Otto-Friedrich-Universität Bamberg

Exchange on premise mit MFA!?

82. DFN-Betriebstagung 25./26.03.2025

Ausgangssituation

Auslöser

- Beschluss der UL zur Einführung von MFA auf Empfehlung CIO mit Absicherung E-Mail Exchange on premise

Ziel

- Eindämmung von Phishingangriffen

Problem

- Exchange Online (EXO) kann OAuth mit allen Clients https://learn.microsoft.com/de-de/exchange/client-developer/legacy-protocols/how-to-authenticate-an-imap-pop-smtp-application-by-using-oauth
- Exchange on premise nicht!, Exchange 2019 on premise nur mit Outlook und Outlook-Apps und ADFS Oauth (mit MFA) unterstützt https://learn.microsoft.com/en-us/exchange/plan-and-deploy/post-installation-tasks/enable-modern-auth-in-exchange-server-on-premises?view=exchserver-2019

Problem

- HybridModernAuthentication (HMA) Warum nicht?
  - P1/P2-Lizen und gleichen Client-Einschränkungen wie Ex2019 https://learn.microsoft.com/de-de/microsoft-365/enterprise/configure-exchange-server-for-hybrid-modern-authentication?view=o365-worldwide&WT.mc_id=M365-MVP-6771
- Clients können nicht vorgeschrieben werden
  ➔ imap und smtp werden weiterhin benötig

Lösung

- App-Passwort für E-Mail-Postfach (Bedienstete ca. 3000, Studierende ca.400 Mailboxen ~ 3 % on premise)
- AD kann keine zusätzlichen Passwörter zum Account verwalten ➔ E-Mail-Postfach vom normalen Nutzerkonto <uid> trennen
  - Zusätzliches Nutzerkonto <uid>-email mit App-Passwort = langes Zufallspasswort
  - Zufallspasswort ist nicht änderbar für Nutzende
  - Umstellung / Herausgabe App-Passwort per Selfservice mit MFA abgesichert

Voraussetzungen

- ADFS für „SAML“ OWA:
  - ADFS: Migration nach Entra nahe gelegt, https://learn.microsoft.com/en-us/windows-server/identity/ad-fs/ad-fs-overview
  - aber weiterhin in Windows-Server 2025 enthalten, kein EOL https://learn.microsoft.com/en-us/answers/questions/2150475/future-of-federation-service-in-windows-server
- ADFS als Proxy nach Shibboleth vor OWA
  - Prinzip Vortrag 71. BT https://download.aai.dfn.de/praesentationen/betriebstagungen/71/BT71_AAI_O365_ADFS_Shibboleth_Scheiterer.pdf

