

SAML-Authentifizierung Anwendung in Schulnetzwerken

Mag. Gerald STACHL
PH Niederösterreich

- ☐ 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++

- Mail an gerald.stachl@ph-noe.ac.at
 - bis 30.04.2017
- Instruktoreneinschulung:
 - HTL Rennweg
 - Christian Schöndorfer

- 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



Authentifizierungsserver BG Babenbergerring

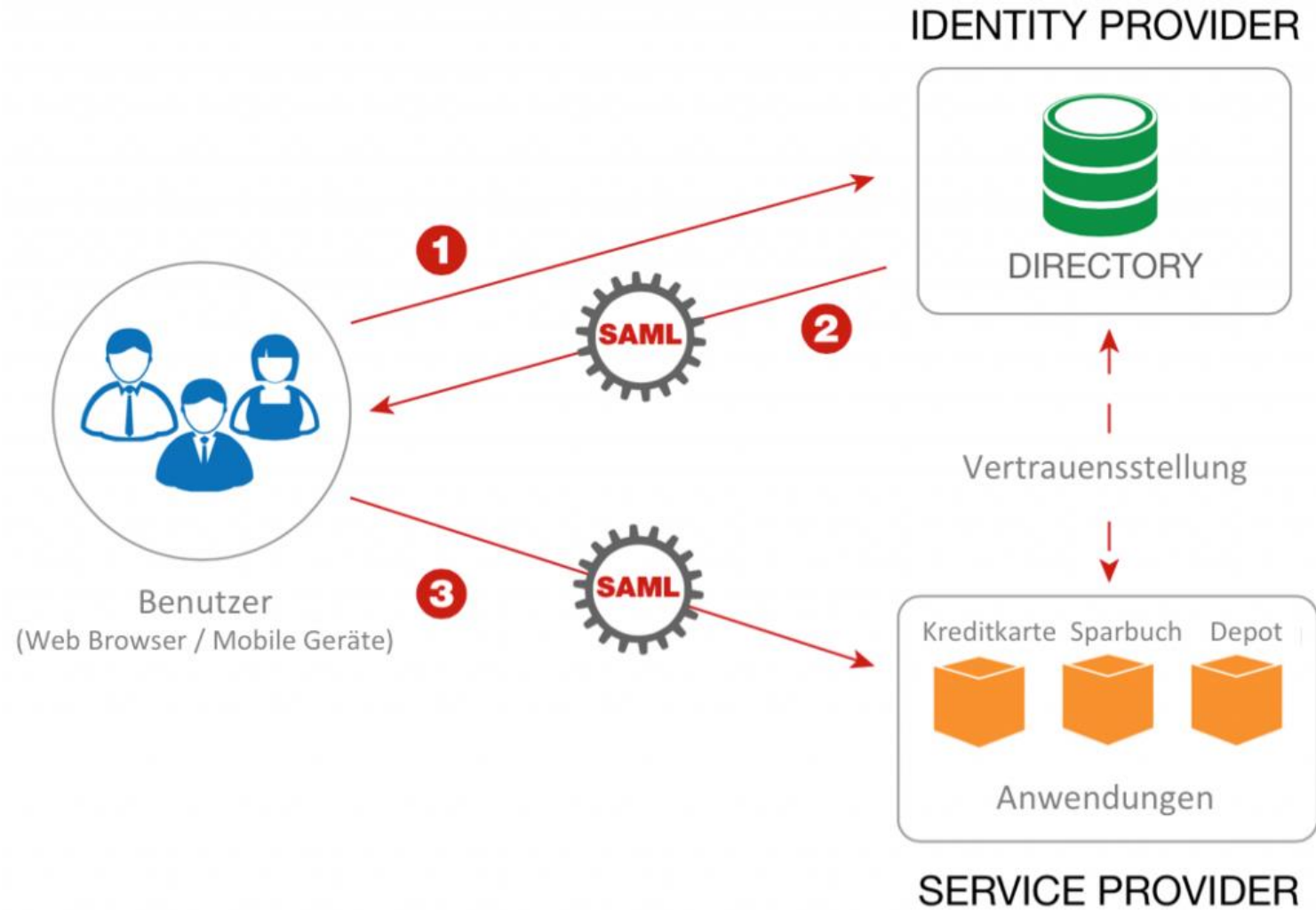
Melden sie sich mit ihrer Benutzerkennung am
BG Babenbergerring an.

