SAML-Authentifizierung Anwendung in Schulnetzwerken

Mag. Gerald STACHL
PH Niederösterreich

INTRO - CISCO

- CCNA R&S: Introduction to Networks
- CCNA R&S: Scaling Networks
- CCNA R&S 6.0 Bridging
- CCNA Discovery 2: Working at a Small-to-Medium Business or ISP
- CCNA Discovery 4: Designing and Supporting Computer Networks
- CCNA Exploration 2: Routing Protocols and Concepts
- CCNA Exploration 4: Accessing the WAN
- Introduction to the Internet of Everything
- IoT Fundamentals: Hackathon Playbook
- Introduction to Cybersecurity
- Get Connected
- Be Your Own Boss
- Packet Tracer Know How 2: Packet Tracer Mobile
- Partner: NDG Linux Essentials
- Partner: NDG Linux II
- Partner: CLA - Programming Essentials in C
- CCNA R&S: Routing and Switching Essentials
- CCNA R&S: Connecting Networks
- CCNA Discovery 1: Networking for Home and Small Business
- CCNA Discovery 3: Introducing Routing and Switching in the Enterprise
- CCNA Exploration 1: Network Fundamentals
- CCNA Exploration 3: LAN Switching and Wireless
- Networking Essentials
- Introduction to IoT
- Entrepreneurship
- Cybersecurity Essentials
- Community: Smart Grid Essentials
- Packet Tracer Know How 1: Packet Tracer 101
- Mobility Fundamentals
- Partner: NDG Linux I
- Partner: CPA - Programming Essentials in C++

Bei Interesse

- Mail an gerald.stachl@ph-noe.ac.at
  - bis 30.04.2017

- Instruktoreneinschulung:
  - HTL Rennweg
  - Christian Schöndorfer

Übersicht

- SAML Grundlagen
- Vergleich: SAML, OpenID, oAuth
- Demoinstallation
  - ADFS + Shibboleth SP am Beispiel Moodle
- weitere Beispiele
  - Shibboleth IDP (PH NÖ)
  - WebUntis als SP
    - Beispiel BG Babenbergerring
    - ADFS, Moodle, WebUntis

Was ist SAML? Wozu??

bundesgymnasium babenbergerring

Authentifizierungsserver
BG Babenbergering

Melden sie sich mit ihrer Benutzerkennung am BG Babenbergerring an.

bgbab\Benutzerkennung

Kennwort

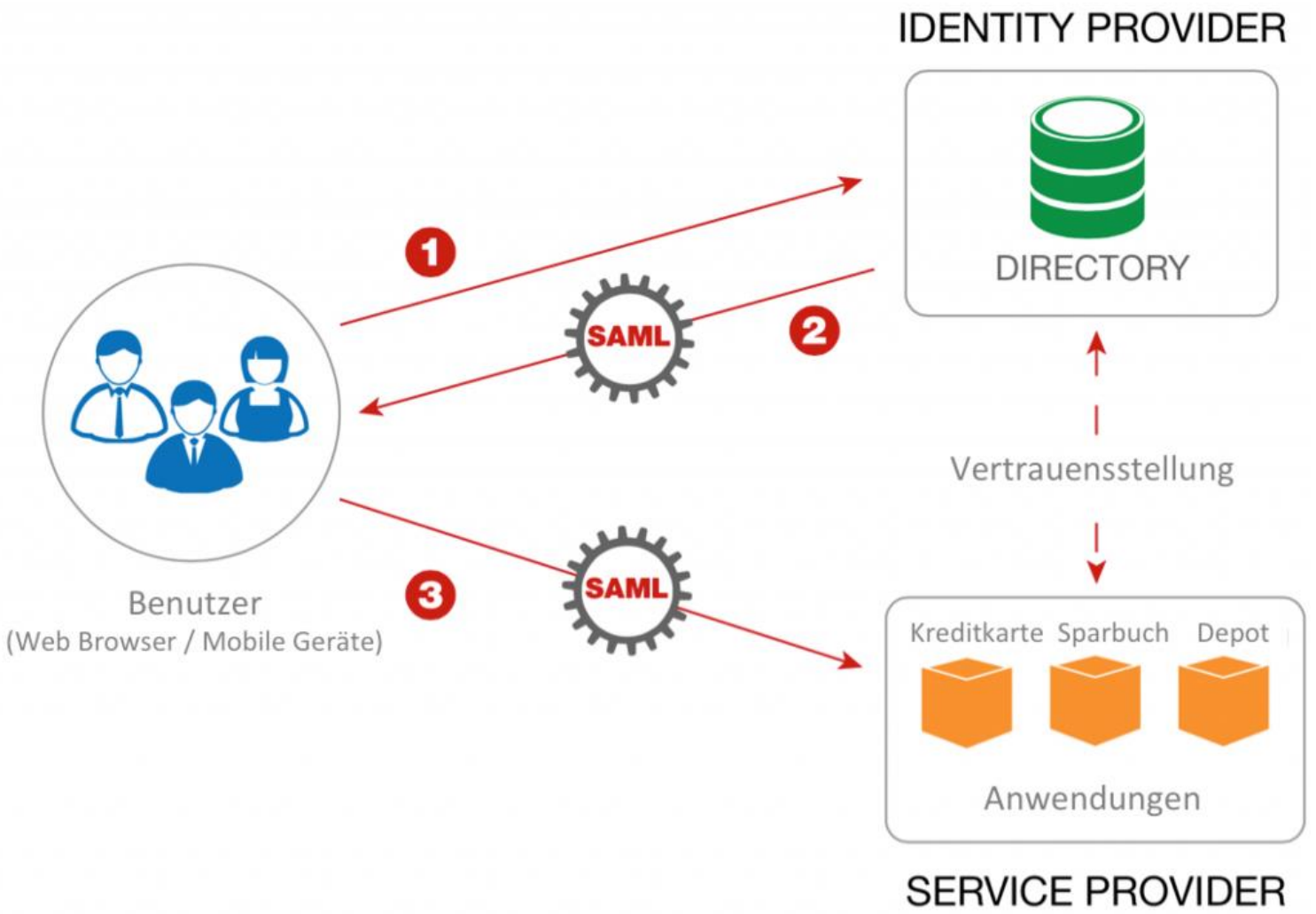
Anmelden

Klicken sie hier für weitere Informationen.

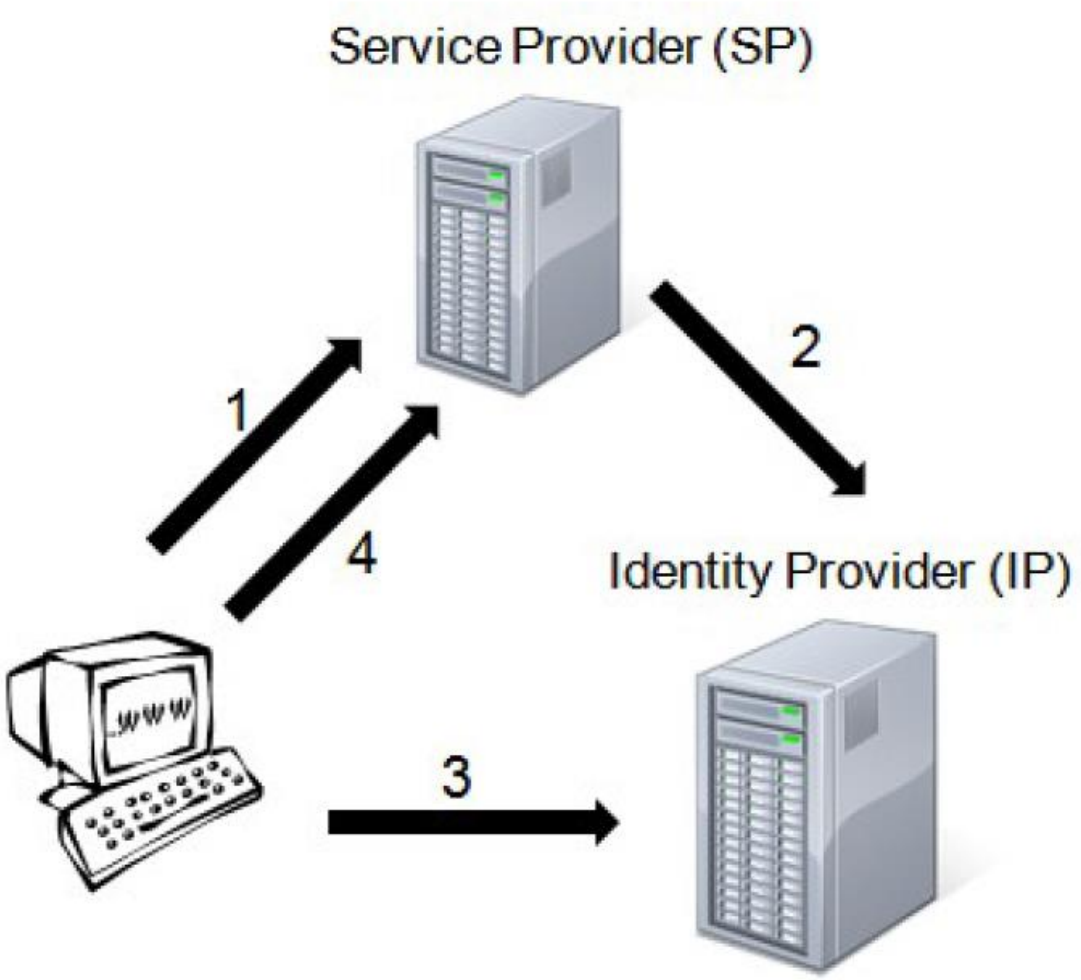
Home Privacy

SAML - ???

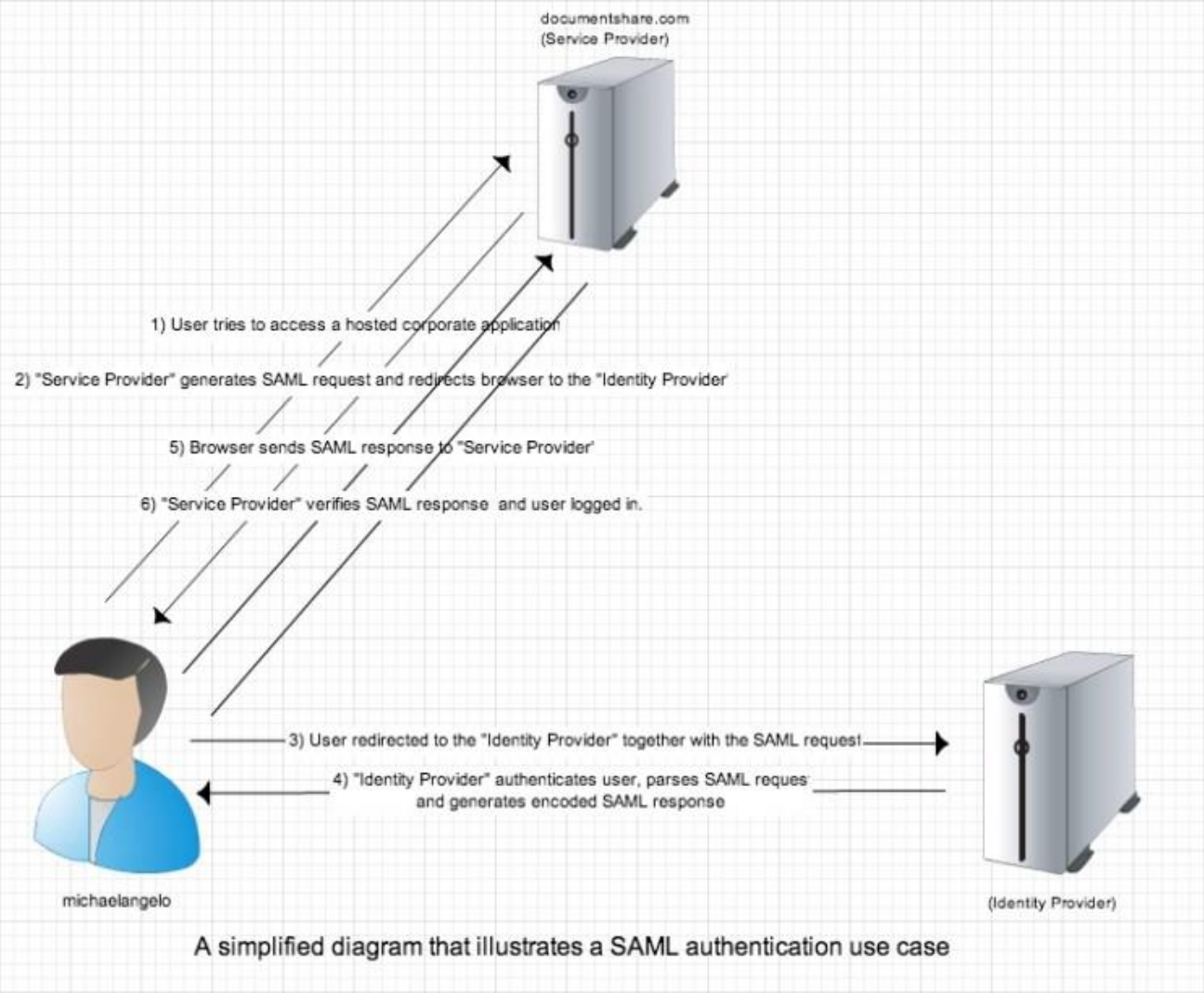
- SAML = Secure Assertion Markup Language
  - XML Framework zum Austausch von
    - Authentifizierungs- und
    - Autorisierungsinformationen
  - Entwicklung: 2001 (OASIS-Konsortium)
  - Ziele:
    - Single Sign-On
    - Verteilte Transaktion
    - Autorisierungsdienste


IDENTITY PROVIDER
DIRECTORY
1
SAML
2
Vertrauensstellung
Benutzer
(Web Browser / Mobile Geräte)
3
SAML
Kreditkarte
Sparbuch
Depot
Anwendungen
SERVICE PROVIDER