Shibboleth – ADFS – OWA

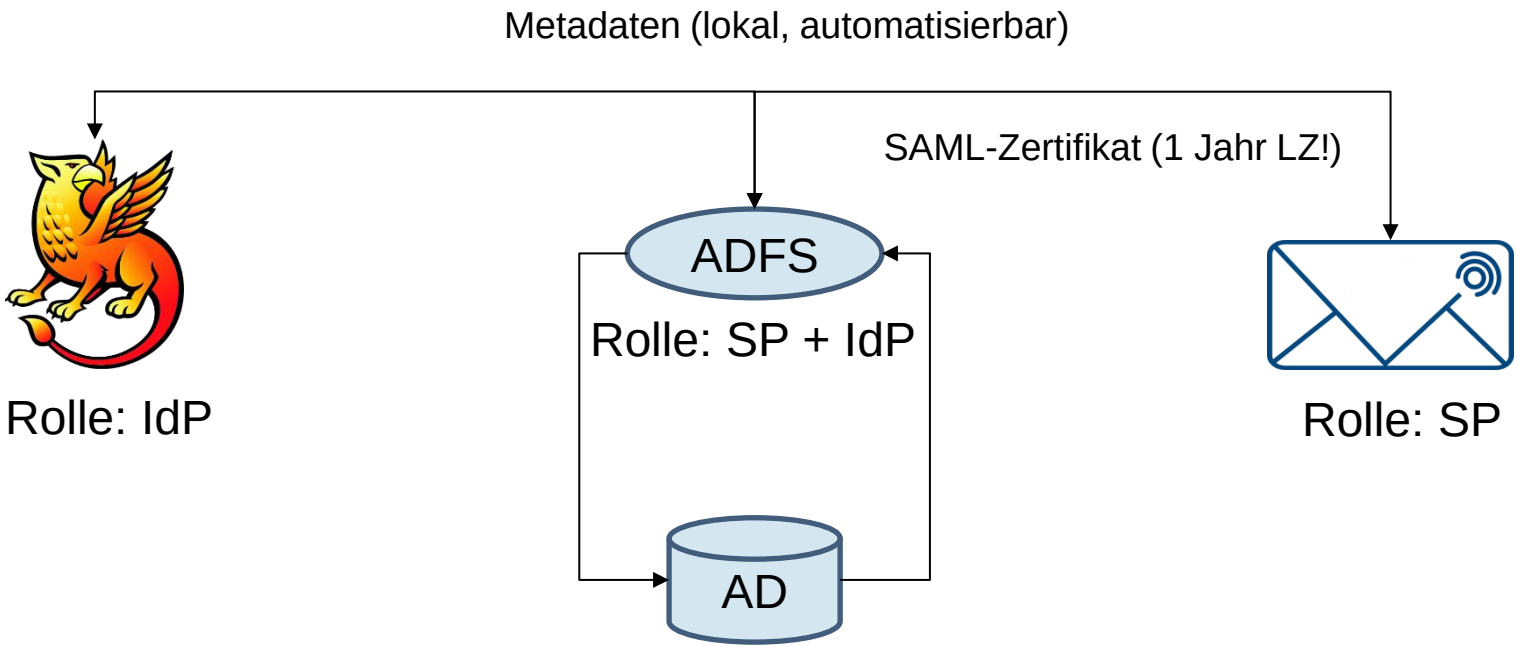

Bild: https://shibboleth.net

Shibboleth – ADFS – OWA – Login

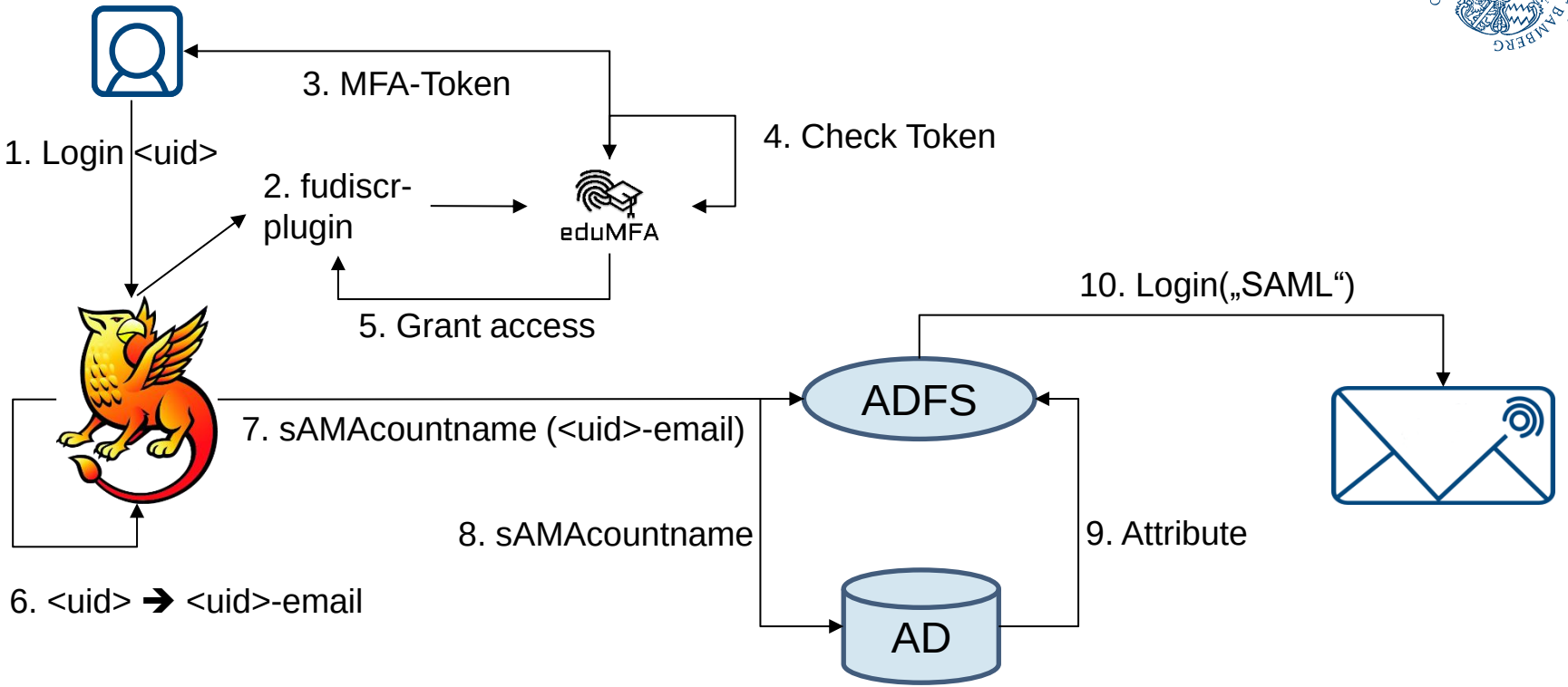

Bild: https://shibboleth.net

Shibboleth <uid> ➔ <uid>-email

attribute-resolver.xml (AD-Ldap-Resolver ist Voraussetzung, uid ist sAMAccountName)

```
<AttributeDefinition xsi:type="ScriptedAttribute" id="internadfssAMAccountName" activationConditionRef="saminternadfs">
        <InputAttributeDefinition ref="uid" />
        <InputAttributeDefinition ref="mail" />
        <InputAttributeDefinition ref="msExchRecipientTypeDetails" />
        <Script>
                <![CDATA[
                uid = uid.getValues().get(0);
                if (mail.getValues().size() > 0 && msExchRecipientTypeDetails.getValues().size() == 0) {
                        tmp = uid+"-email";
                } else {
                        tmp = uid;
                }
                internadfssAMAccountName.getValues().clear();
                internadfssAMAccountName.getValues().add(tmp);
                ]]>
        </Script>
</AttributeDefinition>
```

Shibboleth <uid> ➔ <uid>-email

../conf/attributes/rule.xml urn:oid:1.2.840.113556.1.4.221 = sAMAccountName (für ADFS)

```
<bean parent="shibboleth.TranscodingProperties">
        <property name="properties">
                <props merge="true">
                        <prop key="id">internadfssAMAccountName</prop>
                        <prop key="transcoder">SAML2StringTranscoder</prop>
                        <prop key="saml2.name">urn:oid:1.2.840.113556.1.4.221</prop>
                        <prop key="displayName.en">Account name</prop>
                        <prop key="displayName.de">Accountname</prop>