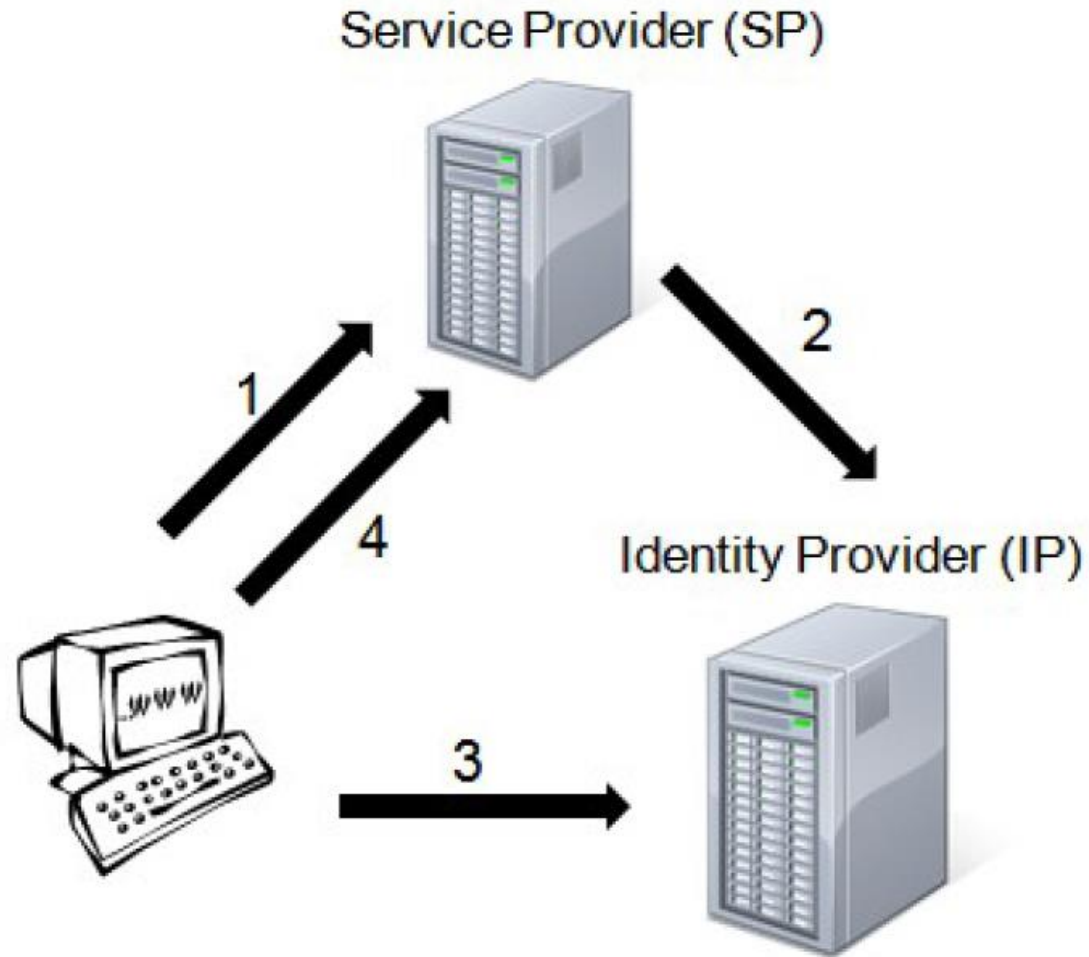
Anmelden

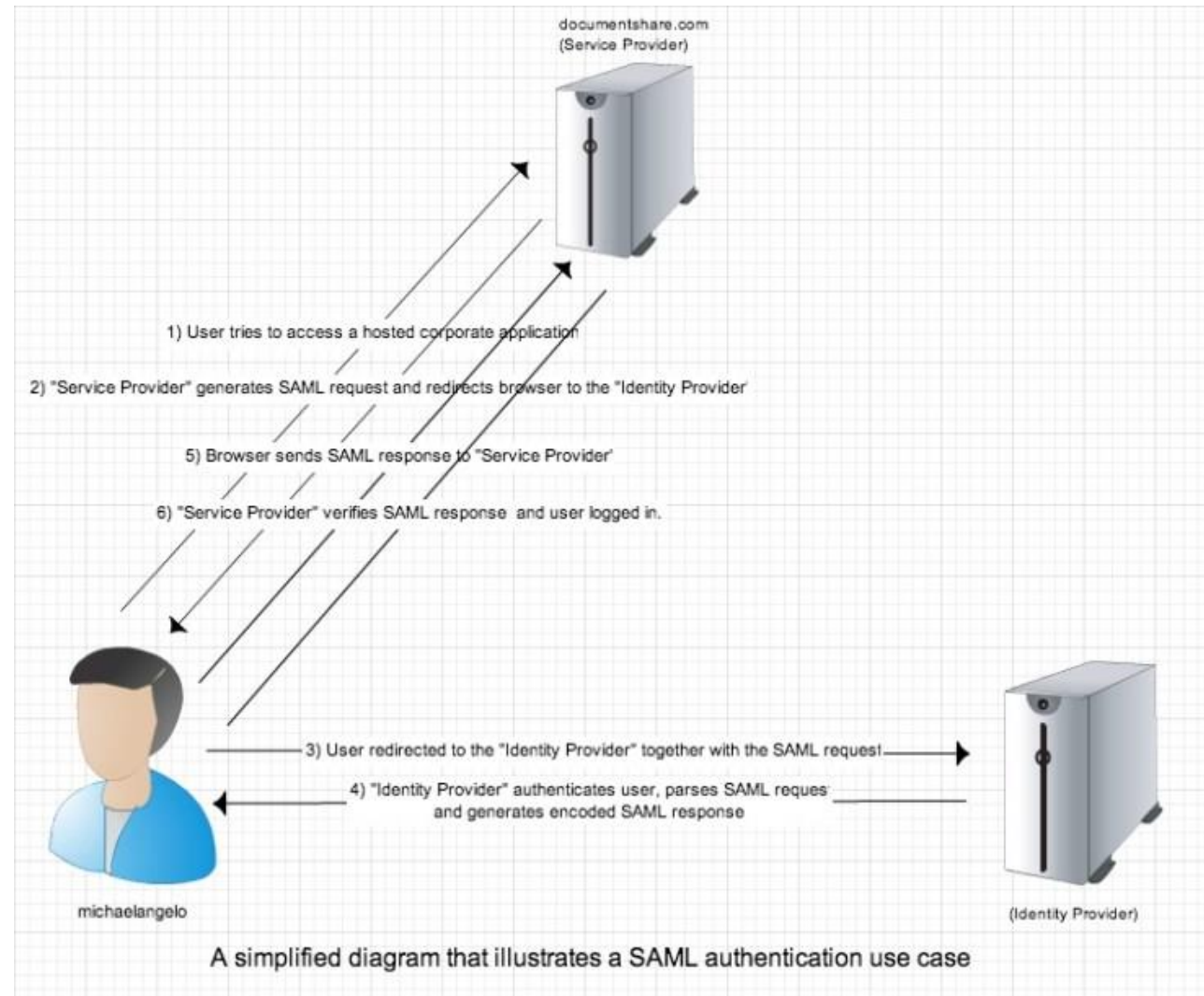
Klicken sie [hier](#) für weitere Informationen.

[Home](#) [Privacy](#)

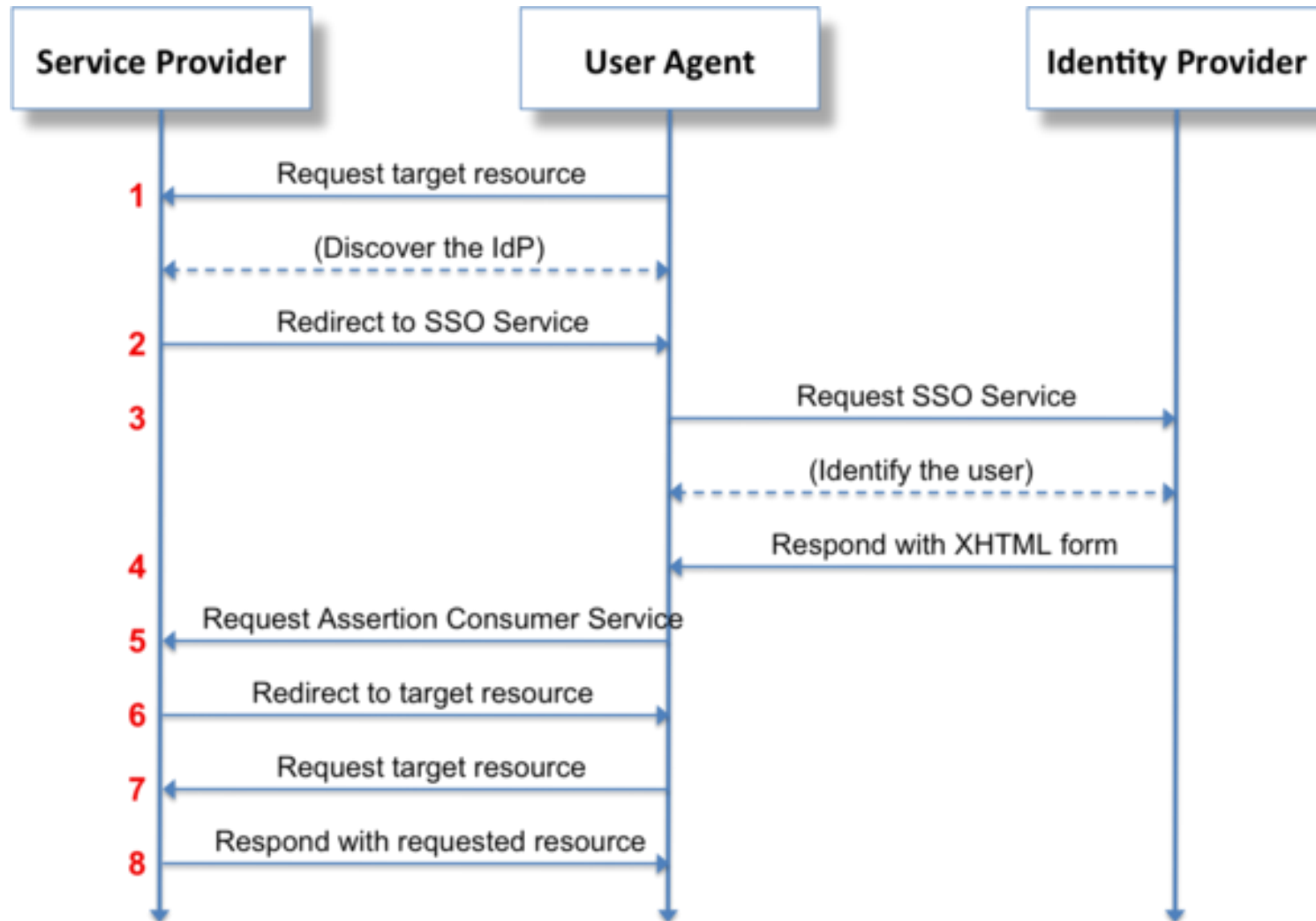
- SAML = Secure Assertion Markup Language
 - XML Framework zum Austausch von
 - Authentifizierungs- und
 - Autorisierungsinformationen
 - Entwicklung: 2001 (OASIS-Konsortium)
 - Ziele:
 - Single Sign-On
 - Verteilte Transaktion
 - Autorisierungsdienste