Service Provider initiierter SSO

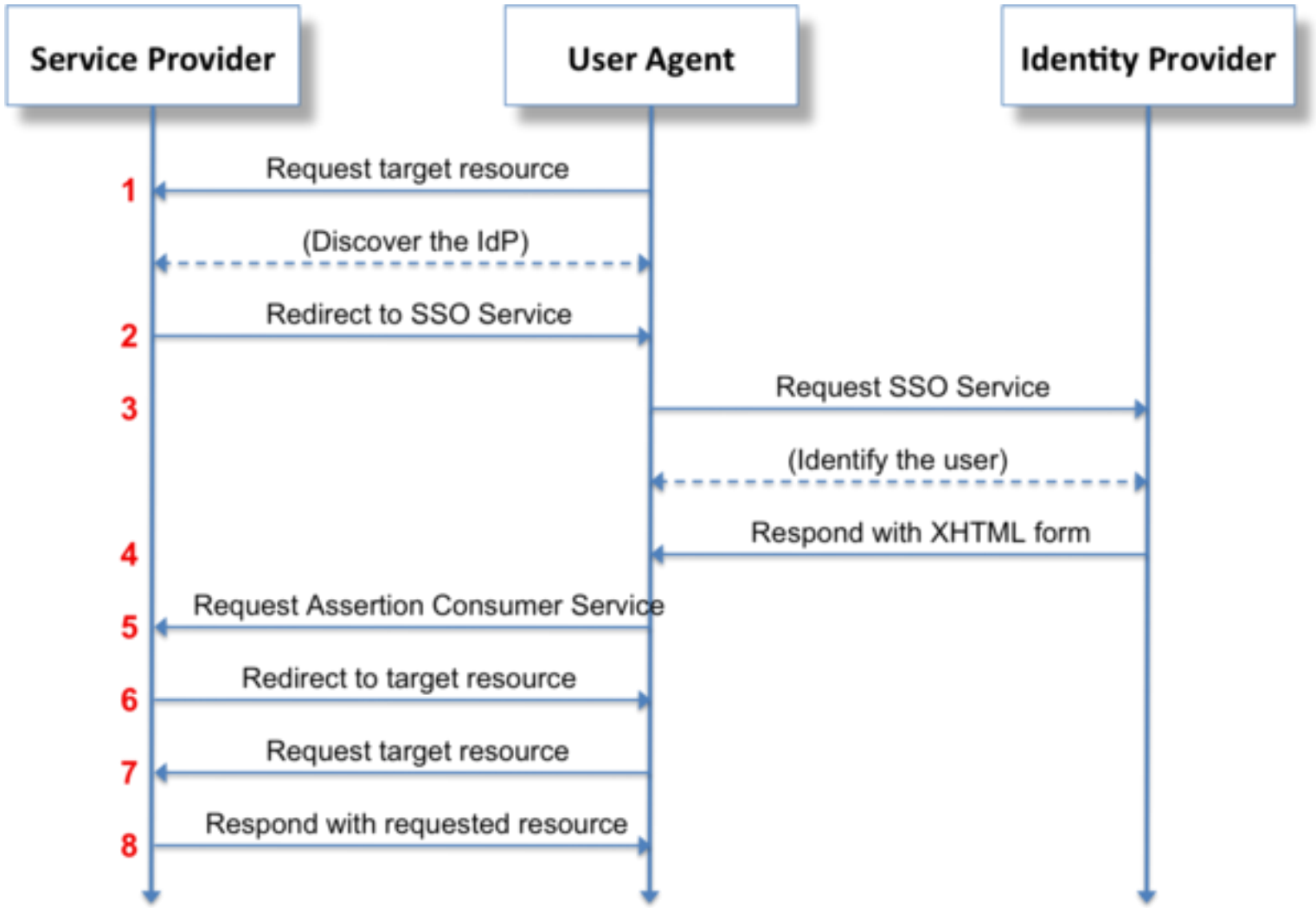


SAML Ablauf



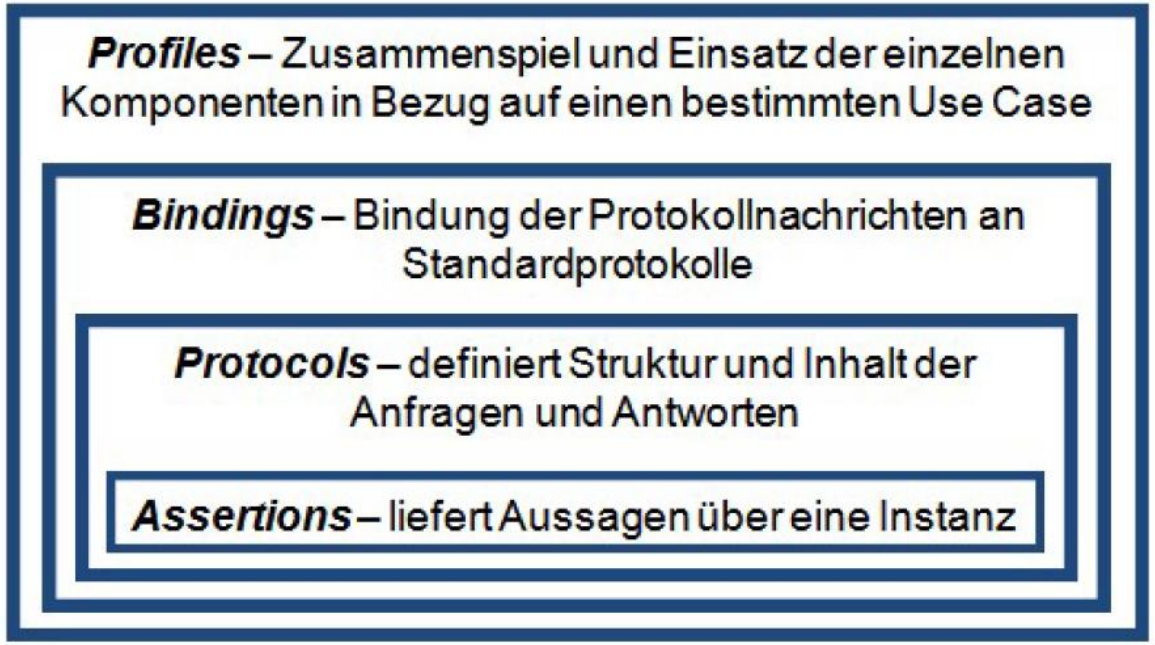
A simplified diagram that illustrates a SAML authentication use case

Ablauf einer SAML Authentifizierung



SAML Aufbau

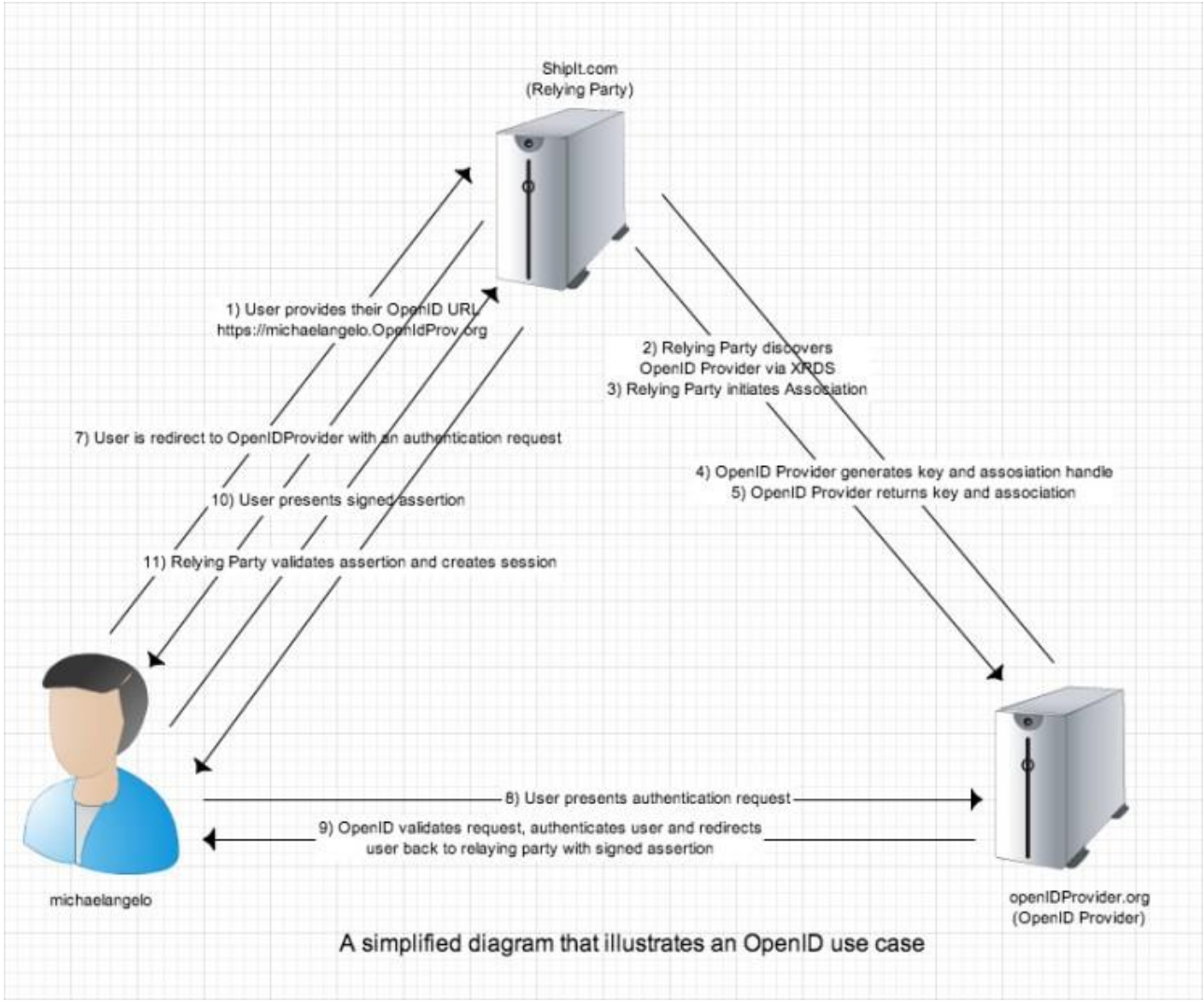
- Assertion
  - Aussagen über Parteien
  - Authentizität
- Protokolle
  - Ablauf der Anfragen und Antworten zwis den Parteien
- Bindungen
  - Zusammenspiel mit Standardprotokollen (HTTP, SOAP)
- Profil
  - Zusammenspiel der Komponenten in einem Anwendungsfall



OpenID

- Open standard sponsored by
  - Facebook
  - Microsoft
  - Google
  - PayPal
  - Ping Identity
  - Symantec
  - Yahoo

OpenID Ablauf

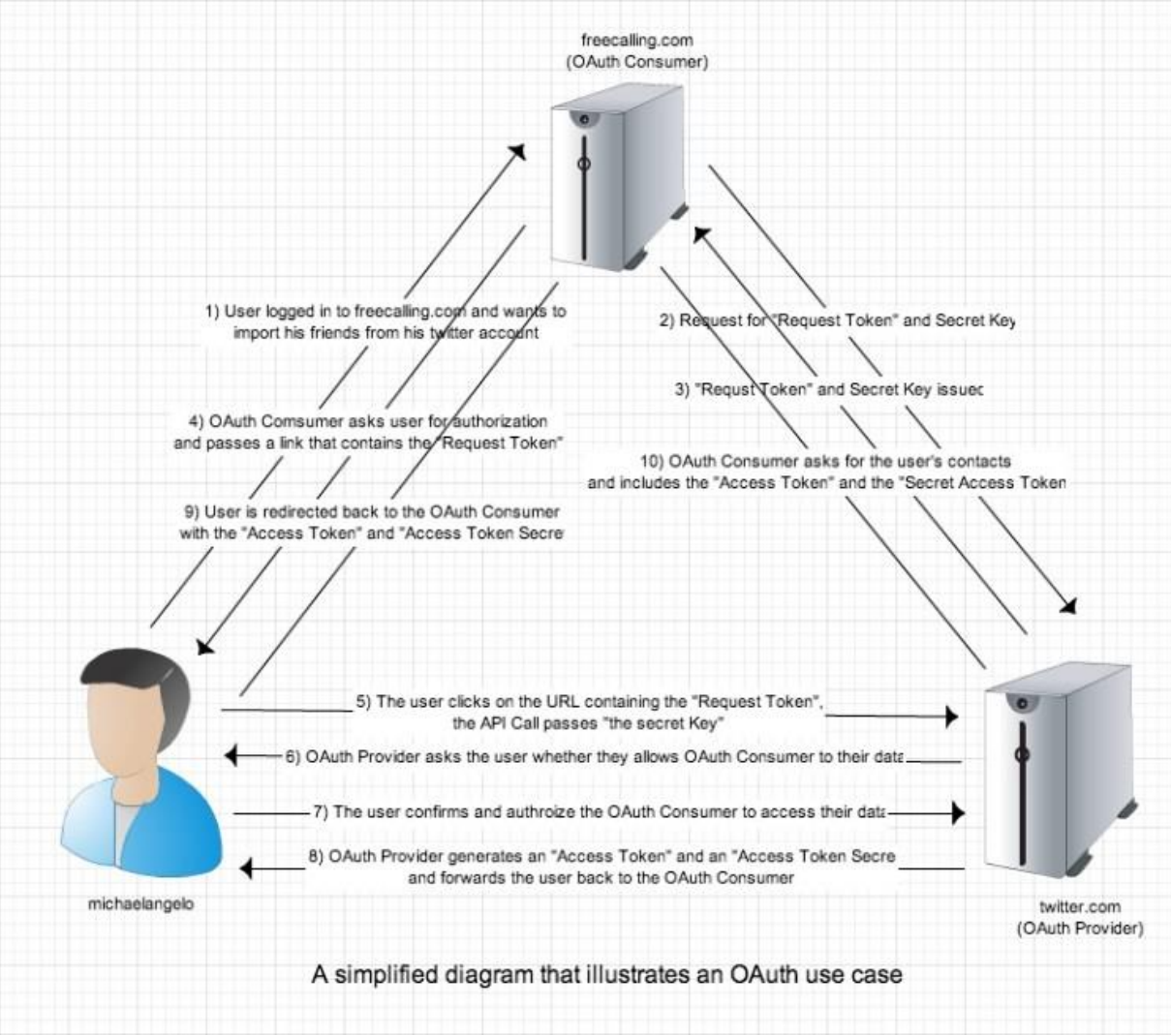


A simplified diagram that illustrates an OpenID use case

oAuth

- nur für Authorisierung
- keine Authentifizierung
- Beispiel:
  - Zugriff auf „Twitter-Freunde“ erlauben
  - Enduser (gewährt Zugriff)
  - oAuth Provider (Twitter.com)
  - oAuth Consumer: Plattform, die Zugriff auf Twitter erhält

oAuth - Ablauf



A simplified diagram that illustrates an OAuth use case

VERGLEICH

	OAuth2	OpenId	SAML
Token (or assertion) format	JSON or SAML2	JSON	XML
Authorization?	Yes	No	Yes
Authentication?	Pseudo-authentication	Yes	Yes
Year created	2005	2006	2001
Current version	OAuth2	OpenID Connect	SAML 2.0
Transport	HTTP	HTTP GET and HTTP POST	HTTP Redirect (GET) binding, SAML SOAP binding, HTTP POST binding, and others

IDP – Identity Provider

- "A kind of provider that creates, maintains, and manages identity information for principals and provides principal authentication to other service providers within a federation, such as with web browser profiles.“
- Beispiele:
  - ADFS (Microsoft), Rolle
  - Shibboleth IDP
    - Java (Tomcat)
    - Linux + Windows

SP – Service Provider

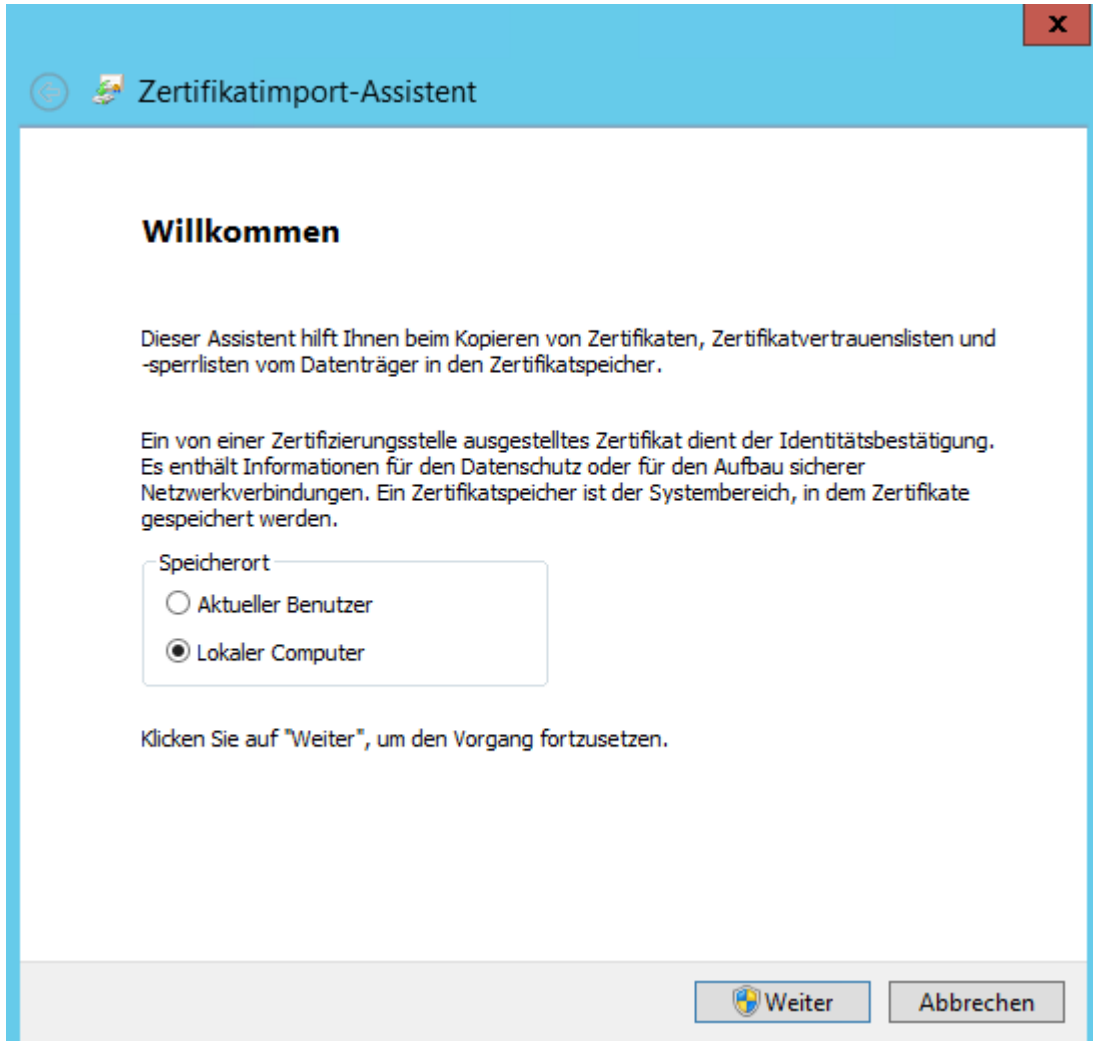
- "A role donned by a system entity where the system entity provides services to principals or other system entities“
- Beispiele
  - Shibboleth SP
  - SimpleSAMLPhP
  - ADFS

