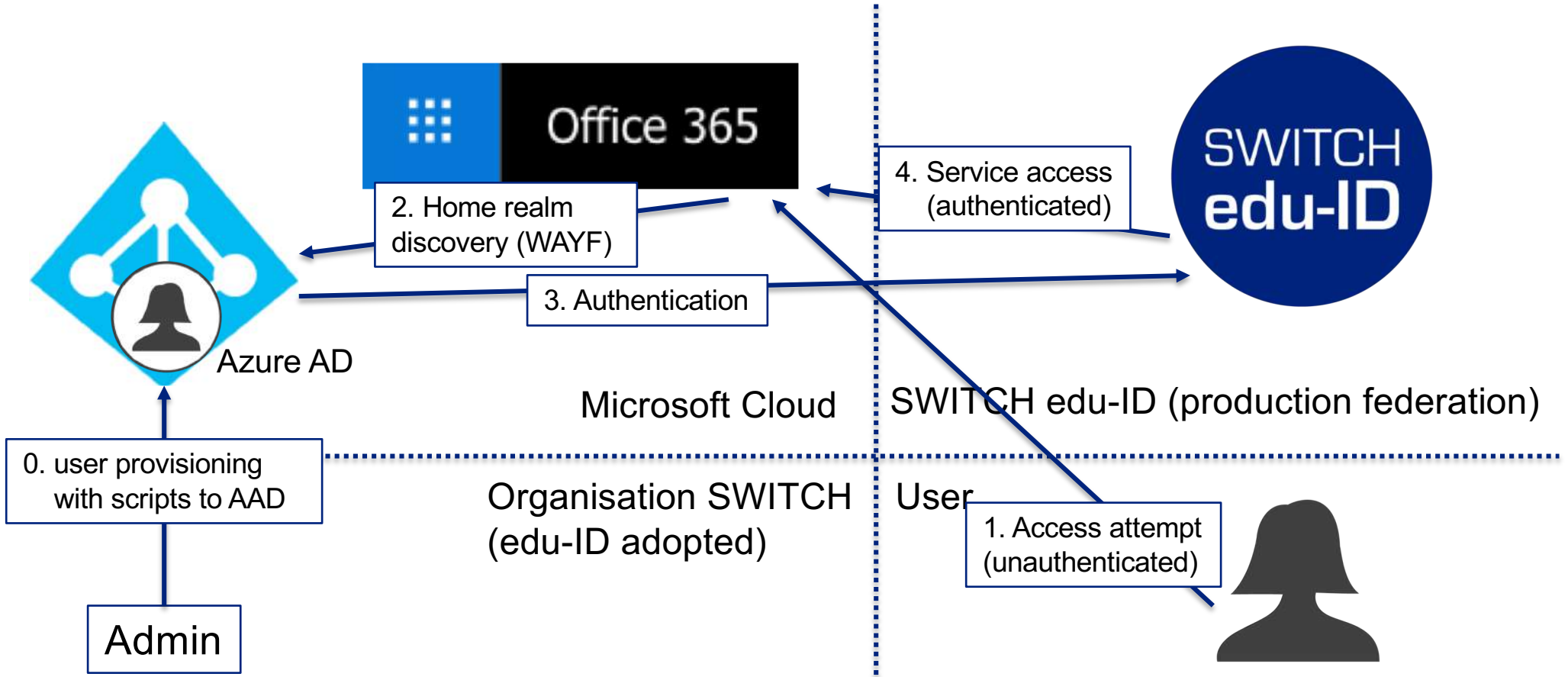
Integrating O365 with SWITCH edu-ID

SWITCH

Thomas Bärecke
thomas.baerecke@switch.ch

15.05.2019, Berne

Process: O365 for edu-ID adopted organization



Demo

- Demo in browser

Enabling federated login (for every AAD custom domain seperately)

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"
$cert = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2("C:\unidemocert.crt")
$certData = [system.convert]::tobase64string($cert.rawdata)


Set-MsolDomainAuthentication –DomainName $dom –federationBrandName $FedBrandName -Authentication Federated -
PassiveLogOnUri $url -SigningCertificate $certData -IssuerUri $uri -LogOffUri $logoutUrl -PreferredAuthenticationProtocol
SAMLP
```

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

SWITCH

Working for a better digital world