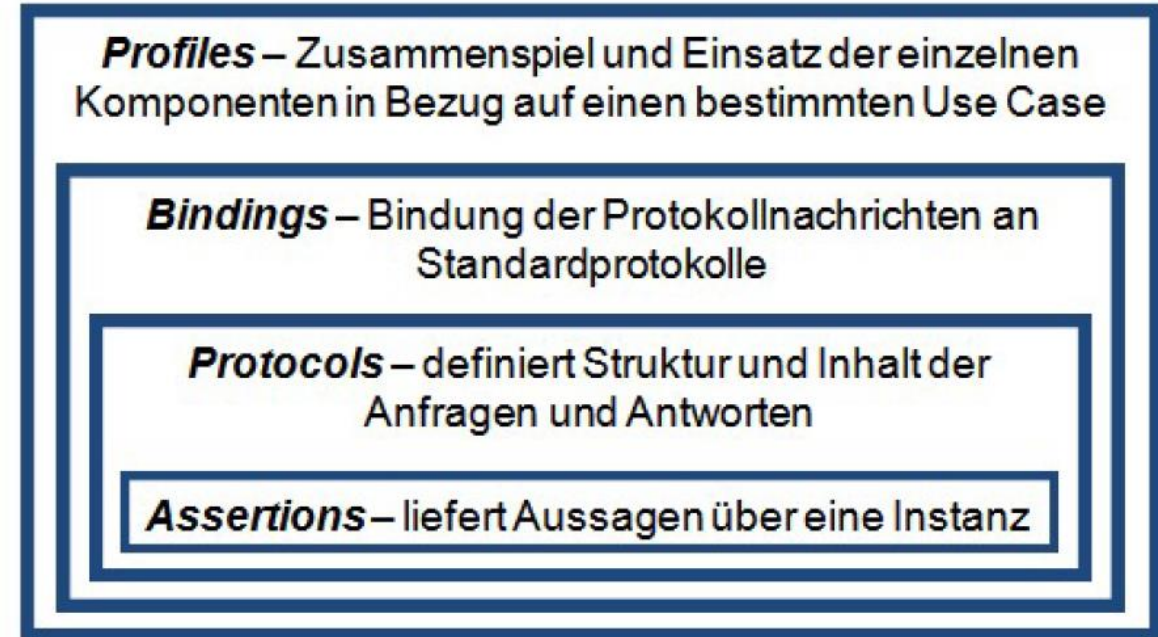




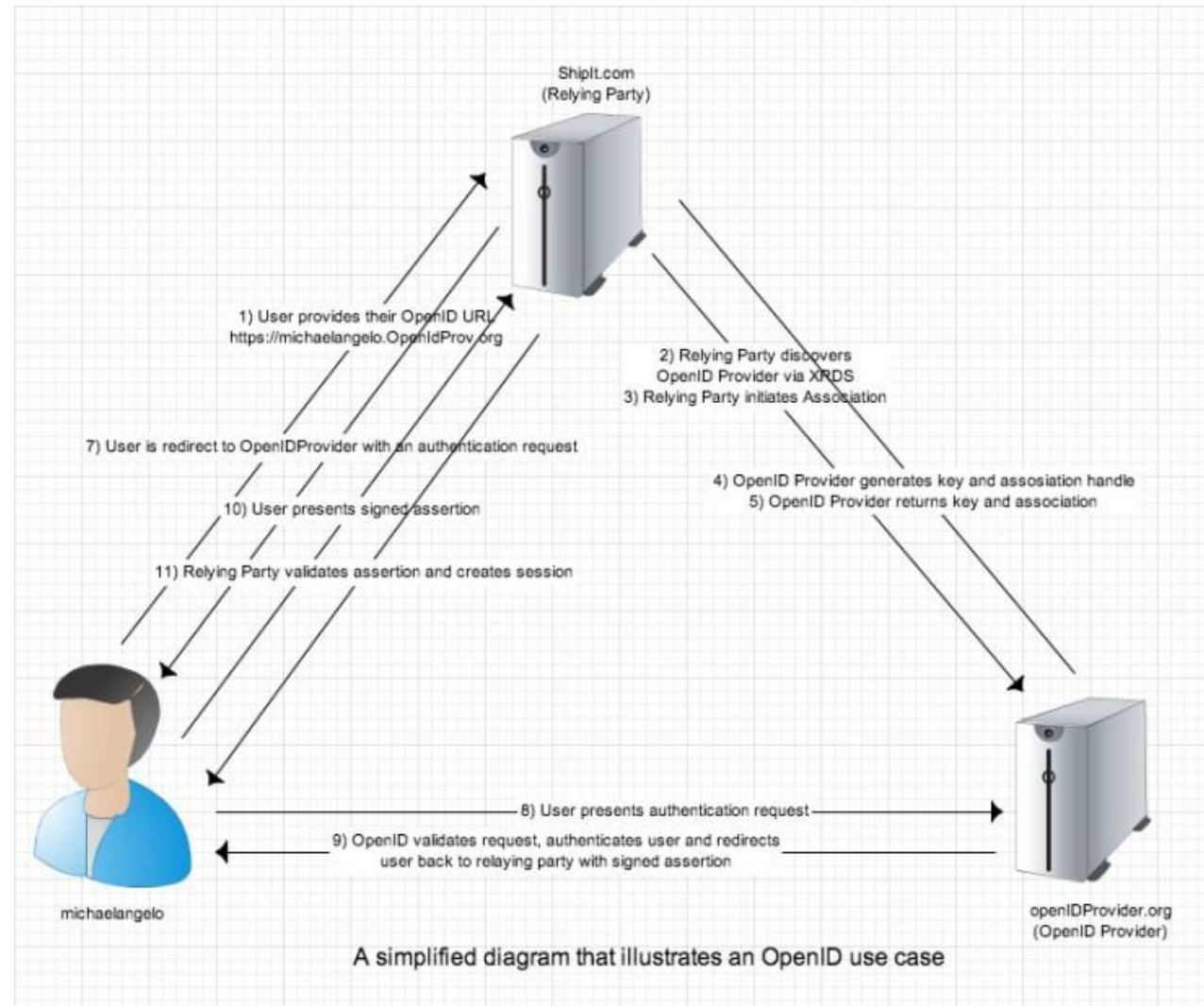
Ablauf einer SAML Authentifizierung



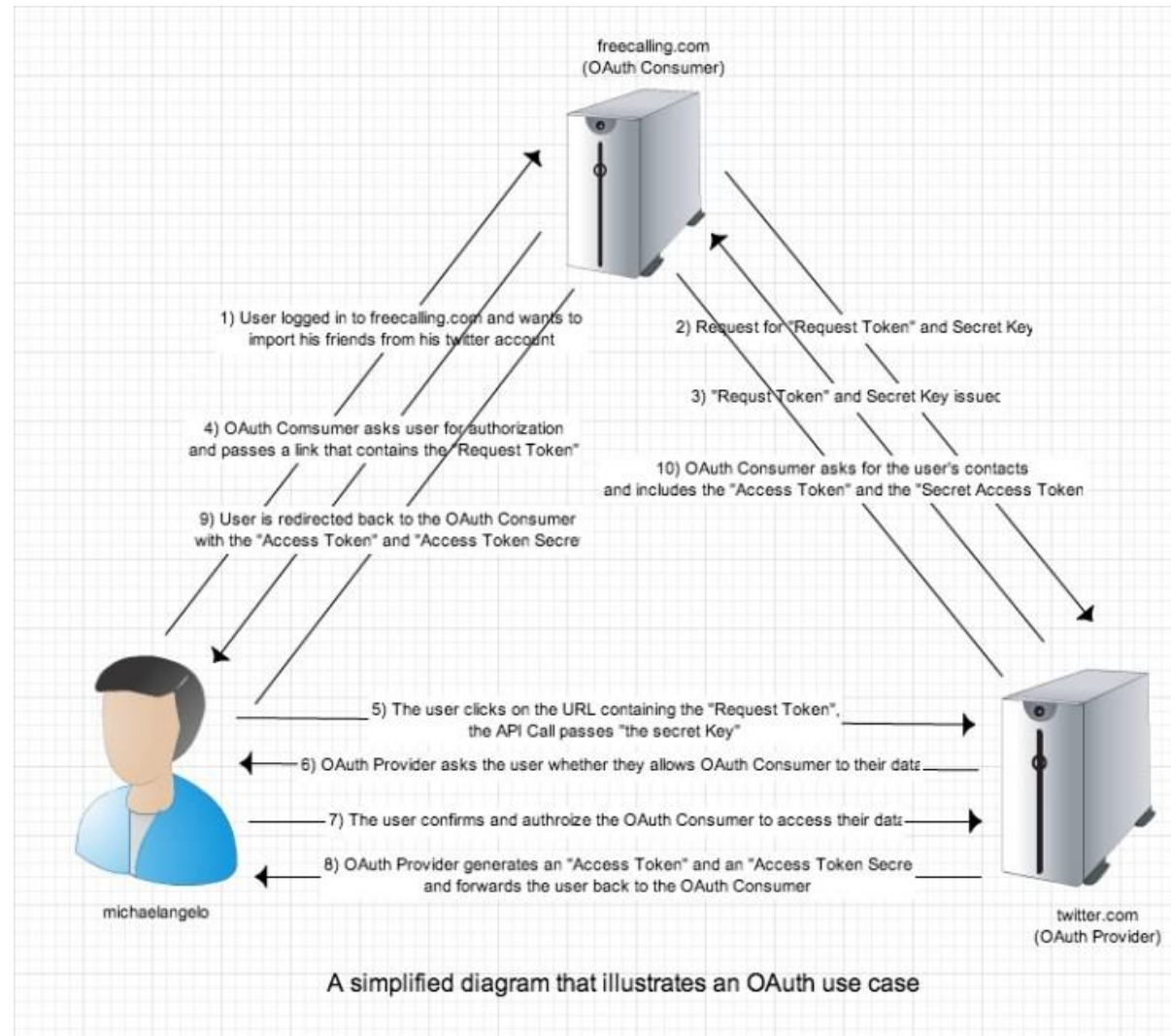
- **Assertion**
 - Aussagen über Parteien
 - Authentizität
- **Protokolle**
 - Ablauf der Anfragen und Antworten zwischen den Parteien
- **Bindungen**
 - Zusammenspiel mit Standardprotokollen (HTTP, SOAP)
- **Profil**
 - Zusammenspiel der Komponenten in einem Anwendungsfall