Anleitungen Shibboleth

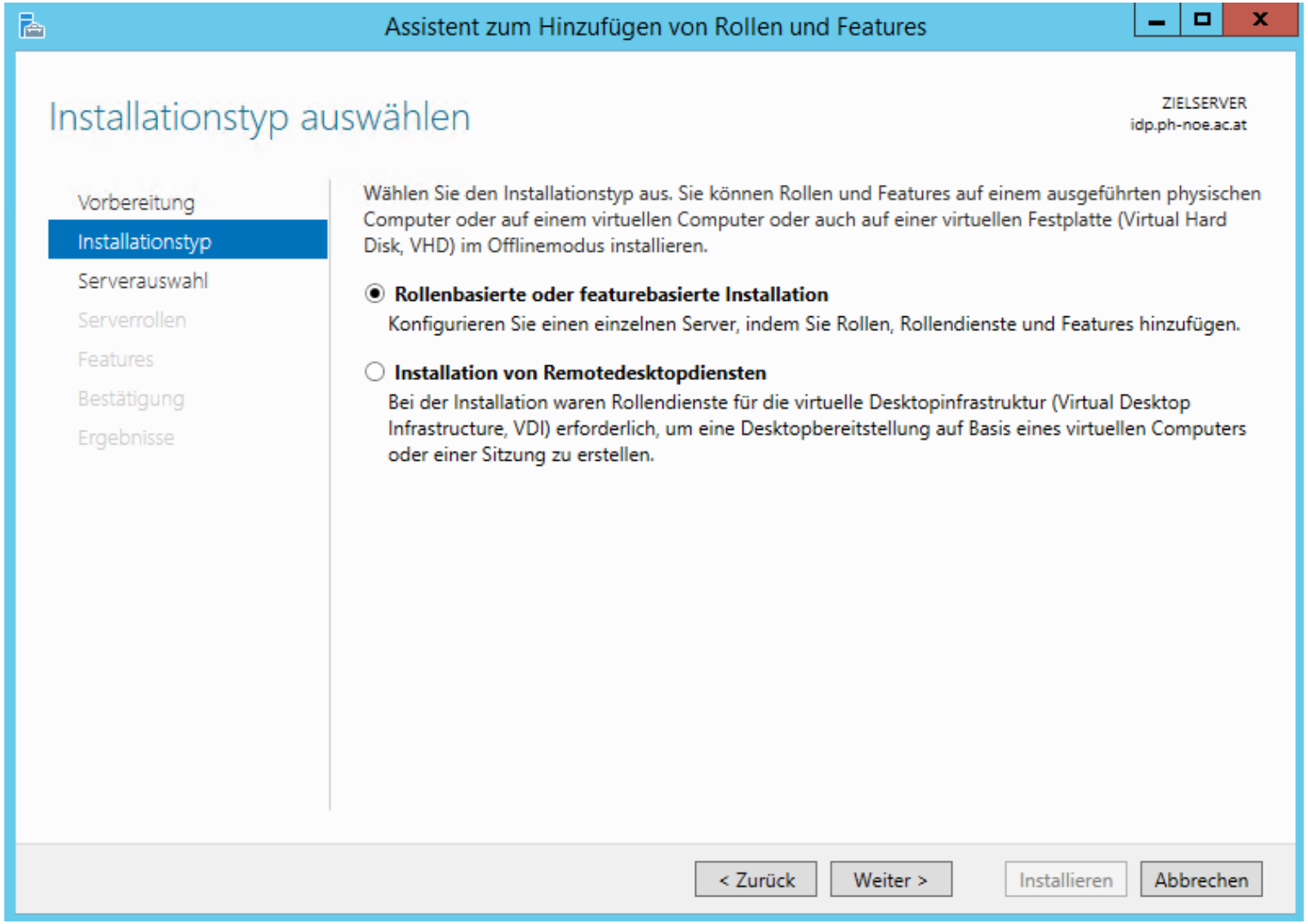
- Shibboleth IDP:
  - https://wiki.univie.ac.at/display/federation/Shibboleth+IDP+3
  - https://wiki.shibboleth.net/confluence/display/SHIB2/IdPConfiguration
- Shibboleth SP:
  - https://wiki.univie.ac.at/display/federation/Shibboleth+SP+2.6
  - https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPConfiguration

Konfiguration von ADFS

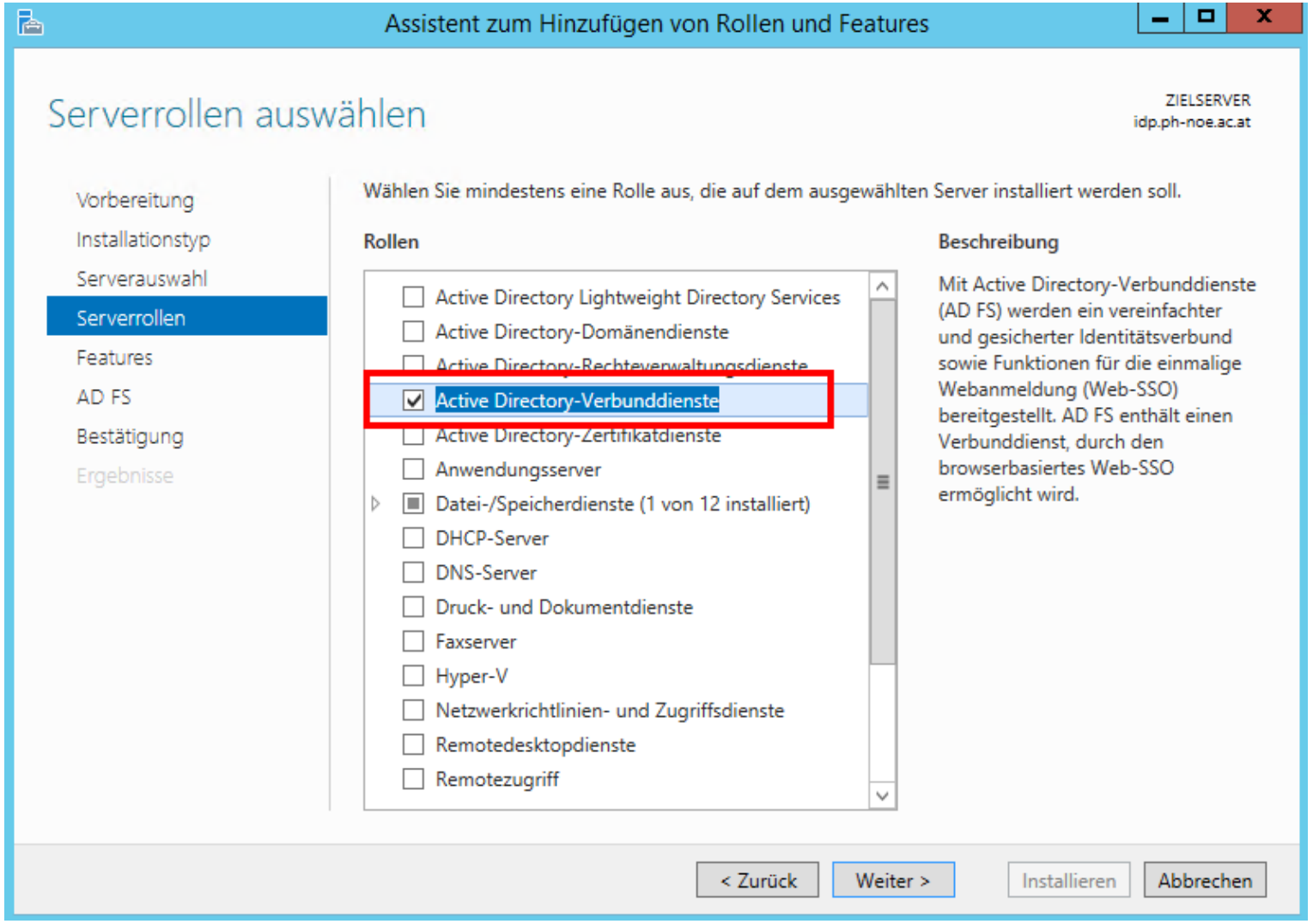
- Zertifikat installieren
  - Zugriff über https => Zertifikat notwendig!
  - ACHTUNG: Rechnername muss im Zertifikat enthalten sein!
  - Beispiel PH NÖ: Wildcard Zertifikat *.ph-noe.ac.at

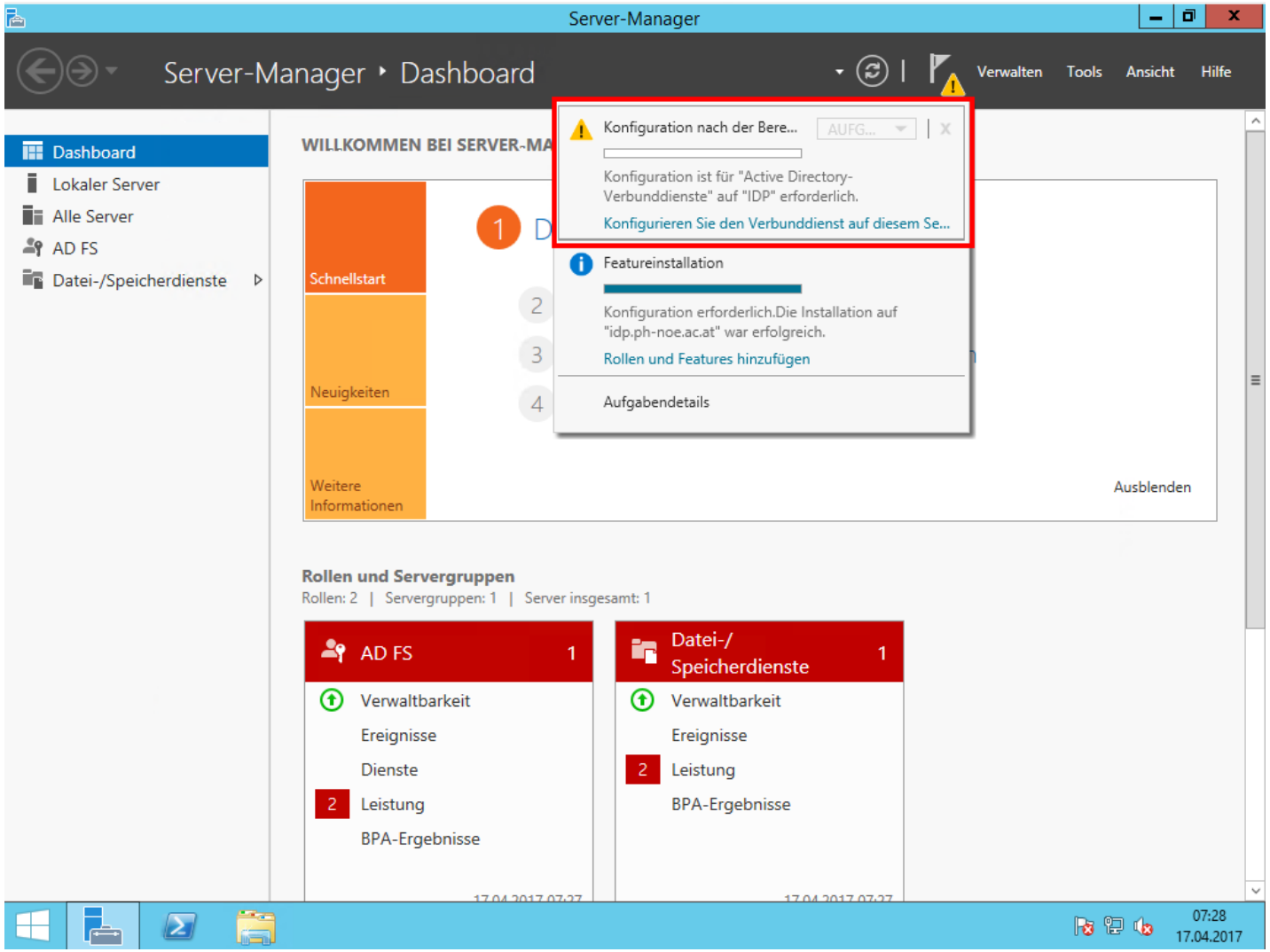


ADFS Rolle installieren

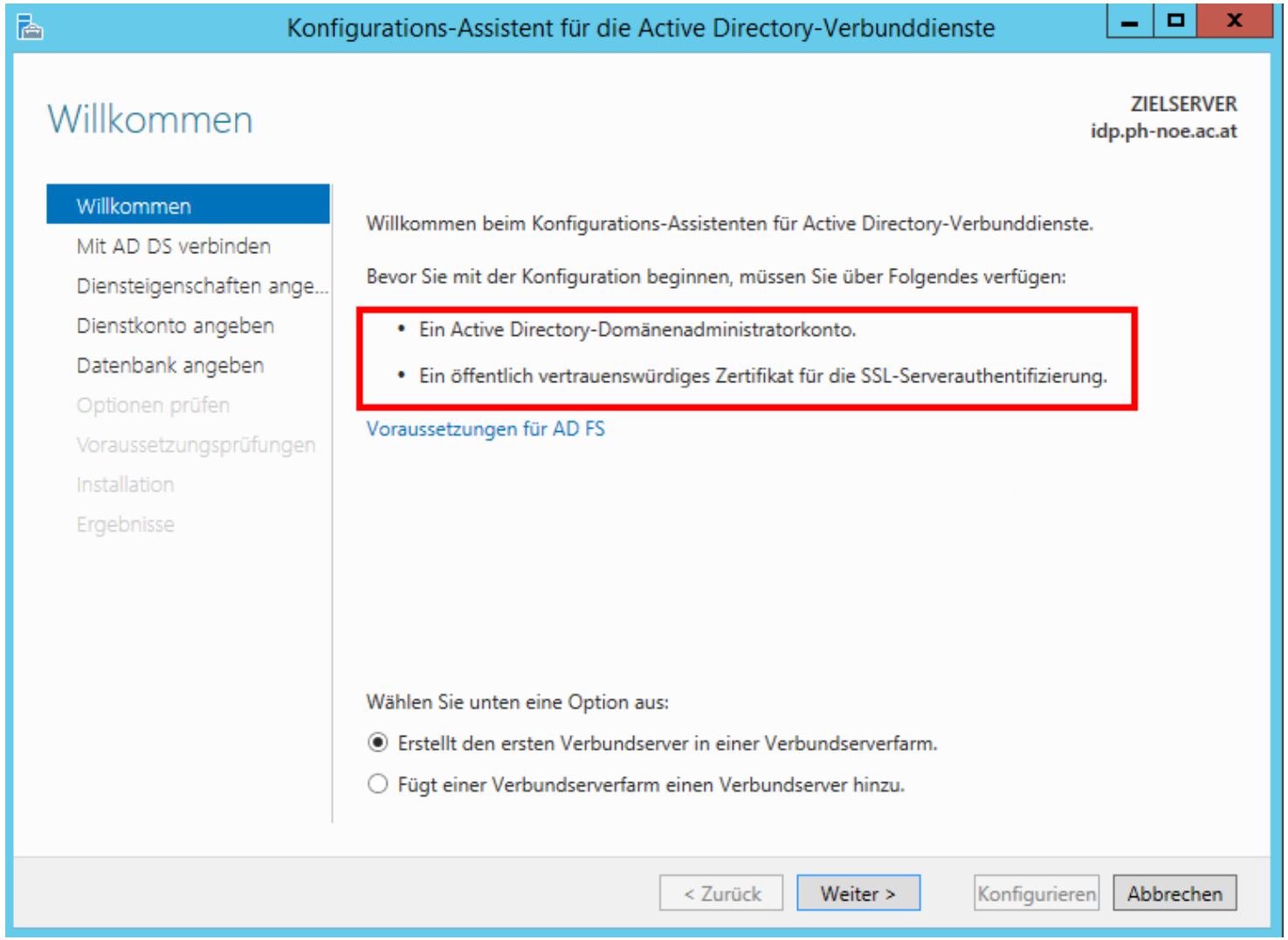


ADFS Rolle installieren

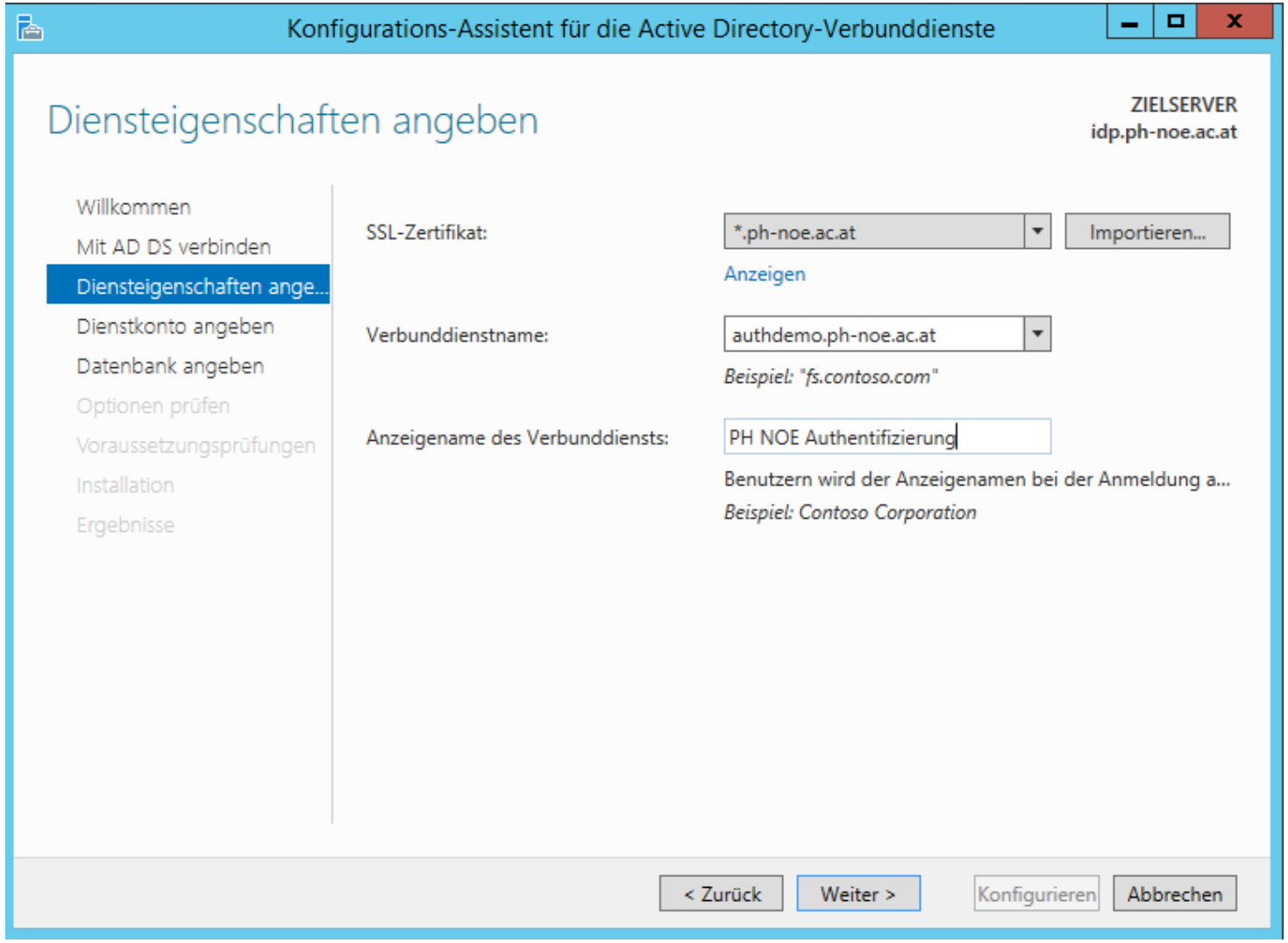



Server-Manager
Server-Manager ▸ Dashboard
Verwalten
Tools
Ansicht
Hilfe
Dashboard
Lokaler Server
Alle Server
AD FS
Datei-/Speicherdienste
WILLKOMMEN BEI SERVER-MA
Konfiguration nach der Bere...
AUFG...
Konfiguration ist für "Active Directory-Verbunddienste" auf "IDP" erforderlich.
Konfigurieren Sie den Verbunddienst auf diesem Se...
Featureinstallation
Konfiguration erforderlich.Die Installation auf "idp.ph-noe.ac.at" war erfolgreich.
Rollen und Features hinzufügen
Aufgabendetails
Schnellstart
Neuigkeiten
Weitere Informationen
Ausblenden
Rollen und Servergruppen
Rollen: 2 | Servergruppen: 1 | Server insgesamt: 1
AD FS
1
Verwaltbarkeit
Ereignisse
Dienste
2
Leistung
BPA-Ergebnisse
Datei-/ Speicherdienste
1
Verwaltbarkeit
Ereignisse
2
Leistung
BPA-Ergebnisse
07:28
17.04.2017