                        <prop key="description.en">name of account</prop>
                        <prop key="description.de">Name des Benutzeraccounts</prop>
                </props>
        </property>
</bean>
```

attribute-filter.xml

```
<AttributeFilterPolicy id="releaseTo_ADFS">
        <PolicyRequirementRule xsi:type="Requester" value="http://<adfsdns>/adfs/services/trust" />
        <AttributeRule attributeID="internadfssAMAccountName" permitAny="true"/>
</AttributeFilterPolicy>
```

Exchange Postfachtransfer

- Alles auf einem Domain Controller!
- Vorbereitung
  - AD-Account <uid>-email erstellen, App-Passwort im IAM speichern
  - User <uid>: Mailbox und Regionalconf auslesen

```
$regConf = Get-MailboxRegionalConfiguration -
Identity $moveFrom
$mailbox = Get-Mailbox -Identity $moveFrom -
DomainController $dc
```

  - Bisherigen Account <uid> sichern

```
$aduserMoveFrom = Get-ADUser -Identity $moveFrom
-Properties *
```

Exchange Postfachtransfer

- Umzug
  - `Disable-Mailbox -Identity $mailbox.LegacyExchangeDN -DomainController $dc -Confirm:$false`
  - `Connect-Mailbox -Identity $mailbox.LegacyExchangeDN -Database $mailbox.Database -user <uid>-email -DomainController $dc -Confirm:$false`
  - Attribute von <uid> nach <uid>-email übertragen (Bildchen, extensionAttributes…)
  - Regionalconf übertragen (nach 25 Sekunden Wartezeit, Sync DCs 20 Sekunden)
  - Addressbookpolicy übertragen
  - Gruppenmitgliedschaften korrigieren
    - Verteilergruppen <uid> ➔ <uid>-email
    - Personengruppen (spezielle securitygroups, die in normale securitygroups aufgenommen werden, da Schachtelungsverbot bei uns securitygroup in securitygroup)
      <uid> entfernen und in Exchange-Personengruppe aufnehmen
      <uid>-email

Fragen und Anregungen