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



- 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



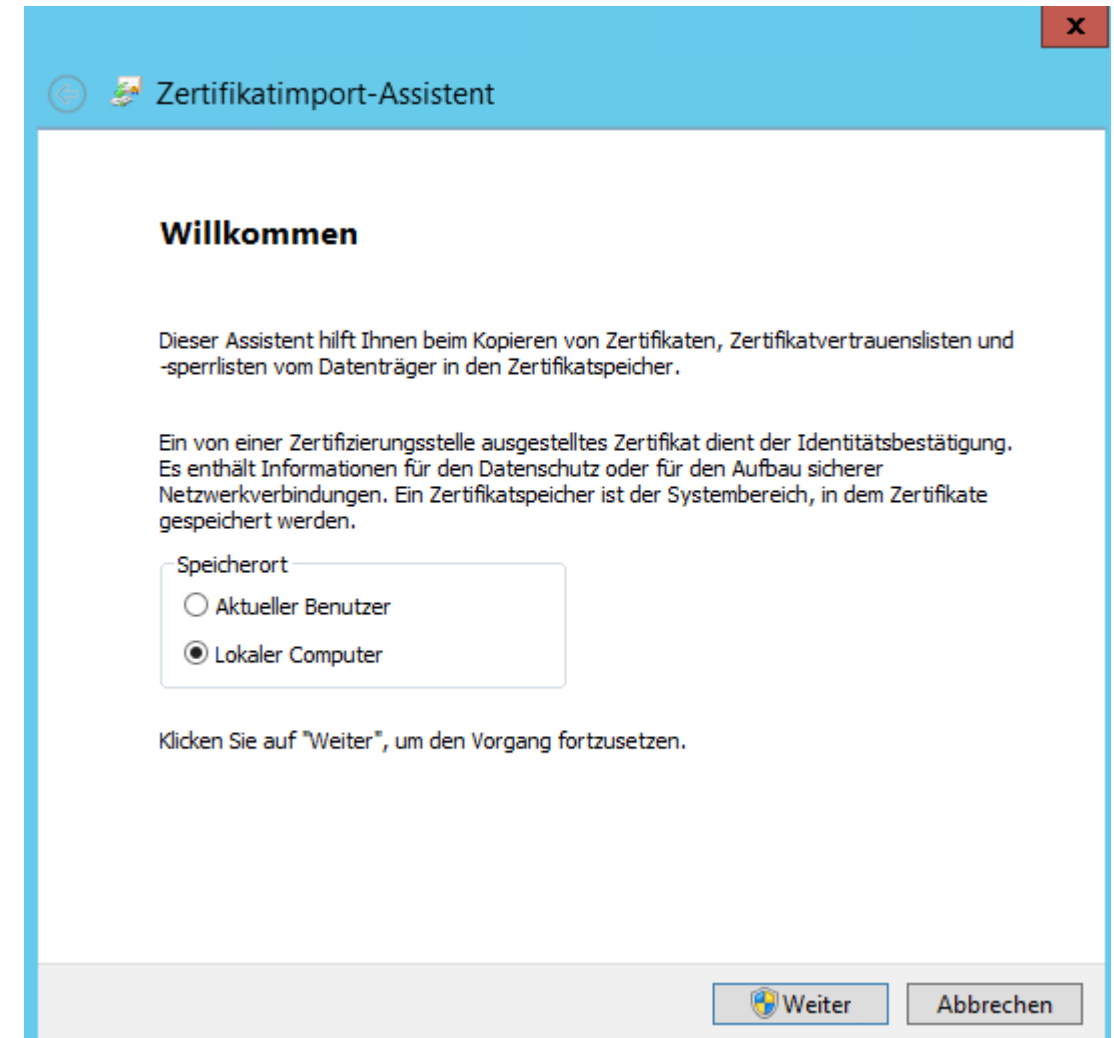
	OAuth2	OpenId	SAML
Token (or assertion) format	JSON or SAML2	JSON	XML
Authorization?	Yes	No	Yes
Authentication?	Pseudo-authentication	Yes	Yes
Year created	2005	2006	2001
Current version	OAuth2	OpenID Connect	SAML 2.0
Transport	HTTP	HTTP GET and HTTP POST	HTTP Redirect (GET) binding, SAML SOAP binding,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

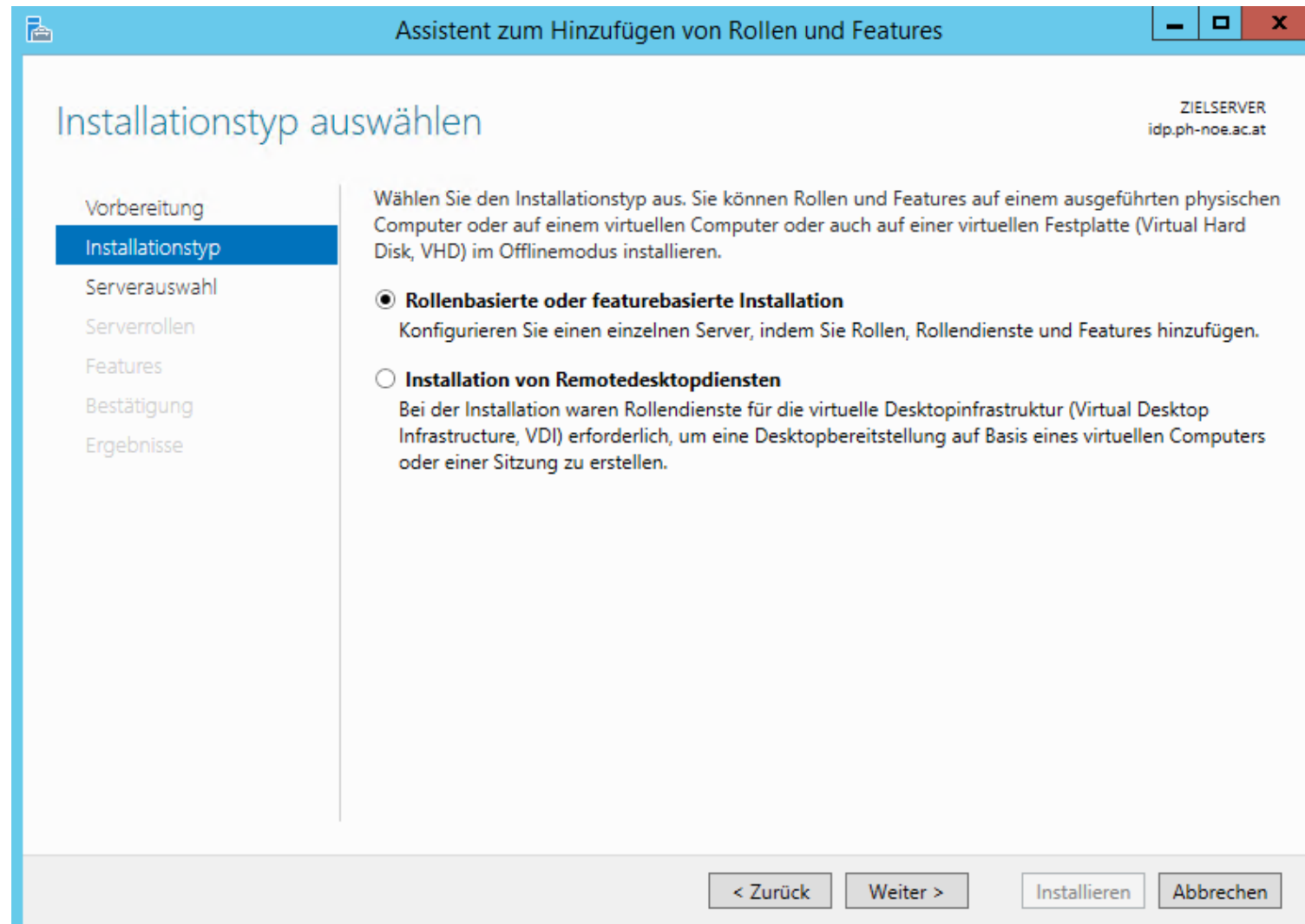
- "A kind of provider that creates, maintains, and manages identity information for principals and provides principal authentication to other service providers within a federation, such as with web browser profiles.“
- Beispiele:
 - ADFS (Microsoft), Rolle
 - Shibboleth IDP
 - Java (Tomcat)
 - Linux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