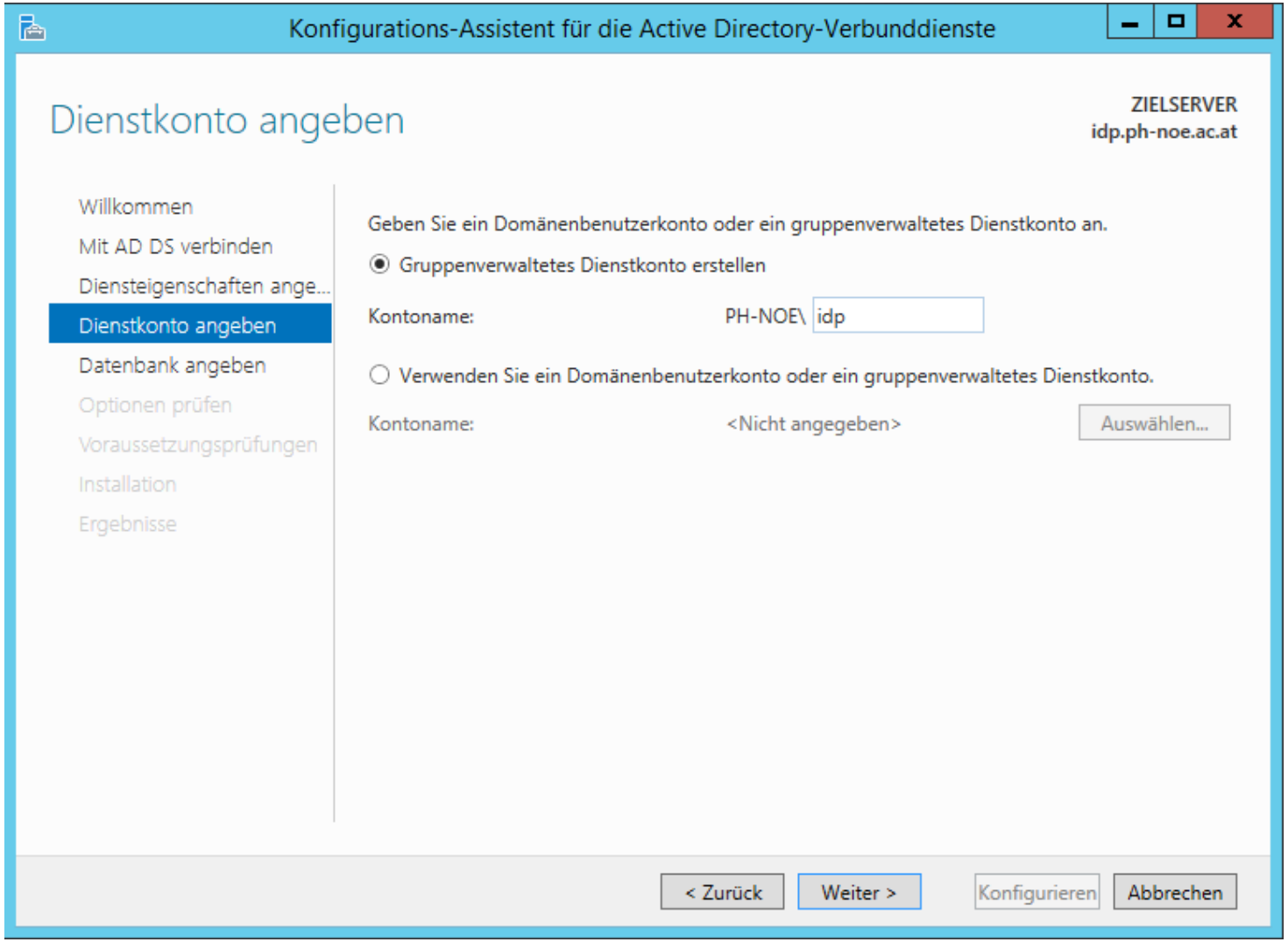
ADFS Konfiguration



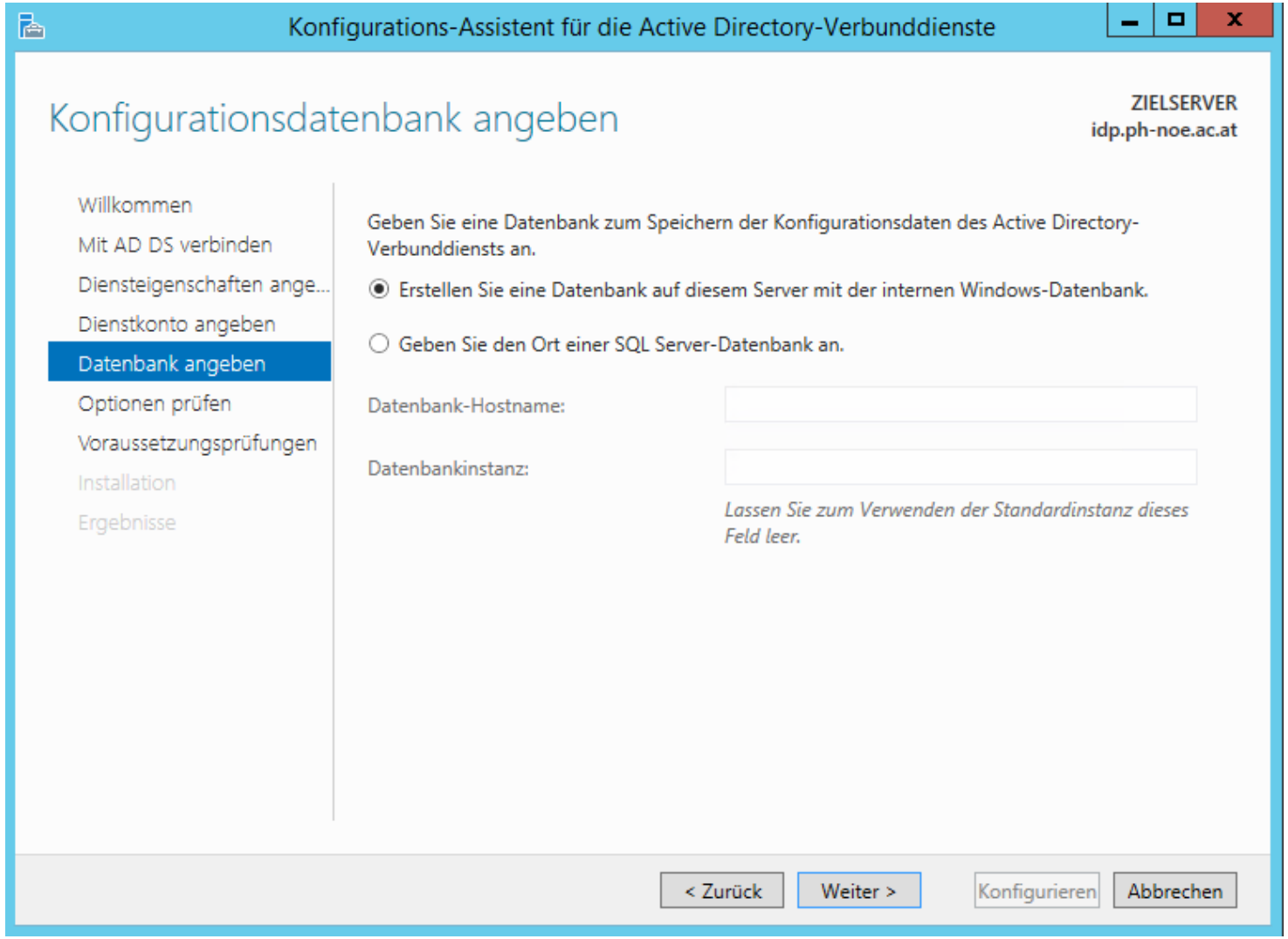
ADFS Konfiguration



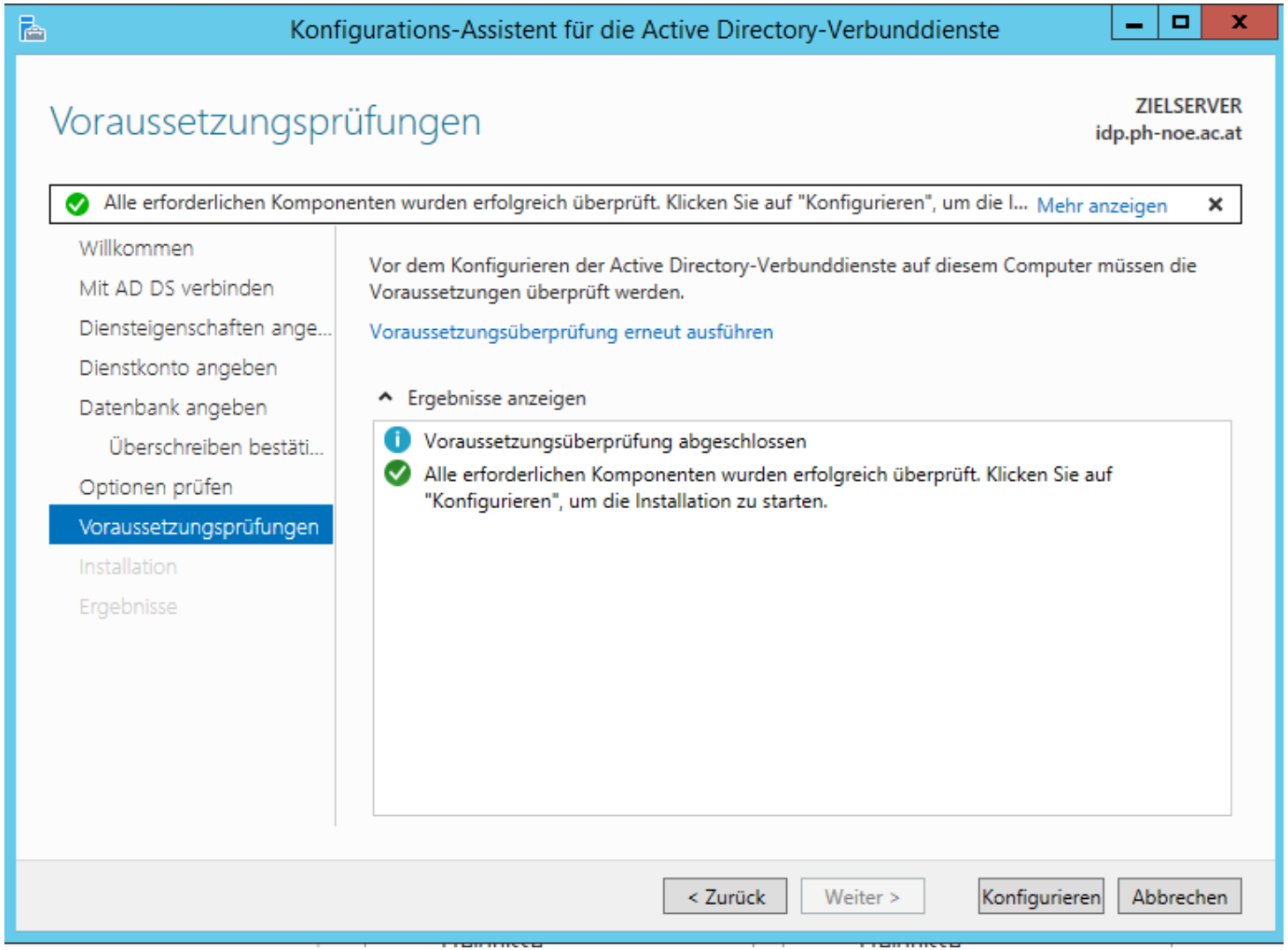
ADFS Konfiguration



ADFS Konfiguration



ADFS Konfiguration



ADFS Test

- https://<SERVERURL>/adfs/ls/idpinitiatedsignon
  - TestLogin

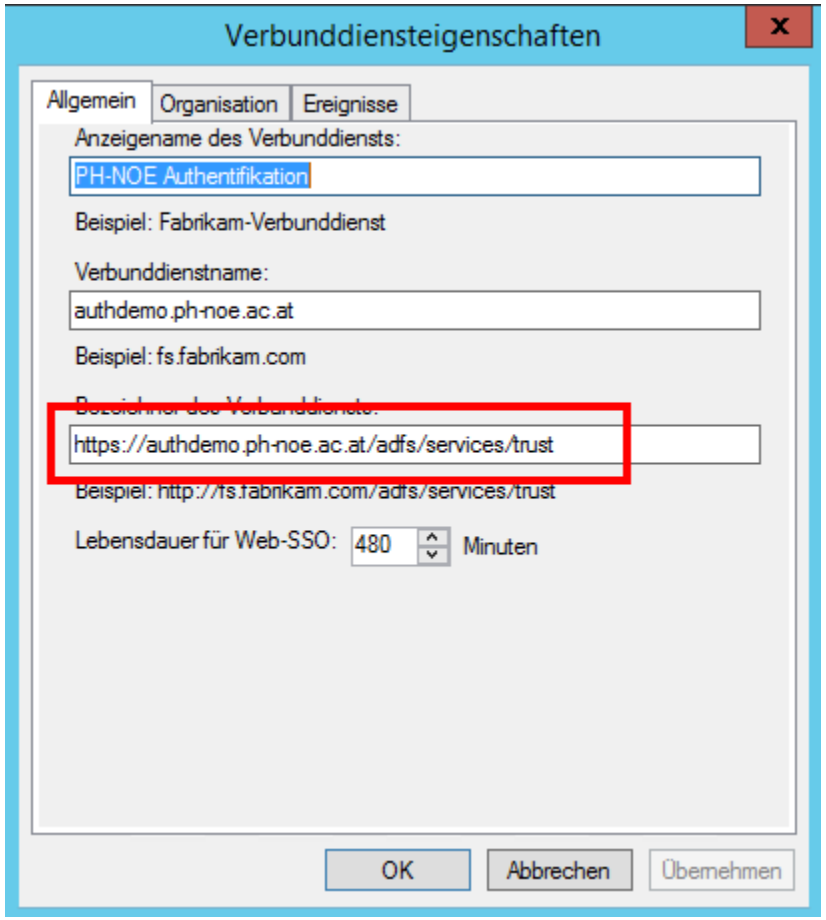
- https://<SERVERURL>/FederationMetadata/2007-06/FederationMetadata.xml
  - Liefert Metadaten des IDP

- https://<SERVERURL>/adfs/portal/updatepassword/
  - URL für Passwortänderung
  - muss aktiviert werden

ADFS Konfiguration

- Set-AdfsWebTheme -TargetName default -Logo @{path="c:\Contoso\logo.png"}
- Set-AdfsGlobalWebContent –CompanyName "Contoso Corp„
- Set-AdfsWebTheme -TargetName default -Illustration @{path="c:\Contoso\illustration.png"}

ADFS Konfiguration



Shibboleth – SP installieren

- https://wiki.shibboleth.net/confluence/display/SHIB2/Installation

- unter Linux: (Ubuntu)
  - https://www.switch.ch/aai/docs/shibboleth/SWITCH/latest/sp/deployment/?os=ubuntu

- Windows:
  - https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPWindowsInstall

Shibboleth – SP installieren

- Zeitsynchronisation:
  - apt install ntp
  - service ntp status
  - ev. /etc/ntp.conf bearbeiten
  - ntpq --peers

```
# Use servers from the NTP Pool Project. Approved by Ubuntu Technical Board
# on 2011-02-08 (LP: #104525). See http://www.pool.ntp.org/join.html for
# more information.
server 192.168.1.100
#pool 0.ubuntu.pool.ntp.org iburst
#pool 1.ubuntu.pool.ntp.org iburst
#pool 2.ubuntu.pool.ntp.org iburst
#pool 3.ubuntu.pool.ntp.org iburst
```

Shibboleth – SP installieren

- Download Repository Key
  - curl -O http://pkg.switch.ch/switchaai/SWITCHaai-swdistrib.asc
- Verify Repository Key
  - gpg --with-fingerprint SWITCHaai-swdistrib.asc
  - → 294E 37D1 5415 6E00 FB96 D7AA 26C3 C469 15B7 6742
- Add Repository Key
  - apt-key add SWITCHaai-swdistrib.asc
- Add Repository
  - echo 'deb http://pkg.switch.ch/switchaai/ubuntu xenial main' | sudo tee /etc/apt/sources.list.d/SWITCHaai-swdistrib.list > /dev/null

Shibboleth – SP installieren

- apt-get update
- apt-get install --install-recommends shibboleth

- Test:
  - shibd -t → *…overall configuration is loadable,…??*
  - apache2ctl configtest → *Syntax OK ??*
  - service apache2 restart
  - https://ServerURL/Shibboleth.sso/Session
    → *A valid session was not found. ??*

Shibboleth – SP Verzeichnisse

- /etc/shibboleth
  - Configuration directory of Shibboleth. The main configuration file is shibboleth2.xml.
- /var/log/shibboleth
  - Log directory where logs are written to. The most important log file is the shibd.log file that should be consulted in case of problems.
- /var/run/shibboleth
  - Runtime directory where process ID and socket files are stored.
- /var/cache/shibboleth
  - Cache directory where metadata backup and CRL files are stored.
- /etc/init.d
  - Init script directory where the startup script for the shibd daemon is stored.