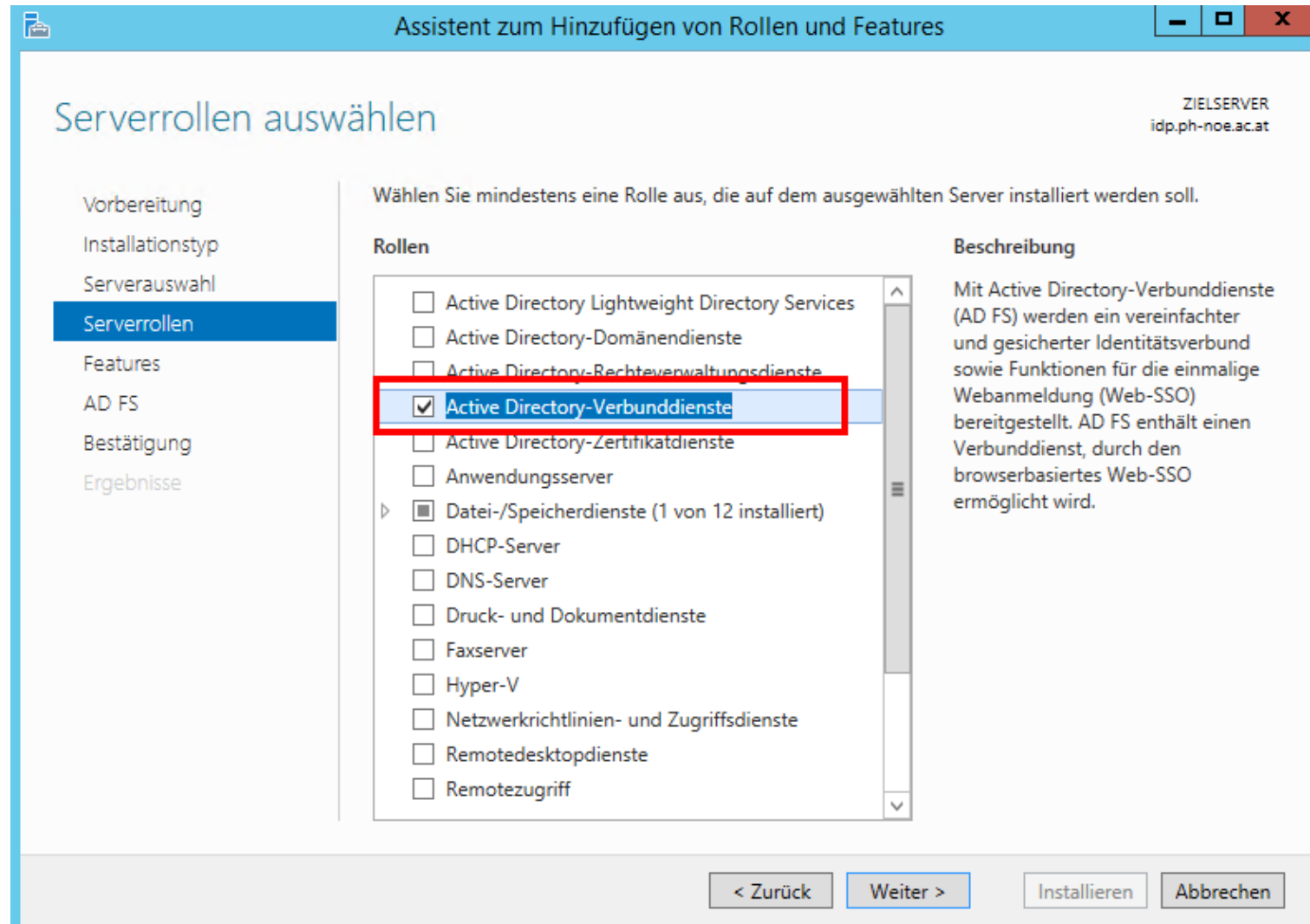
- "A role donned by a system entity where the system entity provides services to principals or other system entities“
- Beispiele
 - Shibboleth SP
 - SimpleSAMLPhP
 - ADFS

- 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>

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







The screenshot shows the Windows Server Manager interface. A warning message is displayed in the top right corner, indicating that configuration is required for "Active Directory-Verbinddienste" on "IDP". The message includes a link to configure the service. Below the warning, a progress bar shows the installation of "Featureinstallation" for "idp.ph-noe.ac.at". The dashboard also displays a "Willkommen bei Server-Manager" section with a "Schnellstart" button and a "Neuigkeiten" section. At the bottom, the "Rollen und Servergruppen" section shows the status of roles and server groups, including "AD FS" and "Datei-/Speicherdienste".

Server-Manager Dashboard

WILLKOMMEN BEI SERVER-MANAGER

Schnellstart

Neuigkeiten

Weitere Informationen

Rollen und Servergruppen

Rollen: 2 | Servergruppen: 1 | Server insgesamt: 1

AD FS 1

- Verwaltbarkeit
- Ereignisse
- Dienste
- Leistung 2
- BPA-Ergebnisse

Datei-/Speicherdienste 1

- Verwaltbarkeit
- Ereignisse
- Leistung 2
- BPA-Ergebnisse

Konfiguration nach der Bere...

Konfiguration ist für "Active Directory-Verbinddienste" auf "IDP" erforderlich.

[Konfigurieren Sie den Verbinddienst auf diesem Se...](#)

Featureinstallation

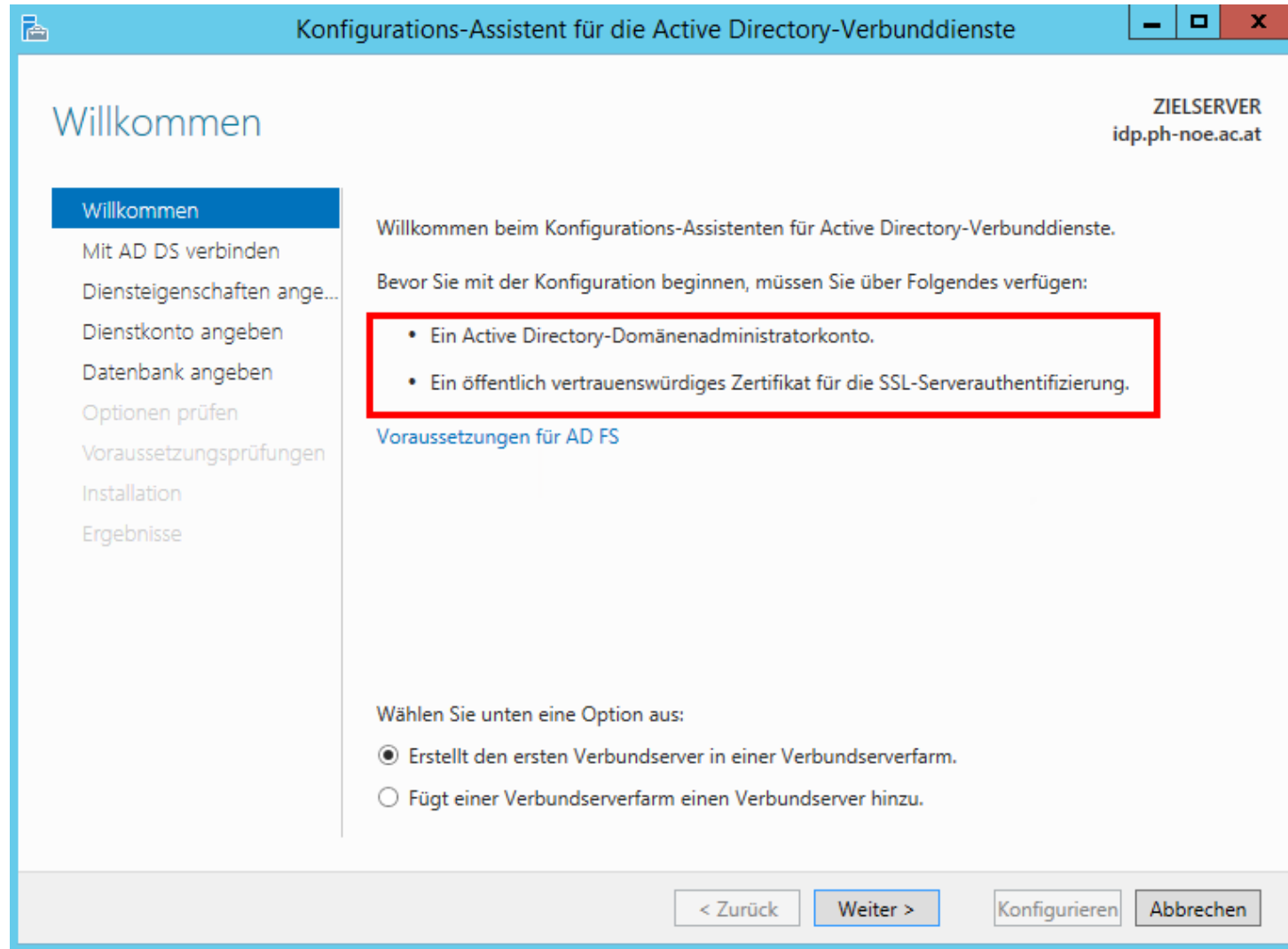
Konfiguration erforderlich. Die Installation auf "idp.ph-noe.ac.at" war erfolgreich.

[Rollen und Features hinzufügen](#)

[Aufgabendetails](#)

Ausblenden

17.04.2017 07:27



Konfigurations-Assistent für die Active Directory-Verbunddienste

Diensteigenschaften angeben

ZIELSERVER
idp.ph-noe.ac.at

Willkommen
Mit AD DS verbinden
Diensteigenschaften ange...
Dienstkonto angeben
Datenbank angeben
Optionen prüfen
Voraussetzungsprüfungen
Installation
Ergebnisse

SSL-Zertifikat: *.ph-noe.ac.at Importieren...
Anzeigen

Verbunddienstname: authdemo.ph-noe.ac.at
Beispiel: "fs.contoso.com"

Anzeigename des Verbunddiensts: PH NOE Authentifizierung
Benutzern wird der Anzeigenamen bei der Anmeldung a...
Beispiel: Contoso Corporation

< Zurück Weiter > Konfigurieren Abbrechen

Konfigurations-Assistent für die Active Directory-Verbinddienste

Dienstkonto angeben

ZIELSERVER
idp.ph-noe.ac.at

Willkommen
Mit AD DS verbinden
Diensteigenschaften ange...
Dienstkonto angeben
Datenbank angeben
Optionen prüfen
Voraussetzungsprüfungen
Installation
Ergebnisse

Geben Sie ein Domänenbenutzerkonto oder ein gruppenverwaltetes Dienstkonto an.

☒ Gruppenverwaltetes Dienstkonto erstellen

Kontoname: PH-NOE\idp

☐ Verwenden Sie ein Domänenbenutzerkonto oder ein gruppenverwaltetes Dienstkonto.

Kontoname: <Nicht angegeben> Auswählen...

< Zurück Weiter > Konfigurieren Abbrechen

Konfigurations-Assistent für die Active Directory-Verbunddienste

Konfigurationsdatenbank angeben

ZIELSERVER
idp.ph-noe.ac.at

Willkommen

Mit AD DS verbinden

Diensteigenschaften ange...

Dienstkonto angeben

Datenbank angeben

Optionen prüfen

Voraussetzungsprüfungen

Installation

Ergebnisse

Geben Sie eine Datenbank zum Speichern der Konfigurationsdaten des Active Directory-Verbunddiensts an.

☒ Erstellen Sie eine Datenbank auf diesem Server mit der internen Windows-Datenbank.

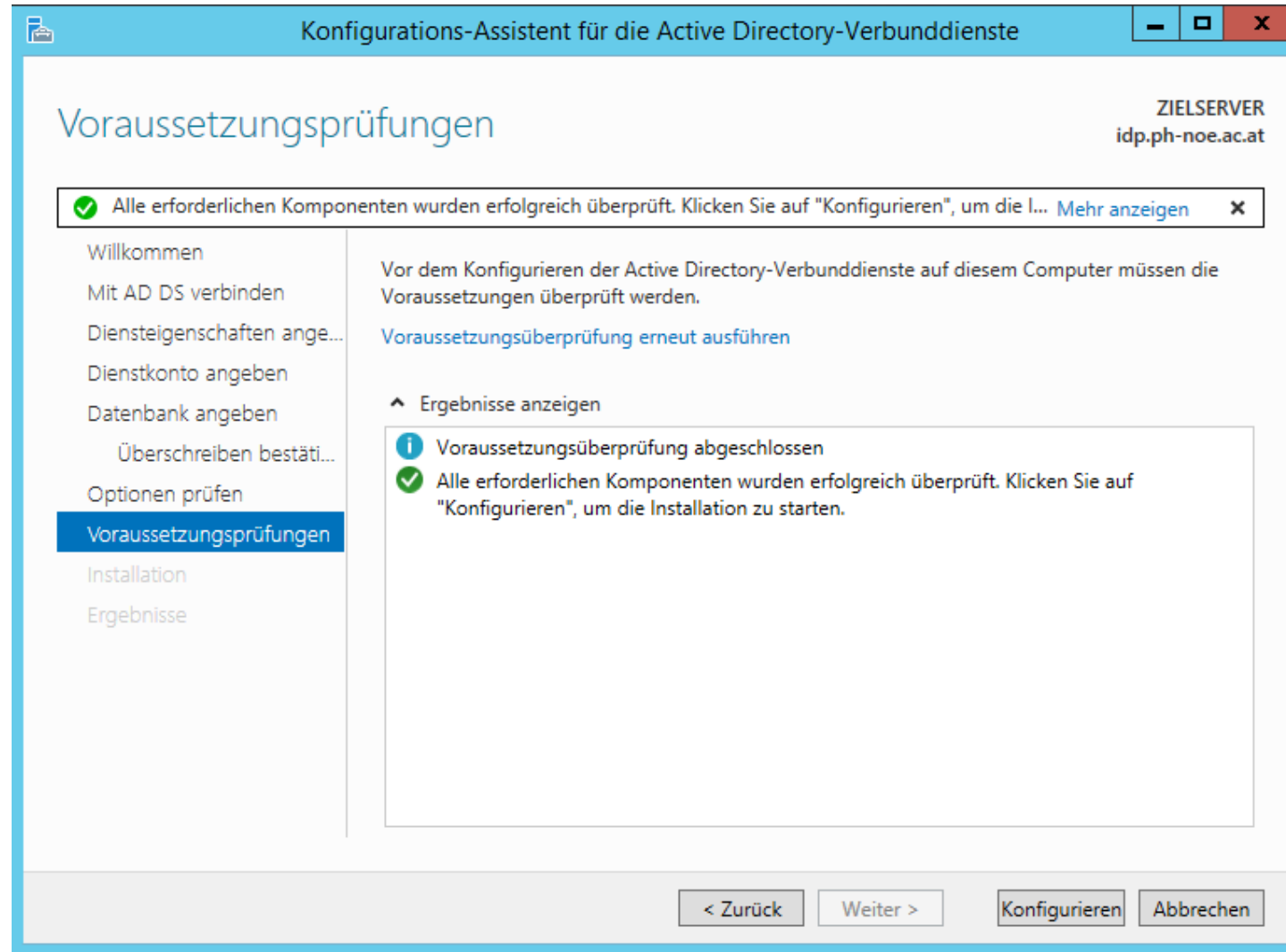
☐ Geben Sie den Ort einer SQL Server-Datenbank an.