Shibboleth – SP Zertifikate

- shib-keygen -f -u _shibd -h yourhost.example.org -y 3 -e https://yourhost.example.org/shibboleth -o /etc/shibboleth/
  - shib-keygen -f -u _shibd -h moodledemo.ph-noe.ac.at -y 3 -e https:// moodledemo.ph-noe.ac.at/shibboleth -o /etc/shibboleth/
  - → /etc/shibboleth/sp-cert.pem
  - → /etc/shibboleth/sp-key.pem

Shibboleth – SP konfigurieren

- /etc/shibboleth/shibboleth2.xml

```
<!-- The ApplicationDefaults element is where most of Shibboleth's SAML bits are defined. -->
<ApplicationDefaults entityID="https://moodledemo.ph-noe.ac.at/shibboleth"
                     REMOTE_USER="eppn persistent-id targeted-id"
                     cipherSuites="ECDHE+AESGCM:ECDHE:!aNULL:!eNULL:!LOW:!EXPORT:!RC4:!SHA:!SSLv2">

    <!--
    Controls session lifetimes, address checks, cookie handling, and the protocol handlers.
    You MUST supply an effectively unique handlerURL value for each of your applications.
    The value defaults to /Shibboleth.sso, and should be a relative path, with the SP computing
    a relative value based on the virtual host. Using handlerSSL="true", the default, will force
    the protocol to be https. You should also set cookieProps to "https" for SSL-only sites.
    Note that while we default checkAddress to "false", this has a negative impact on the
    security of your site. Stealing sessions via cookie theft is much easier with this disabled.
    -->
    <Sessions lifetime="28800" timeout="3600" relayState="ss:mem"
              checkAddress="false" handlerSSL="true" cookieProps="https">

        <!--
```

Shibboleth – SP konfigurieren

- /etc/shibboleth/shibboleth2.xml → IDP Verbindung
- (Übereinstimmung mit Metadaten des IDP!!)

```
Configures SSO for a default IdP. To allow for >1 IdP, remove
entityID property and adjust discoveryURL to point to discovery service.
(Set discoveryProtocol to "WAYF" for legacy Shibboleth WAYF support.)
You can also override entityID on /Login query string, or in RequestMap/htaccess.
-->
<SSO entityID="https://authdemo.ph-noe.ac.at/adfs/services/trust"
     discoveryProtocol="SAMLDS" discoveryURL="https://ds.example.org/DS/WAYF">
  SAML2 SAML1
</SSO>

<!-- SAML and local-only logout. -->
<Logout>SAML2 Local</Logout>

<!-- Extension service that generates "approximate" metadata based on SP configuration. -->
<Handler type="MetadataGenerator" Location="/Metadata" signing="false"/>
```

Shibboleth – SP konfigurieren

- /etc/shibboleth/shibboleth2.xml → Metadaten des IDP

```
<MetadataProvider type="XML" validate="false"
  uri="https://authdemo.ph-noe.ac.at/FederationMetadata/2007-06/FederationMetadata.xml"
        backingFilePath="federation-metadata.xml" reloadInterval="7200">
          <MetadataFilter type="RequireValidUntil" maxValidityInterval="2419200"/>
      <MetadataFilter type="Signature" certificate="fedsigner.pem"/>
      <DiscoveryFilter type="Blacklist" matcher="EntityAttributes" trimTags="true"
        attributeName="http://macedir.org/entity-category"
        attributeNameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
        attributeValue="http://refeds.org/category/hide-from-discovery" />-->
</MetadataProvider>
```

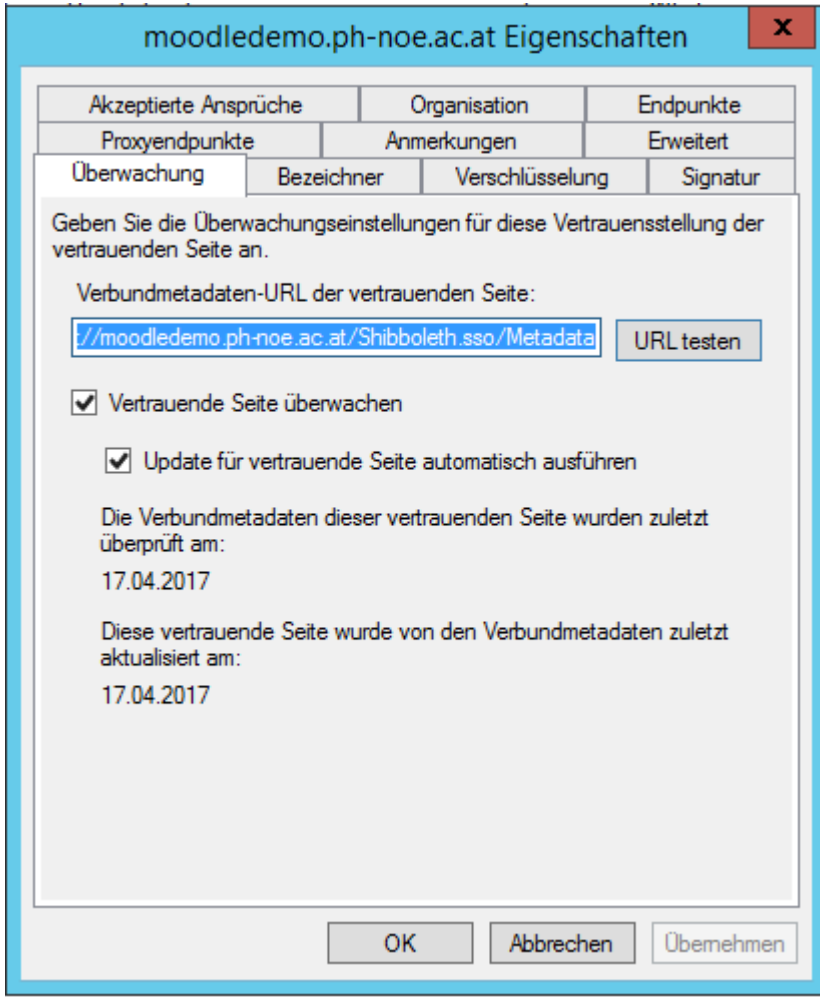
Shibboleth – SP konfigurieren

- /etc/shibboleth/attribute-map.xml → LDAP Attribute aktivieren!

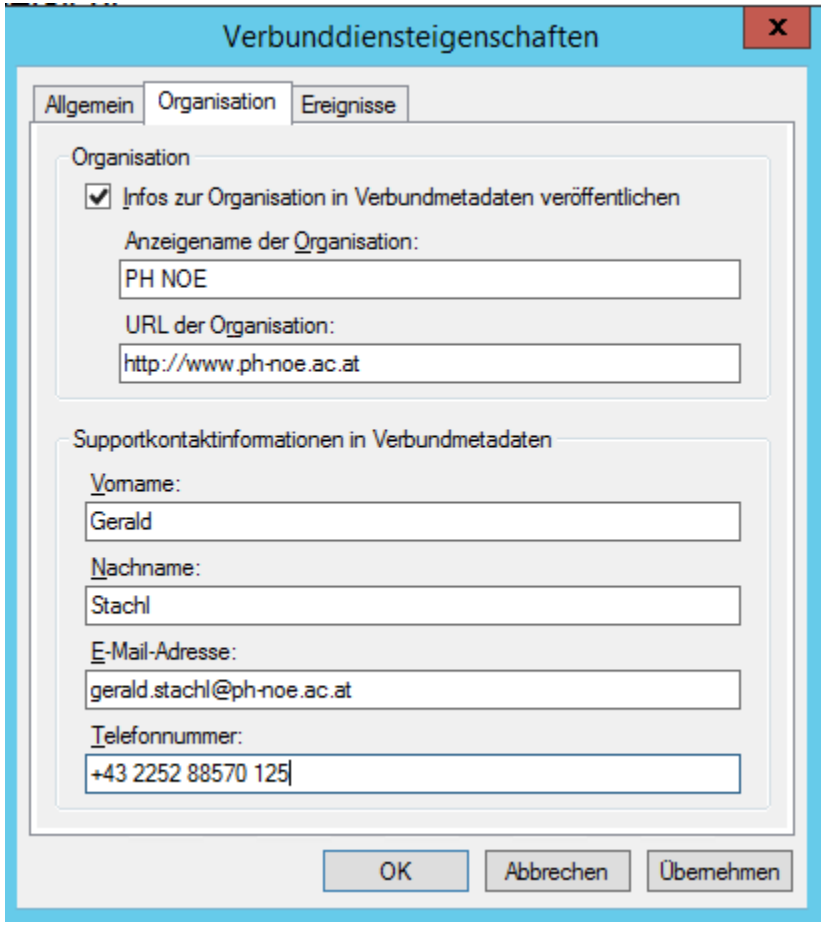
```
<!-- Examples of LDAP-based attributes, uncomment to use these... -->
<Attribute name="urn:oid:2.5.4.3" id="cn"/>
<Attribute name="urn:oid:2.5.4.4" id="sn"/>
<Attribute name="urn:oid:2.5.4.42" id="givenName"/>
<Attribute name="urn:oid:2.16.840.1.113730.3.1.241" id="displayName"/>
<Attribute name="urn:oid:0.9.2342.19200300.100.1.1" id="uid"/>
<Attribute name="urn:oid:0.9.2342.19200300.100.1.3" id="mail"/>
<Attribute name="urn:oid:2.5.4.20" id="telephoneNumber"/>
<Attribute name="urn:oid:2.5.4.12" id="title"/>
<Attribute name="urn:oid:2.5.4.43" id="initials"/>
<Attribute name="urn:oid:2.5.4.13" id="description"/>
<Attribute name="urn:oid:2.16.840.1.113730.3.1.1" id="carLicense"/>
<Attribute name="urn:oid:2.16.840.1.113730.3.1.2" id="departmentNumber"/>
<Attribute name="urn:oid:2.16.840.1.113730.3.1.3" id="employeeNumber"/>
<Attribute name="urn:oid:2.16.840.1.113730.3.1.4" id="employeeType"/>
<Attribute name="urn:oid:2.16.840.1.113730.3.1.39" id="preferredLanguage"/>
<Attribute name="urn:oid:0.9.2342.19200300.100.1.10" id="manager"/>
<Attribute name="urn:oid:2.5.4.34" id="seeAlso"/>
<Attribute name="urn:oid:2.5.4.23" id="facsimileTelephoneNumber"/>
<Attribute name="urn:oid:2.5.4.9" id="street"/>
```

ADFS Konfiguration - Metadaten

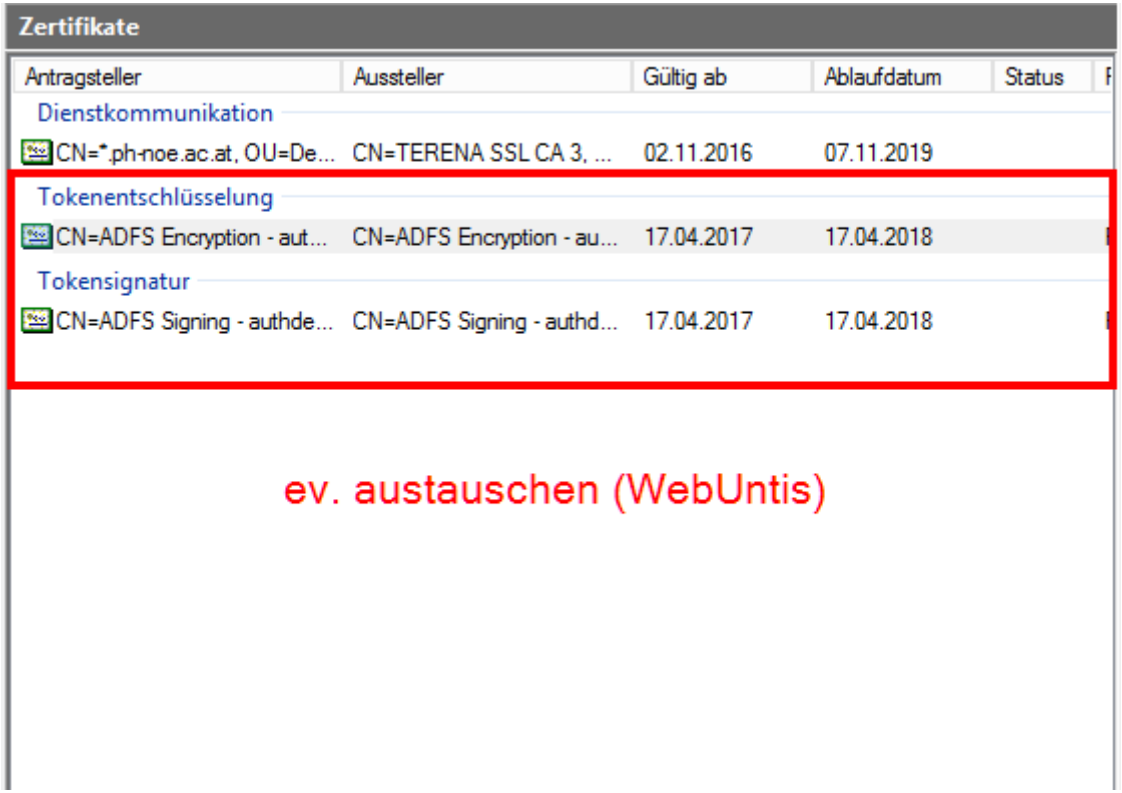
- Metadaten des „vertrauenswürdigen“ ServiceProviders importieren:
- z.B. per URL:
  - https://moodledemo.ph-noe.ac.at/Shibboleth.sso/Metadata



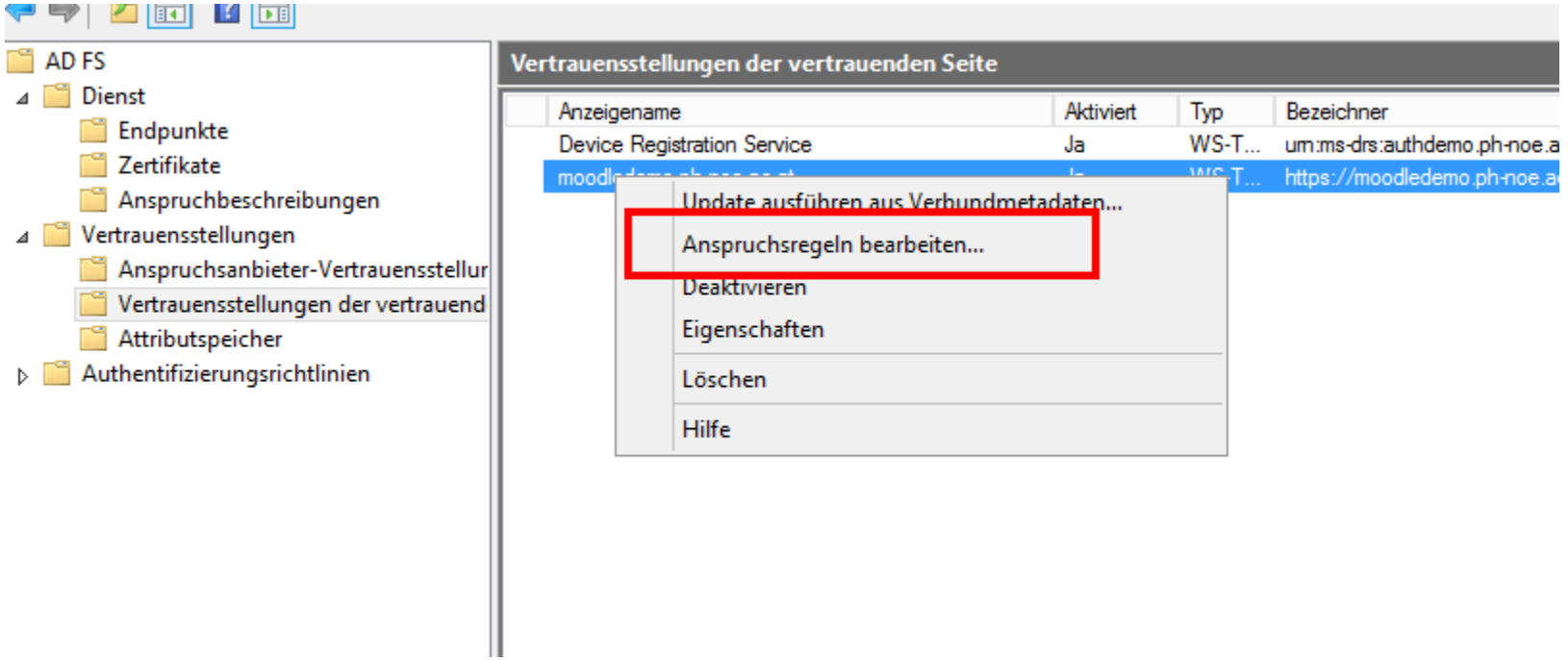
ADFS Konfiguration (optional)