Datenbank-Hostname:

Datenbankinstanz:

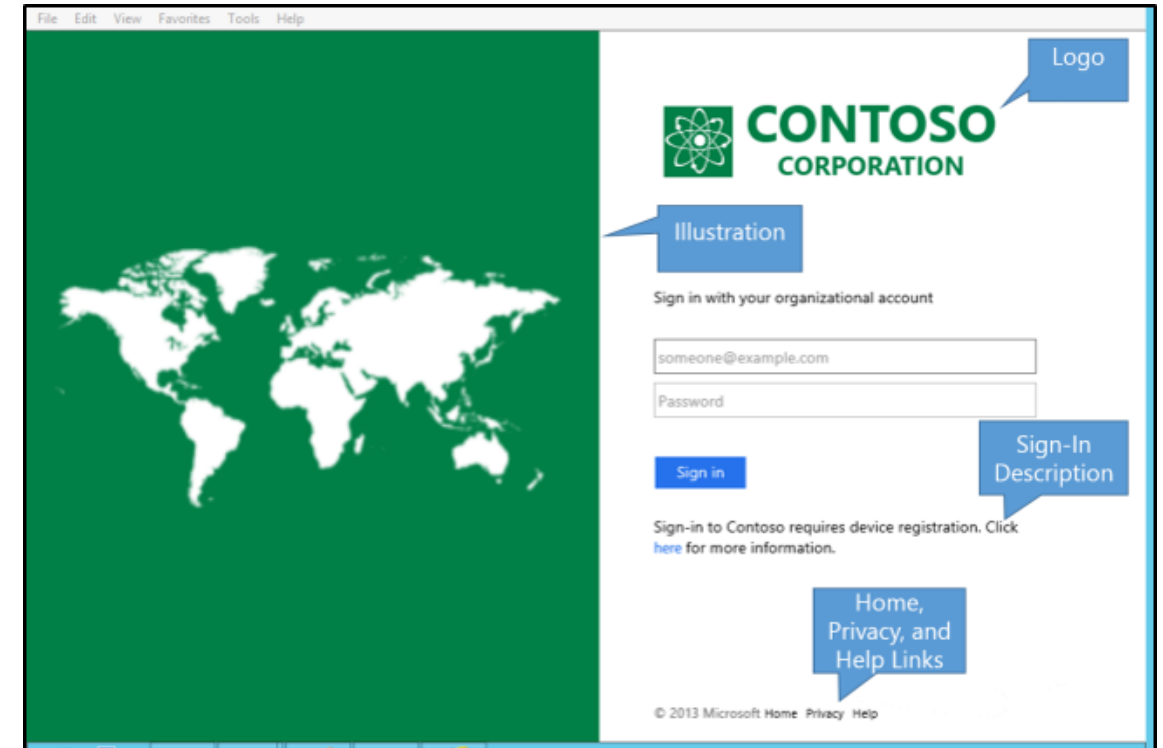
Lassen Sie zum Verwenden der Standardinstanz dieses Feld leer.

< Zurück Weiter > Konfigurieren Abbrechen



- <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

- 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"}



Verbunddiensteigenschaften

Allgemein Organisation Ereignisse

Anzeigename des Verbunddiensts:

Beispiel: Fabrikam-Verbunddienst

Verbunddienstname:

Beispiel: fs.fabrikam.com

Bezeichner des Verbunddiensts:

Beispiel: http://fs.fabrikam.com/adfs/services/trust

Lebensdauer für Web-SSO: Minuten

OK Abbrechen Übernehmen

- <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>

- 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
```

- 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`

- 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. ??*

- /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.

- `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`

- /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">

    <!--
```

- /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"/>

```


- /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>
```