ADFS Konfiguration (optional)

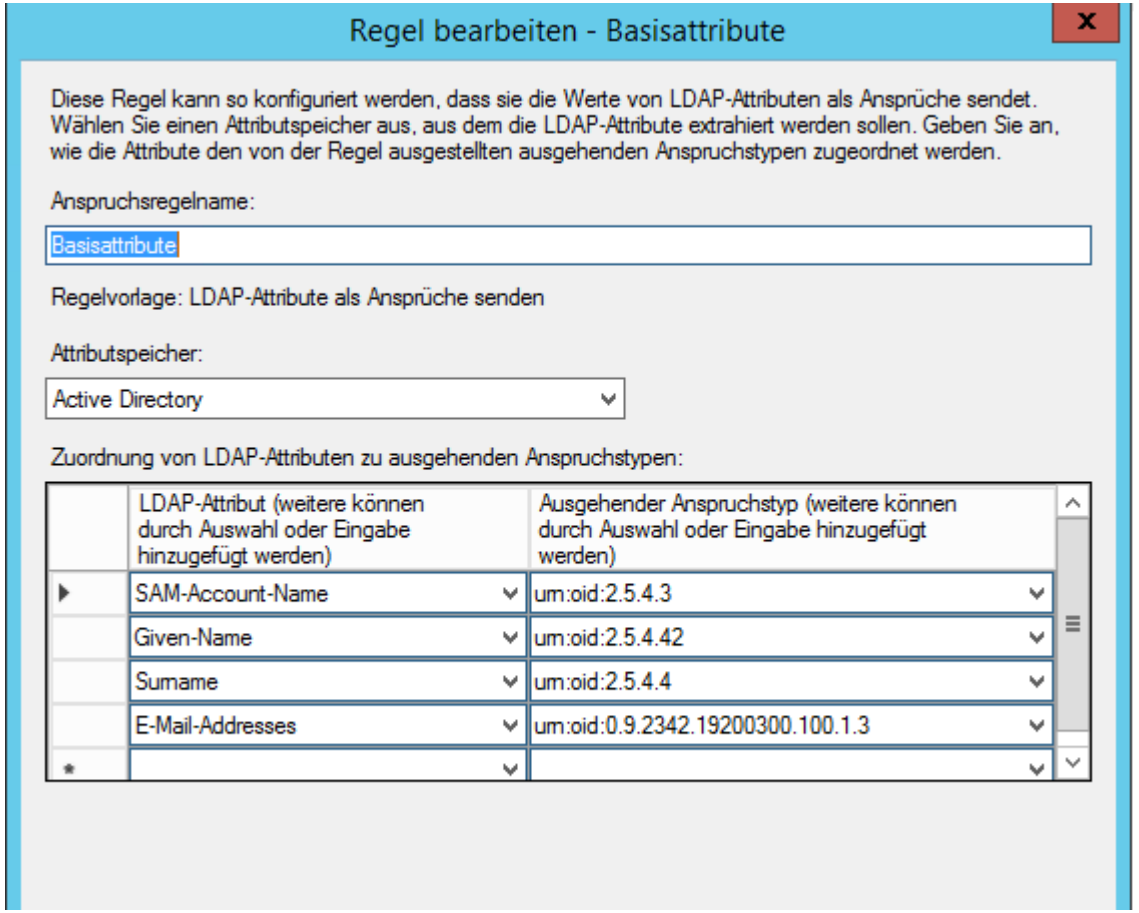


ADFS Konfiguration - Attribute



ADFS - Attribute für Moodle

- Mindestanforderung:
  - LoginName (zwingend notwendig)
  - Vorname
  - Nachname
  - Email
- wenn ein Attribut fehlt → Redirect auf Profil-Seite!



SAML Auth in Moodle

- Shibboleth-Authentifizierung für ./auth/shibboleth

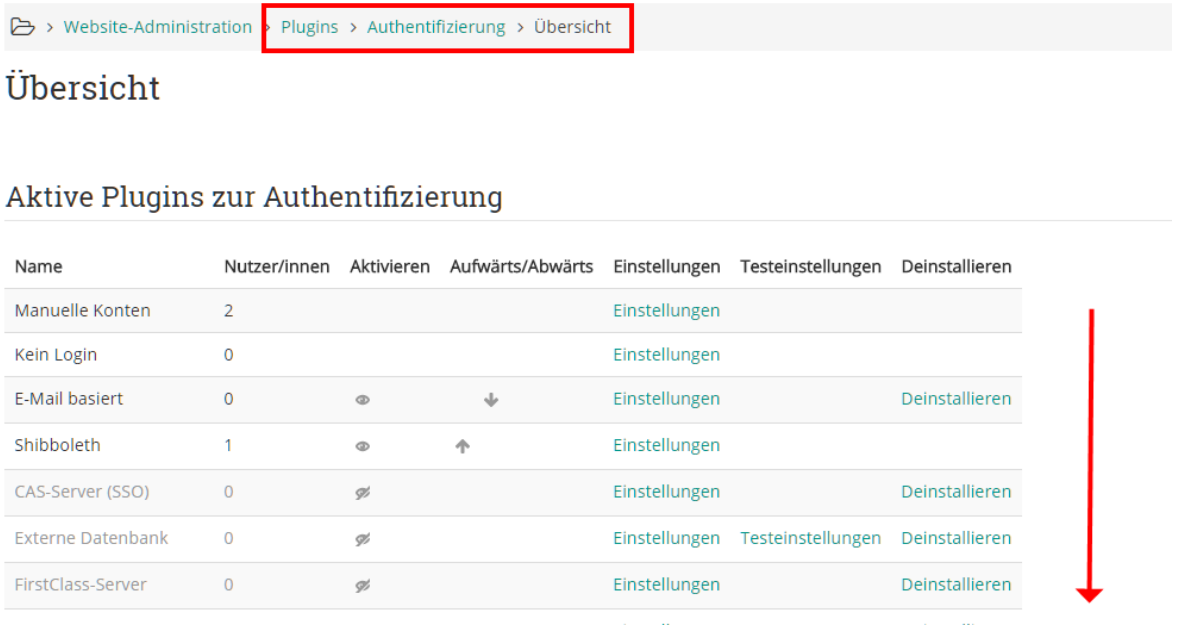
```
<Directory  /var/www/html/auth/shibboleth>
        AuthType shibboleth
        ShibRequireSession On
        require valid-user
</Directory>
```

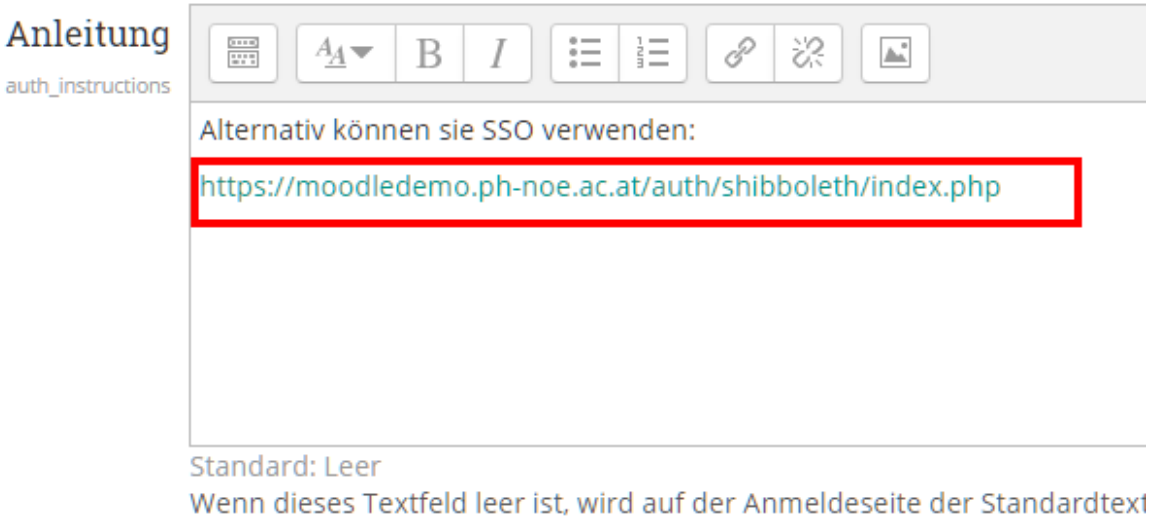
SAML Auth in Moodle

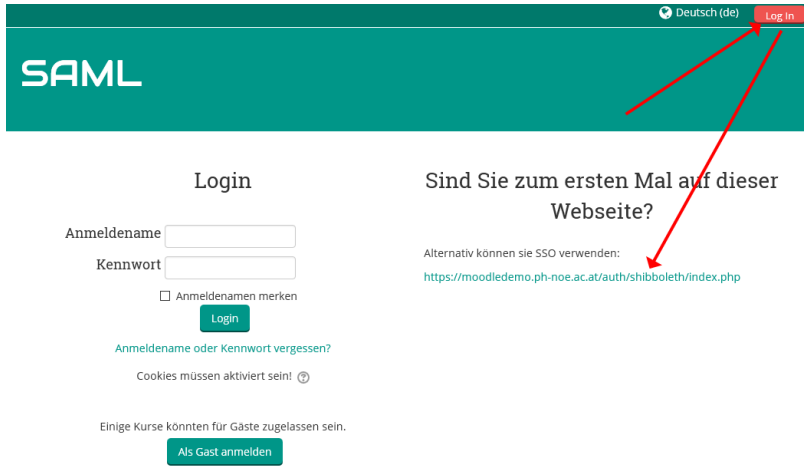
- Shibboleth-Authentifizierung für ./auth/shibboleth

```
<Directory  /var/www/html/auth/shibboleth>
        AuthType shibboleth
        ShibRequireSession On
        require valid-user
</Directory>
```

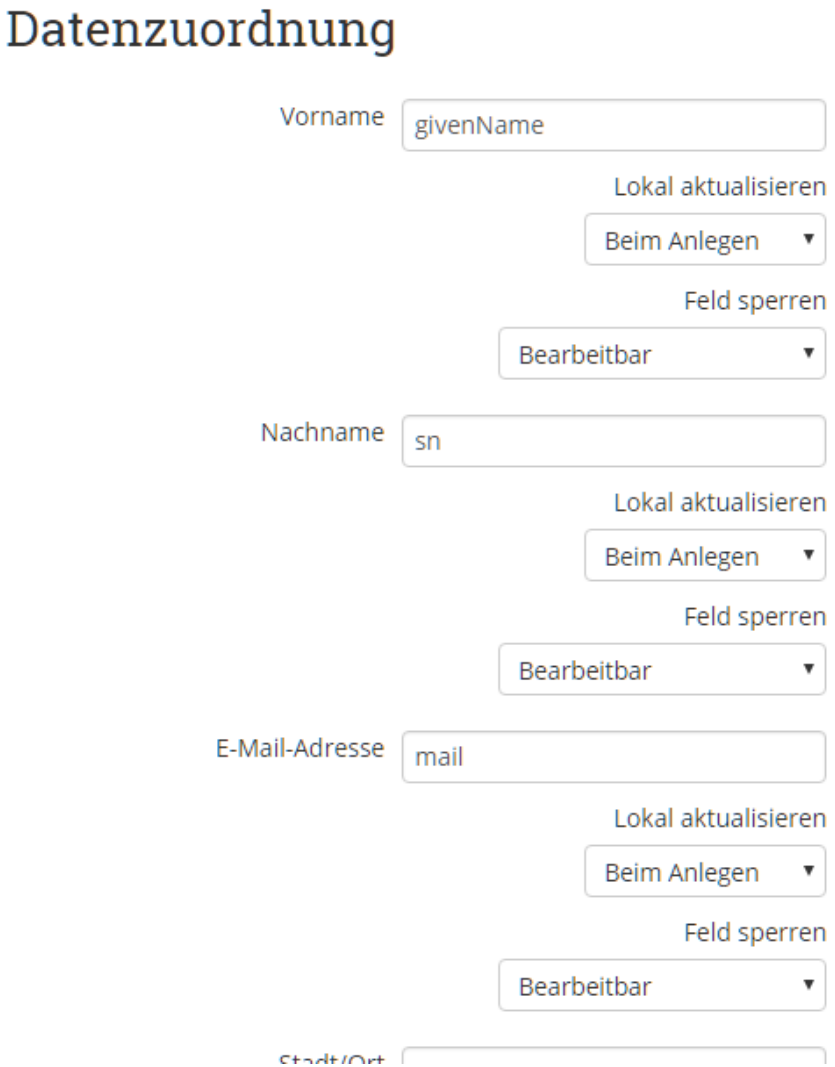
Shibboleth als alternatives Login







Shibboleth in Moodle konfigurieren



Sonderfall: IIS als Webserver

Authentifizierung wird in shibboleth2.xml definiert!

```
<RequestMapper type="Native">
    <RequestMap>
        <!--The example requires a session for documents in /secure on the containing host with http and
        https on the default ports. Note that the name and port in the <Host> elements MUST match
        Apache's ServerName and Port directives or the IIS Site name in the <ISAPI> element above.-->

        <Host name="moodle.bg-bab.ac.at">
                <Path name="auth/shibboleth" authType="shibboleth" requireSession="true" >
                    <AccessControl>
                        <Rule require="valid-user"/>
                    </AccessControl>
                </Path>
        </Host>

        <!--Example of a second vhost mapped to a different applicationId.-->
        <!--<Host name="admin.example.org" applicationId="admin" authType="shibboleth"
        requireSession="true"/>-->
    </RequestMap>
</RequestMapper>
```

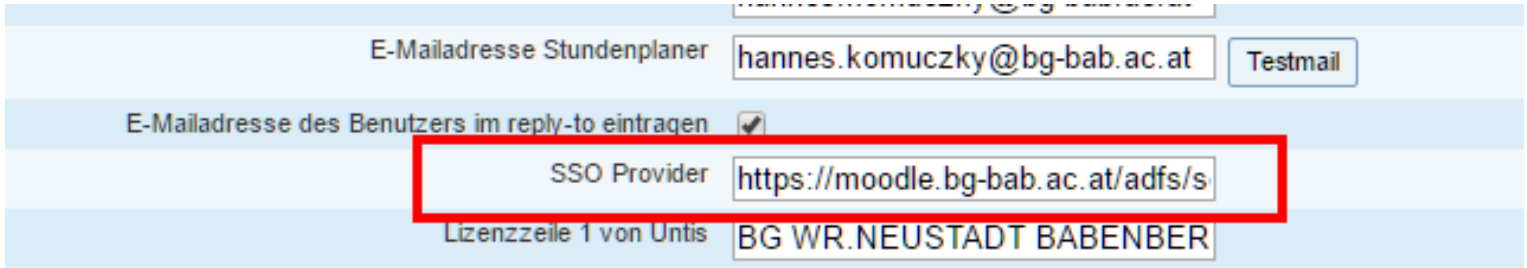
Sonderfall: IIS als Webserver

Variable mit HTTP_....

SAML Auth für WebUntis

- Metadatenaustausch mit Gruber&Peters
- Instanz muss auf hepta (=SP) liegen:
  - https://hepta.webuntis.com/WebUntis/index.do#main

- SSO Provider (IDP) in Administration → Einstellungen:



SAML Auth für WebUntis

Integration

Untis | SAML | Office365 | Sokrates | Smartschool

Allgemeine Einstellungen

SAML Mail Attribut	urn:oid:0.9.2342.19200300.100.1.3
SAML Benutzergruppe Attribut	urn:oid:1.3.6.1.4.1.5923.1.1.1.1
Mail bei jeder Anmeldung übernehmen	☐
Unbekannten Benutzer nach erfolgreicher Anmeldung anlegen	☑
Anmeldung für nicht identifizierten Benutzer nicht erlauben	☐
Rollenidentifzierung	Attribut
SAML Personenrolle Attribut	urn:oid:1.3.6.1.4.1.5923.1.1.1.1

Rollenbezogene Einstellungen

	Lehrer	Schüler
Personenrolle	lehrer	schueler
Personenidentifzierung	Einzelattribut	Einzelattribut
SAML ID Attribut	urn:oid:2.5.4.3	urn:oid:2.5.4.3
Elementdaten ID Feld	Kurzname	externKey
Numerischer Vergleich	☐	☑
Groß-/Kleinschreibung ignorieren	☑	☑
Standard-Benutzergruppe	Lehrerkollegium	user

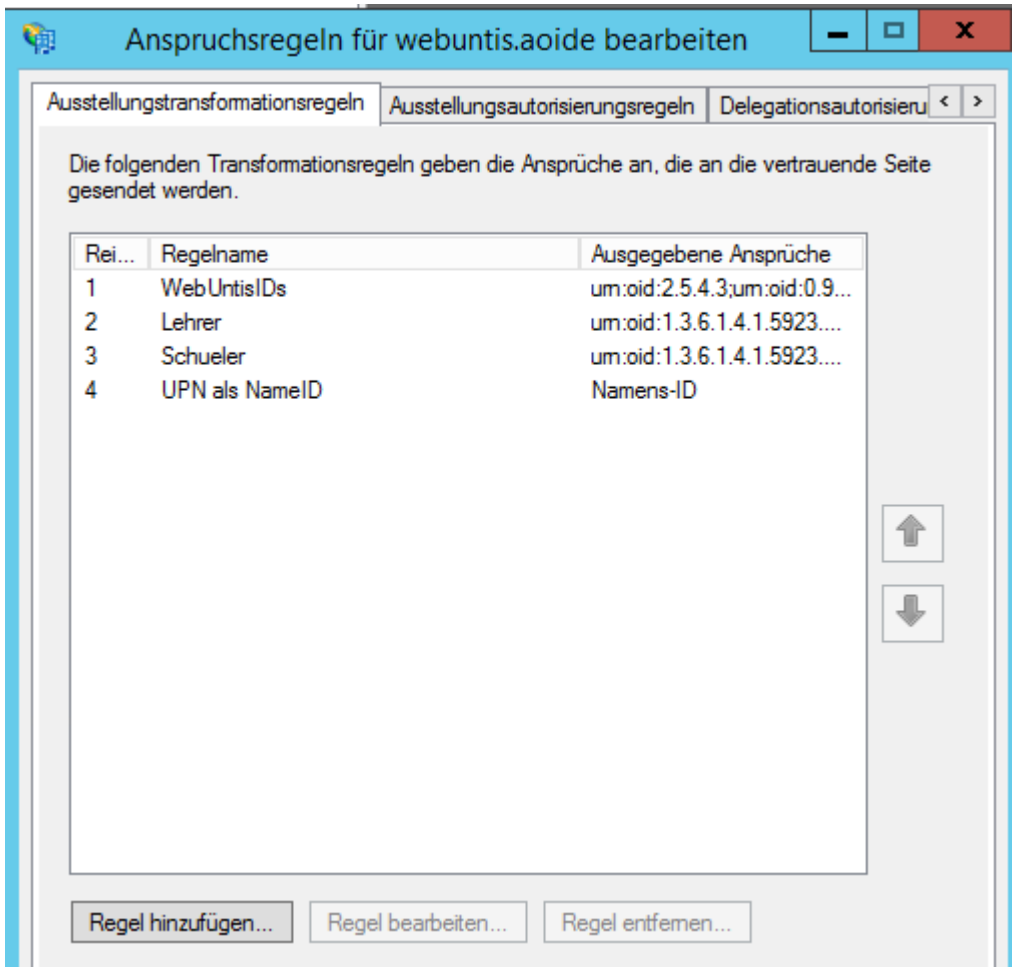
Speichern

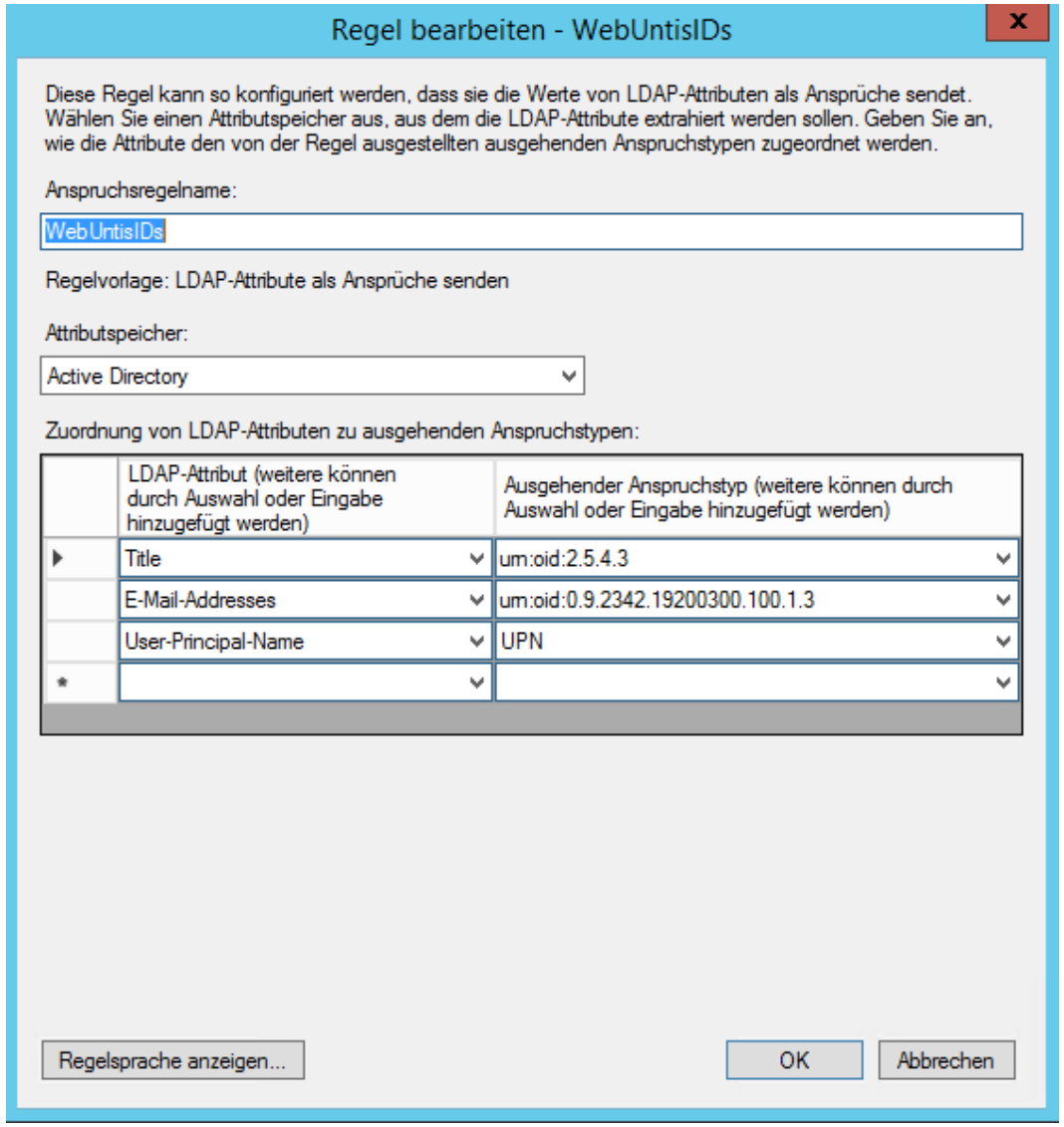
Vorbereitungen AD

- Email-Attribute pflegen
  - Lehrer waren vorhanden
  - Schüler müssen nachgetragen werden (PowerShell)

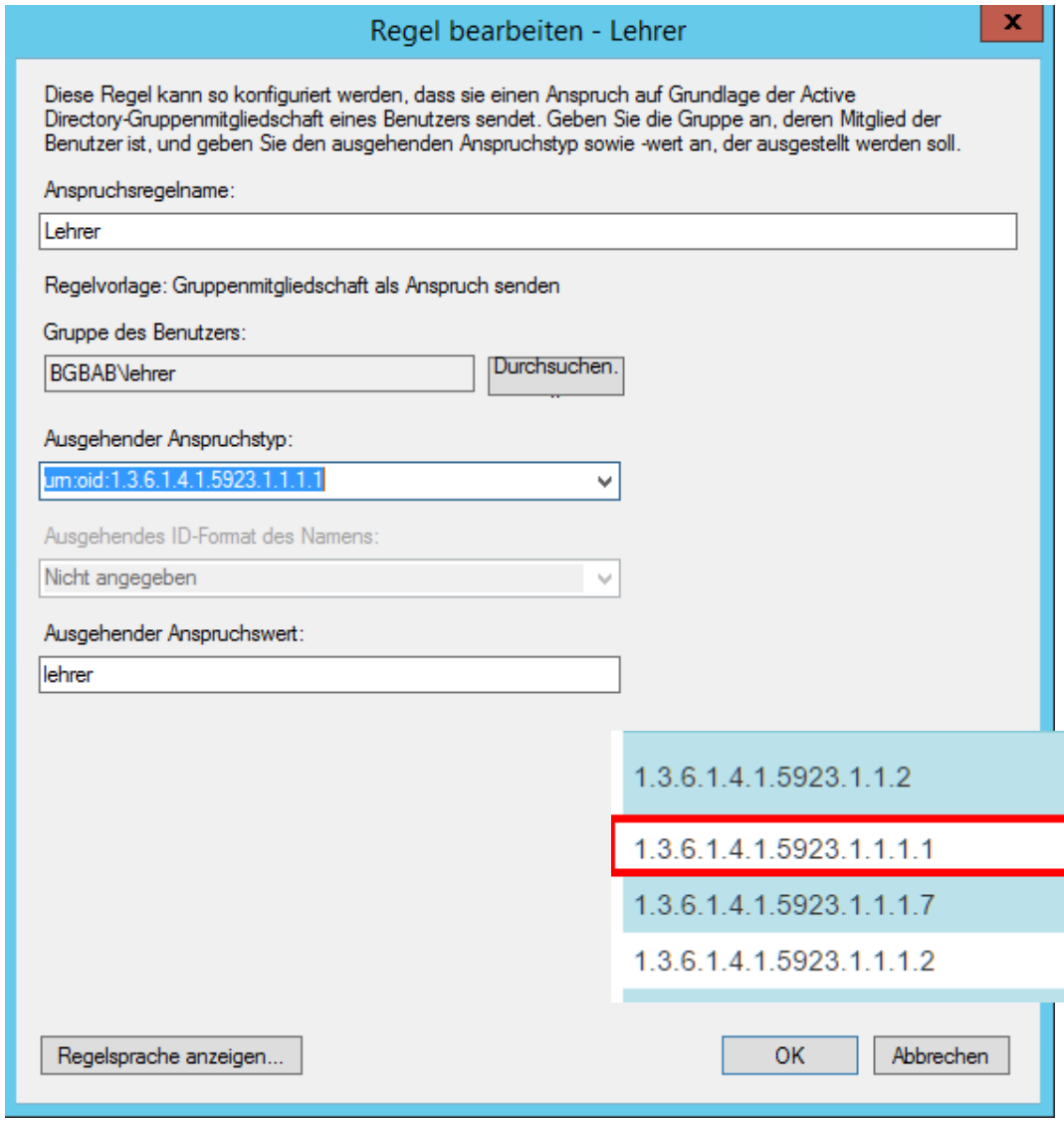
- (bisher nicht verwendetes) Title-Attribut:
  - WebUntis - Kennung für Schüler und Lehrer
  - nur EIN Feld möglich!

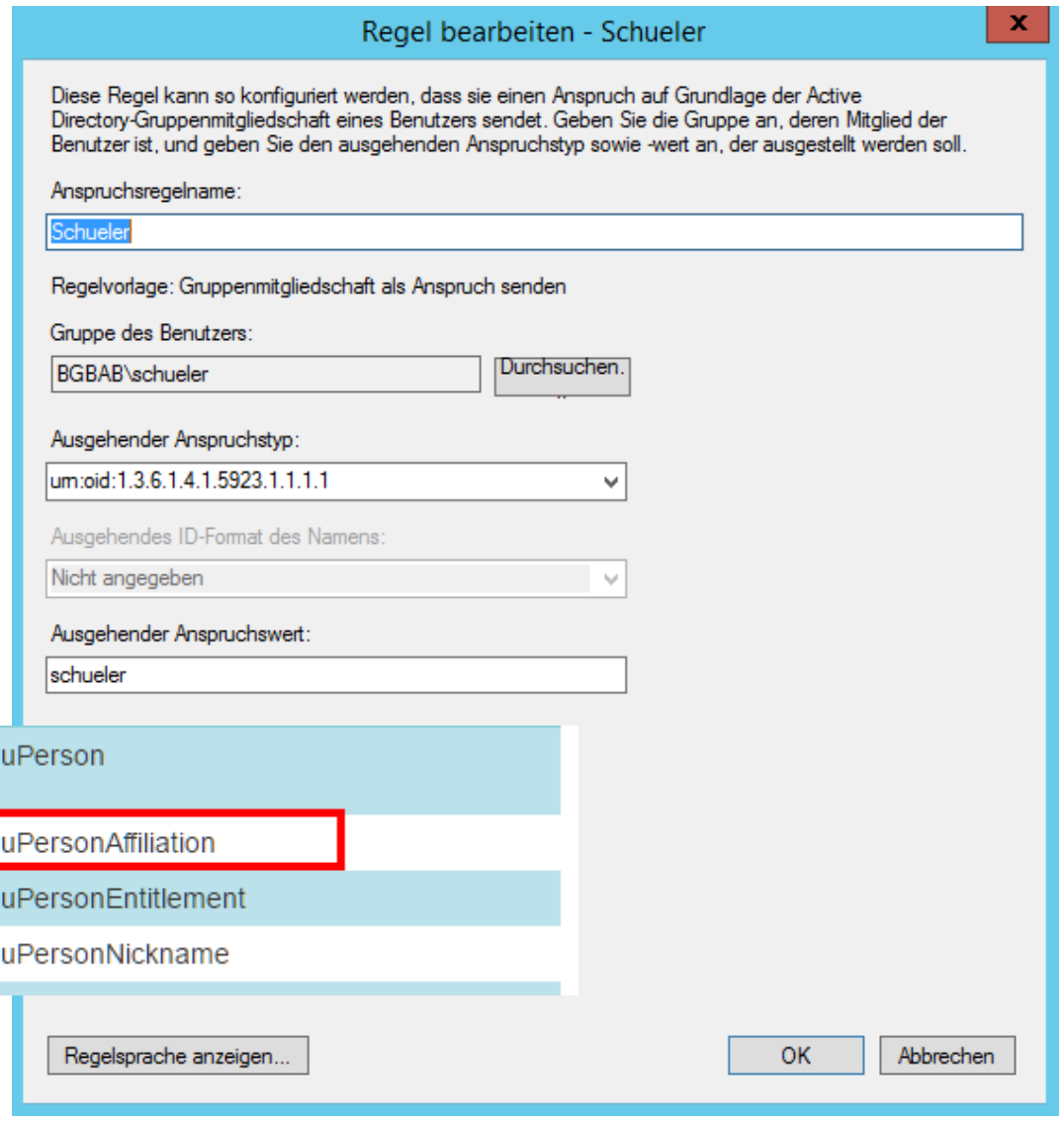
Webuntis Attribute in ADFS





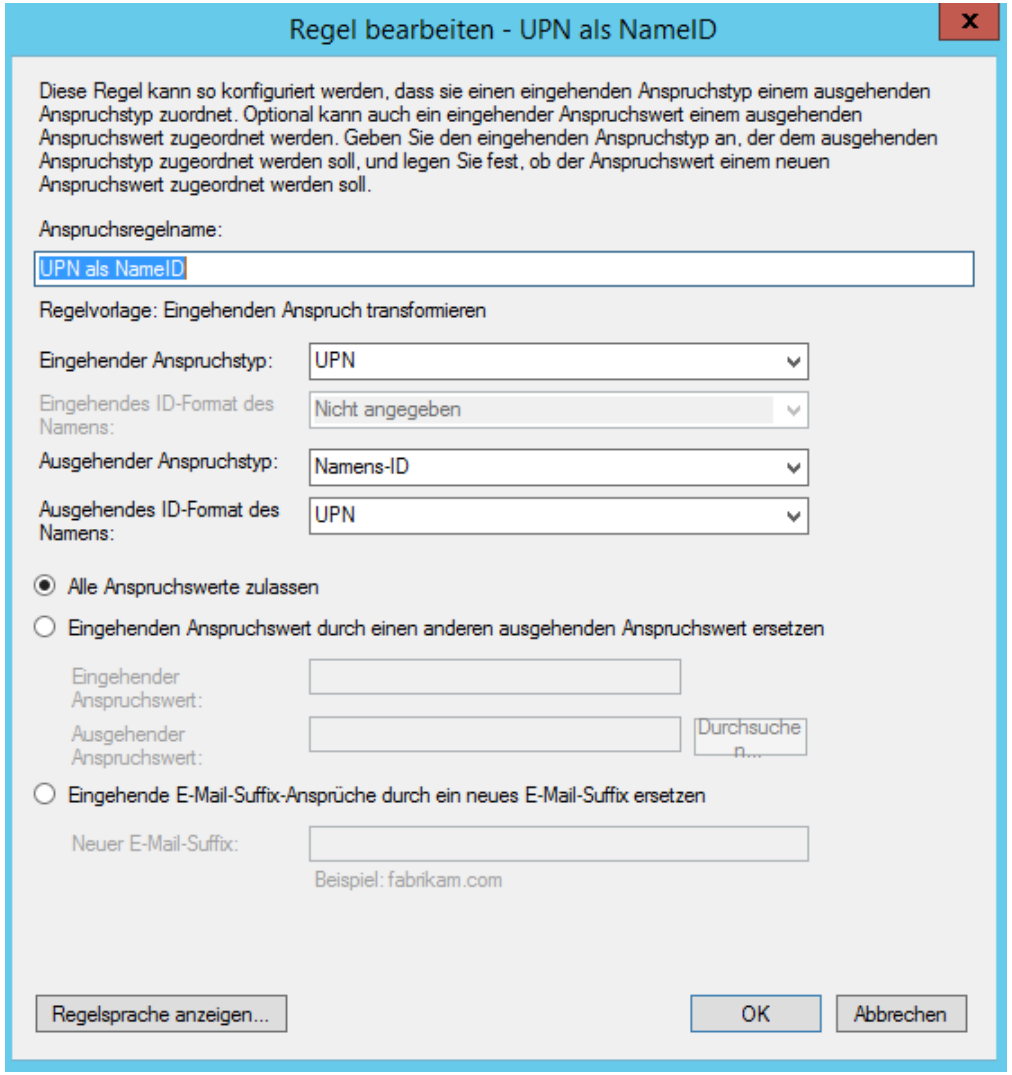
Webuntis Attribute in ADFS



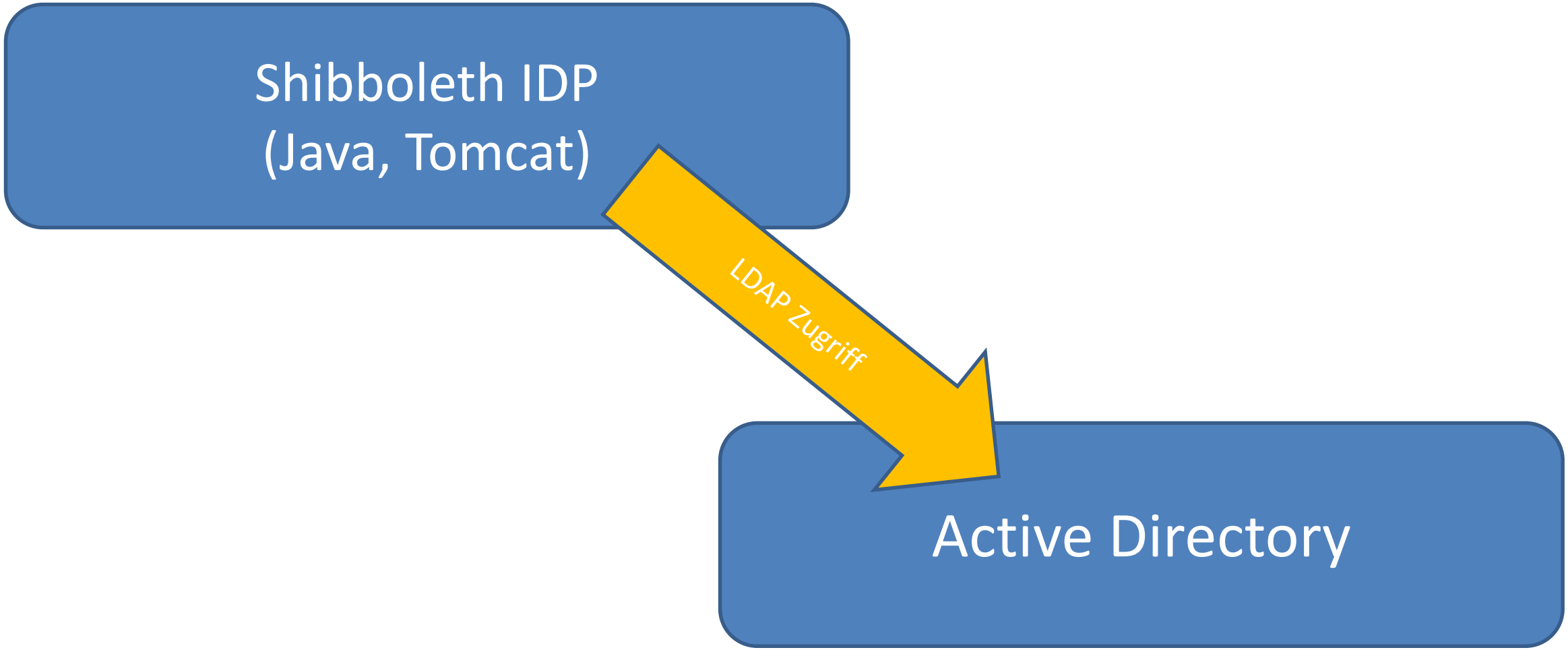


1.3.6.1.4.1.5923.1.1.2	eduPerson
1.3.6.1.4.1.5923.1.1.1.1	eduPersonAffiliation
1.3.6.1.4.1.5923.1.1.1.7	eduPersonEntitlement
1.3.6.1.4.1.5923.1.1.1.2	eduPersonNickname

Webuntis Attribute in ADFS



Shibboleth IDP



LDAP Verbindung in Shibboleth

```
<DataConnector id="ad.phnoe" xsi:type="LDAPDirectory" ldapURL="%{idp.attribute.resolver.LDAP.ldapURL}" principal="%{idp.authn.LDAP.bindDN}" prin
    <FilterTemplate>
        <![CDATA[
            %{idp.attribute.resolver.LDAP.searchFilter}
        ]]>
    </FilterTemplate>
    <ConnectionPool
        minPoolSize="%{idp.pool.LDAP.minSize:3}"
        maxPoolSize="%{idp.pool.LDAP.maxSize:10}"
        blockWaitTime="%{idp.pool.LDAP.blockWaitTime:PT3S}"
        validatePeriodically="%{idp.pool.LDAP.validatePeriodically:true}"
        validateTimerPeriod="%{idp.pool.LDAP.validatePeriod:PT5M}"
        expirationTime="%{idp.pool.LDAP.idleTime:PT10M}"
        failFastInitialize="%{idp.pool.LDAP.failFastInitialize:false}" />
</DataConnector>
```

Standard-Attribute

```
<!-- surname and givenName  -->
<AttributeDefinition id="surname" xsi:type="Simple" sourceAttributeID="sn">
    <Dependency ref="ad.phnoe" />
    <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:sn" encodeType="false" />
    <AttributeEncoder xsi:type="SAML2String" name="urn:oid:2.5.4.4" friendlyName="sn" encodeType="false" />
</AttributeDefinition>

<AttributeDefinition id="givenName" xsi:type="Simple" sourceAttributeID="givenName">
    <Dependency ref="ad.phnoe" />
    <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:givenName" encodeType="false" />
    <AttributeEncoder xsi:type="SAML2String" name="urn:oid:2.5.4.42" friendlyName="givenName" encodeType="false" />
</AttributeDefinition>
```

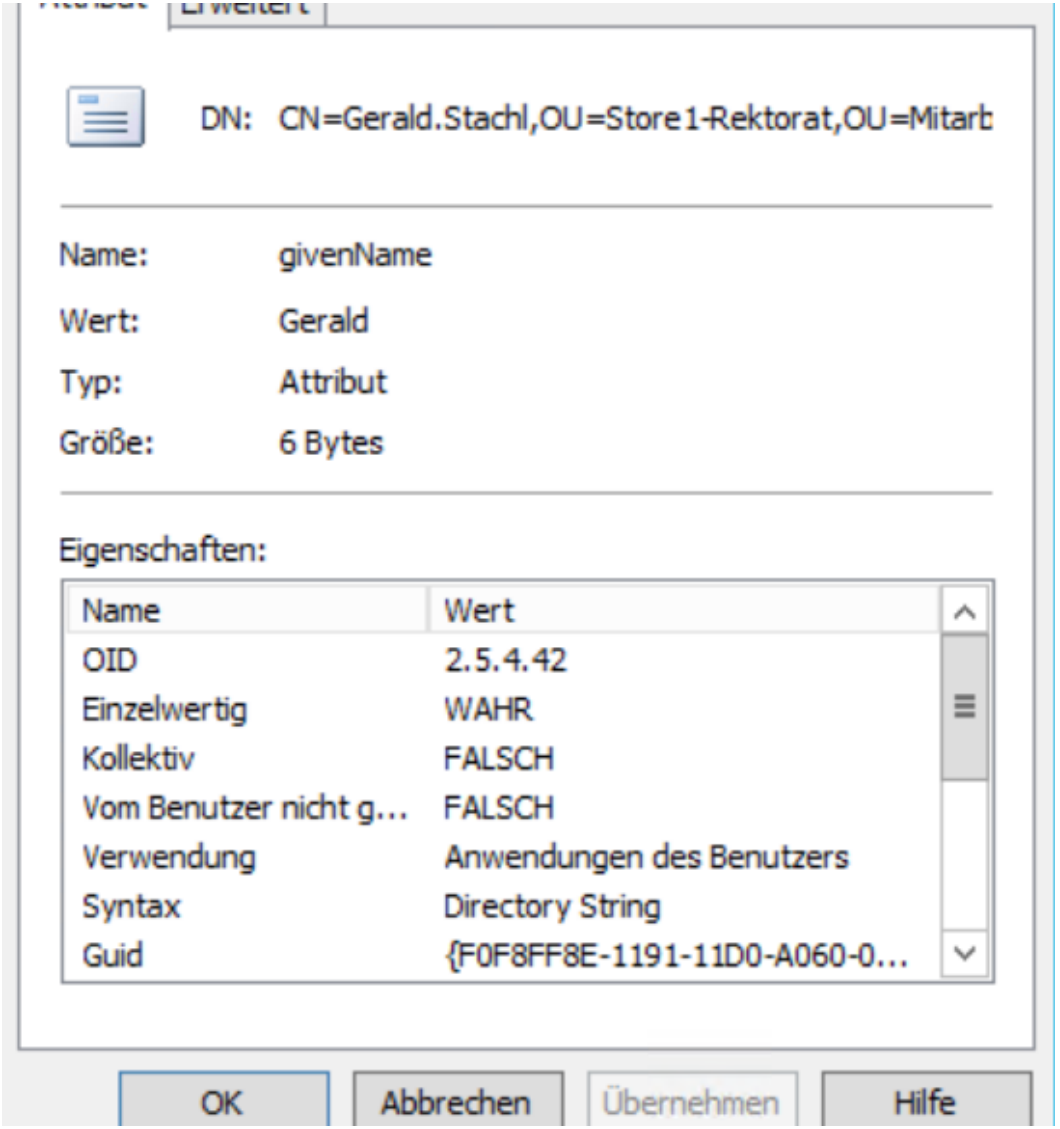
einfache Manipulation

```
 <!-- Generate displayName from givenName and surname -->
<AttributeDefinition id="displayName" xsi:type="Template">
    <Dependency ref="ad.phnoe" />
    <Template>${givenName} ${sn}</Template>
    <SourceAttribute>givenName</SourceAttribute>
    <SourceAttribute>sn</SourceAttribute>
    <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:displayName" encodeType="false" />
    <AttributeEncoder xsi:type="SAML2String" name="urn:oid:2.16.840.1.113730.3.1.241" friendlyName="displayName" encodeType="false" />
 </AttributeDefinition>
```

Mapped Attributes

```
<!-- Generate eduPersonScopedAffiliation from phoUsergroup -->
<AttributeDefinition id="eduPersonAffiliation" xsi:type="Mapped" dependencyOnly="true" sourceAttributeID="phoUsergroup">
    <Dependency ref="ad.phnoe" />
    <DefaultValue>affiliate</DefaultValue>
    <ValueMap>
        <ReturnValue>faculty</ReturnValue>
        <SourceValue partialMatch="true">B</SourceValue>
    </ValueMap>
    <ValueMap>
        <ReturnValue>student</ReturnValue>
        <SourceValue partialMatch="true">ST</SourceValue>
    </ValueMap>
    <ValueMap>
        <ReturnValue>alum</ReturnValue>
        <SourceValue partialMatch="true">A</SourceValue>
    </ValueMap>
    <ValueMap>
        <ReturnValue>member</ReturnValue>
        <SourceValue>[^ ]+</SourceValue>
    </ValueMap>
</AttributeDefinition>
```

- eindeutige Identifizierung (x.500 – Verzeichnisdienste)
- siehe: Eigenschaften bei LDAP Browser
- https://wiki.shibboleth.net/confluence/display/SHIB2/AttributeNaming

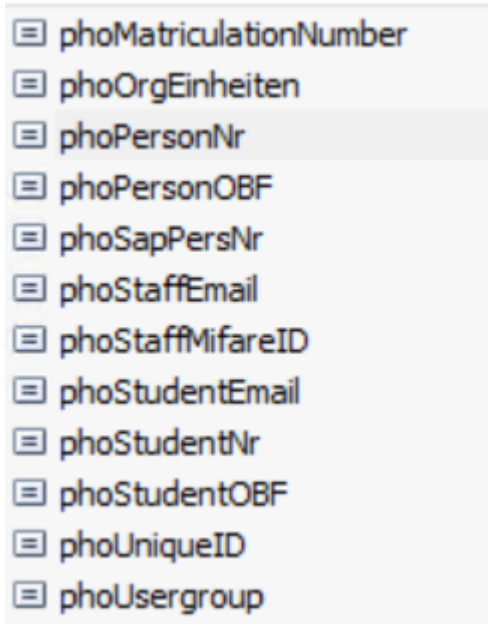


Scripted Attributes

```
<!-- Generate mail from phoStaffEmail and  phoStudentEmail-->
<AttributeDefinition id="mail" xsi:type="ScriptedAttribute">
    <Dependency ref="ad.phnoe" />
    <Script><![CDATA[
    mail.getValues().retainAll([]);
        if (phoUsergroup.getValues().get(0).indexOf('B')>-1) {
            mail.addValue(phoStaffEmail.getValues().get(0));
        } else {
            mail.addValue(phoStudentEmail.getValues().get(0));
        }
    ]]></Script>
    <AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:attribute-def:mail" encodeType="false" />
    <AttributeEncoder xsi:type="SAML2String" name="urn:oid:0.9.2342.19200300.100.1.3" friendlyName="mail" encodeType="false" />
</AttributeDefinition>
```

urn:oid (non-Standard)

- private Attribute:
- z.B: Infos aus PH-ONLINE:
- http://oidref.com/1.3.6.1.4.1.38425
- Beispiele:



iri oid

- /iso/identified-organization/dod/internet/private/enterprise/38425
- /iso/identified-organization/dod/internet/private/enterprises/38425
- /iso/org/dod/internet/private/enterprise/38425
- /iso/org/dod/internet/private/enterprises/38425
- /iso/iso-identified-organization/dod/internet/private/enterprise/38425
- /iso/iso-identified-organization/dod/internet/private/enterprises/38425

iri by oid_info

/ISO/Identified-Organization/6/1/4/1/38425

creation date

Aug. 9, 2011

Description by oid_info

Private University College of Education of the Diocese of Linz
View at oid-info.com

First Registration Authority

Wolfgang Uebermasser

Brothers (48142)

Service Provider einordnen

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:disco="urn:oasis:names:tc:SAML
  <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:Extensions>
      <disco:DiscoveryResponse Binding="urn:oasis:names:tc:SAML:profiles:SSO:idp-discovery-protocol" Location="https://moodle.ph-noe.ac.at/Shibboleth.s
    </md:Extensions>
    <md:KeyDescriptor>
      <ds:KeyInfo>
        <ds:X509Data>
          <ds:X509Certificate>
MIIC2TCCAcGgAwIBAgIJAO+G172Kp9WxMA0GCSqGSIb3DQEBBQUAMBExDzANBgNV
BAMTBm1vb2RsZTAeFw0xNzAyMTkyMTI0NTVaFw0yNzAyMTcyMTI0NTVaMBExDzAN
```

```
yFVMOCFzmy5U/BkTeIRnT0npfVK6FRLrcT1aLYh9f0oT5zJsmShQrjvE05hQE3oy
5QXd5MUgw4mYK9dPyatif8QUCkw+enon6dpr7oz7wZ1WMVramXMFxhYdwK4bz2pF
Jpzl4Zbk99WdVmE1tQ==
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://moodle.ph-noe.ac.at/Shibboleth.sso/SAML2/PO
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST-SimpleSign" Location="https://moodle.ph-noe.ac.at/Shibboleth.s
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:PAOS" Location="https://moodle.ph-noe.ac.at/Shibboleth.sso/SAML2/ECP" in
  </md:SPSSODescriptor>
</md:EntityDescriptor>
```

Attribute freigeben

```
<AttributeFilterPolicy id="LocalEntitiesNOTinFederation">
   <PolicyRequirementRule xsi:type="InEntityGroup" groupID="https://auth.ph-noe.ac.at/local-entities" />
    <AttributeRule attributeID="surname">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
    <AttributeRule attributeID="givenName">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
    <AttributeRule attributeID="uid">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
    <AttributeRule attributeID="displayName">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
    <AttributeRule attributeID="eduPersonPrincipalName">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
    <AttributeRule attributeID="mail">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
    <AttributeRule attributeID="eduPersonUniqueId">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
    <AttributeRule attributeID="schacHomeOrganization">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
    <AttributeRule attributeID="eduPersonScopedAffiliation">
        <PermitValueRule xsi:type="ANY" />
    </AttributeRule>
</AttributeFilterPolicy>
```

SAML Auth - Wo noch?

- Office 365:
  - https://msdn.microsoft.com/en-us/library/azure/dn641269.aspx
  - https://wiki.shibboleth.net/confluence/display/IDP30/Office+365
- Google Apps:
  - https://support.google.com/a/answer/60224?hl=de
- Joomla:
  - https://github.com/onelogin/joomla-saml
- WordPress:
  - https://tah.wordpress.org/plugins/wp-saml-auth/
- Typo3: (bis 6.3)
- Mahara (ePortfolio)