- /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"/>
```

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

moodledemo.ph-noe.ac.at Eigenschaften

Akzeptierte Ansprüche	Organisation	Endpunkte
Proxyendpunkte	Anmerkungen	Erweitert
Überwachung	Bezeichner	Verschlüsselung
		Signatur

Geben Sie die Überwachungseinstellungen für diese Vertrauensstellung der vertrauenden Seite an.

Verbundmetadaten-URL der vertrauenden Seite:

☒ Vertrauende Seite überwachen

☒ Update für vertrauende Seite automatisch ausführen

Die Verbundmetadaten dieser vertrauenden Seite wurden zuletzt überprüft am:

17.04.2017

Diese vertrauende Seite wurde von den Verbundmetadaten zuletzt aktualisiert am:

17.04.2017

The screenshot shows the 'Verbunddiensteigenschaften' (Federated Service Properties) dialog box with the 'Organisation' tab selected. The dialog contains two main sections: 'Organisation' and 'Supportkontaktinformationen in Verbundmetadaten'.

Organisation Section:

- ☒ Infos zur Organisation in Verbundmetadaten veröffentlichen
- Anzeigename der Organisation: PH NOE
- URL der Organisation: http://www.ph-noe.ac.at

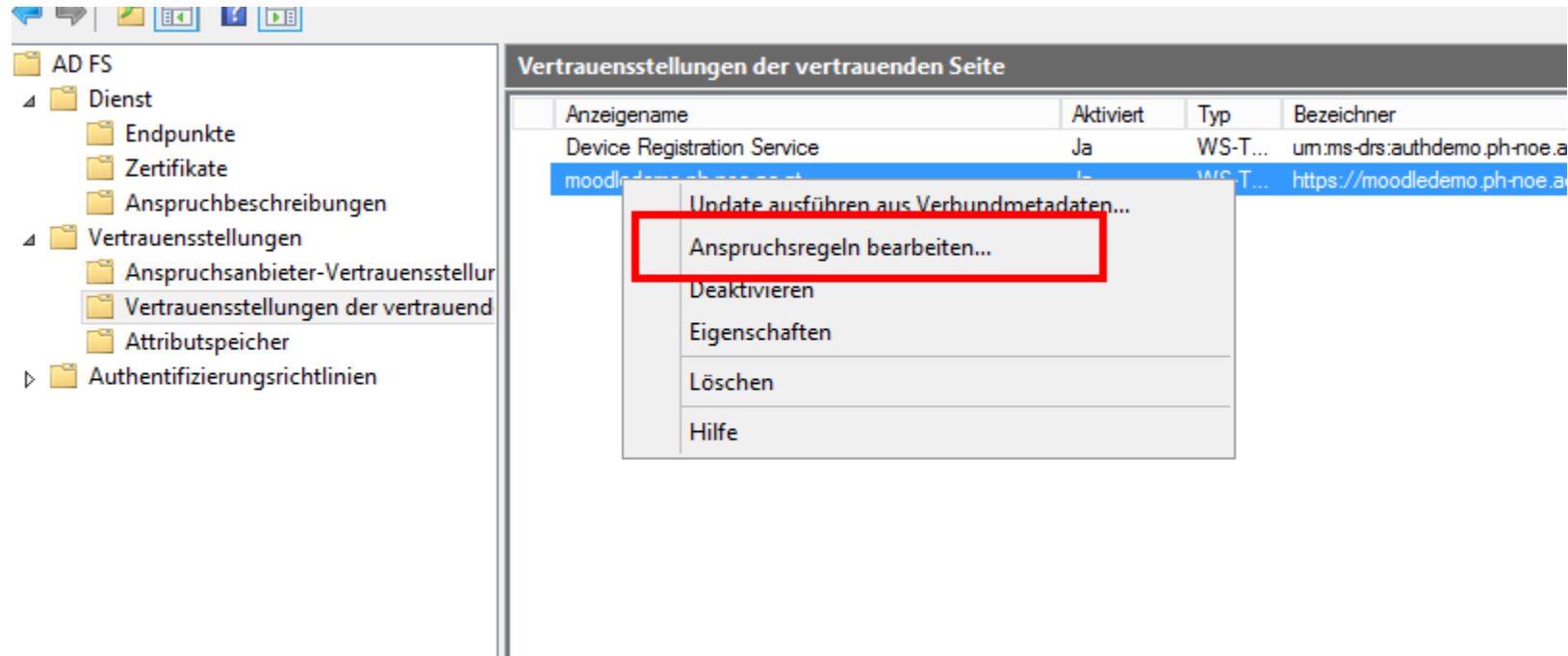
Supportkontaktinformationen in Verbundmetadaten Section:

- Vorname: Gerald
- Nachname: Stachl
- E-Mail-Adresse: gerald.stachl@ph-noe.ac.at
- Telefonnummer: +43 2252 88570 125

At the bottom of the dialog are three buttons: OK, Abbrechen, and Überehmen.

Zertifikate					
Antragsteller	Aussteller	Gültig ab	Ablaufdatum	Status	
Dienstkommunikation					
 CN=*.ph-noe.ac.at, OU=De...	CN=TERENA SSL CA 3, ...	02.11.2016	07.11.2019		
Tokenentschlüsselung					
 CN=ADFS Encryption - aut...	CN=ADFS Encryption - au...	17.04.2017	17.04.2018		
Tokensignatur					
 CN=ADFS Signing - authde...	CN=ADFS Signing - authd...	17.04.2017	17.04.2018		

ev. austauschen (WebUntis)



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

Regel bearbeiten - Basisattribute ✕

Diese Regel kann so konfiguriert werden, dass sie die Werte von LDAP-Attributen als Ansprüche sendet. Wählen Sie einen Attributspeicher aus, aus dem die LDAP-Attribute extrahiert werden sollen. Geben Sie an, wie die Attribute den von der Regel ausgestellten ausgehenden Anspruchstypen zugeordnet werden.

Anspruchsregelname:

Regelvorlage: LDAP-Attribute als Ansprüche senden

Attributspeicher:

Zuordnung von LDAP-Attributen zu ausgehenden Anspruchstypen:

	LDAP-Attribut (weitere können durch Auswahl oder Eingabe hinzugefügt werden)	Ausgehender Anspruchstyp (weitere können durch Auswahl oder Eingabe hinzugefügt werden)
▶	SAM-Account-Name	um:oid:2.5.4.3
	Given-Name	um:oid:2.5.4.42
	Surname	um:oid:2.5.4.4
	E-Mail-Addresses	um:oid:0.9.2342.19200300.100.1.3
*		

- Shibboleth-Authentifizierung für ./auth/shibboleth

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


- Shibboleth-Authentifizierung für ./auth/shibboleth

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

> Website-Administration > Plugins > Authentifizierung > Übersicht

Übersicht

Aktive Plugins zur Authentifizierung

Name	Nutzer/innen	Aktivieren	Aufwärts/Abwärts	Einstellungen	Testeinstellungen	Deinstallieren
Manuelle Konten	2			Einstellungen		
Kein Login	0			Einstellungen		
E-Mail basiert	0		↓	Einstellungen		Deinstallieren
Shibboleth	1		↑	Einstellungen		
CAS-Server (SSO)	0			Einstellungen		Deinstallieren
Externe Datenbank	0			Einstellungen	Testeinstellungen	Deinstallieren
FirstClass-Server	0			Einstellungen		Deinstallieren



Anleitung

auth_instructions



Alternativ können sie SSO verwenden:

<https://moodledemo.ph-noe.ac.at/auth/shibboleth/index.php>

Standard: Leer

Wenn dieses Textfeld leer ist, wird auf der Anmeldeseite der Standardtext



Login

Anmeldename

Kennwort

☐ Anmeldenamen merken

[Anmeldename oder Kennwort vergessen?](#)

Cookies müssen aktiviert sein! ⓘ

Einige Kurse könnten für Gäste zugelassen sein.

Sind Sie zum ersten Mal auf dieser Webseite?

Alternativ können sie SSO verwenden:

<https://moodledemo.ph-noe.ac.at/auth/shibboleth/index.php>

Anmeldename: Na

Datenmodifikation APU: Sie

Datenzuordnung

Vorname

Lokal aktualisieren
Beim Anlegen ▼

Feld sperren
Bearbeitbar ▼

Nachname

Lokal aktualisieren
Beim Anlegen ▼

Feld sperren
Bearbeitbar ▼

E-Mail-Adresse

Lokal aktualisieren
Beim Anlegen ▼

Feld sperren
Bearbeitbar ▼

Stadt/Ort

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>
```

Shibboleth

Mit diesem Verfahren können Sie die Verbindung zu einem bestehenden Shibboleth Server herstellen, um Zugänge zu prüfen und anzulegen.

Anmeldename: Name der Shibboleth Umgebungsvariable, die als Moodle-Nutzername verwandt werden soll

Datenmodifikation APU: Sie können diese API nutzen, um Daten von Shibboleth zu bearbeiten. [Hier](#) finden Sie weitere Hinweise.

Moodle WAYF Service: ☐ Nach der Aktivierung verwendet Moodle den eigenen WAYF Service an Stelle des für Shibboleth konfigurierten. Moodle zeigt dann eine Dropdownliste der verfügbaren alternativen Login-Seiten wo der Nutzer seinen Identity Provider auszuwählen hat.

Identity-Provider: Stellen Sie eine Liste der Identity-Provider zur Verfügung aus der die Nutzer auf der Loginseite auswählen können. In jeder Zeile muss ein kommagetrenntes Tupple für identityID der IdP (siehe Shibboleth Metadatadatei) und Name des IdP wie es in der Dropdownliste gezeigt werden soll eingetragen werden. Als optionaler dritter Parameter kann der Ort des Shibboleth Session Initiators eingetragen werden falls die Moodle-Installation im Verbund genutzt wird.

Shibboleth Service Provider Logout URL Handler: Tragen Sie die URL für den Shibboleth Service Provider Logout Handler ein. Typischerweise ist dies Shibboleth.sso/Logout

Alternative URL nach Logout: Auf diese Seite werden Shibboleth-Nutzer nach dem Logout geleitet. Bleibt das Feld leer wird die Standardseite von Moodle genutzt.

Bezeichnung der Authentifizierungsmethode: Vergeben Sie für die verwendete Shibboleth-Methode einen Titel, der den Nutzern vertraut ist, z.B. der Titel des Shibboleth-Verbunds (SWITCHaa1 Login oder Gemeinsamer Login).

URL zur Kennwortänderung: Hier können Sie eine Adresse angeben, über die die Nutzer ihren Anmeldenamen erfahren und ihr Kennwort zurücksetzen können, sofern sie diese Daten vergessen haben. Diese Option wird als Schaltfläche auf der Anmeldungsseite angeboten. Wenn Sie dieses Feld leer lassen, wird die Option nicht angeboten.

Datenzuordnung

Vorname

Nachname

E-Mail-Adresse

Variable mit
HTTP_....

- Metadatenaustausch mit Gruber&Peters
- Instanz muss auf hepta (=SP) liegen:
 - <https://hepta.webuntis.com/WebUntis/index.do#main>
- SSO Provider (IDP) in Administration → Einstellungen:

E-Mailadresse Stundenplaner	hannes.komuczky@bg-bab.ac.at	Testmail
E-Mailadresse des Benutzers im reply-to eintragen	☒	
SSO Provider	https://moodle.bg-bab.ac.at/adfs/s	
Lizenzzeile 1 von Untis	BG WR.NEUSTADT BABENBERG	

Integration

Untis
SAML
Office365
Socrates
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	☐
Rollenidentifizierung	Attribut
SAML Personenrolle Attribut	urn:oid:1.3.6.1.4.1.5923.1.1.1.1

Rollenbezogene Einstellungen

	Lehrer	Schüler
Personenrolle	lehrer	schueler
Personenidentifizierung	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

- 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!

Anspruchsregeln für webuntis.aoide bearbeiten

Ausstellungstransformationsregeln | **Ausstellungsautorisierungsregeln** | Delegationsautorisierungsregeln

Die folgenden Transformationsregeln geben die Ansprüche an, die an die vertrauende Seite gesendet werden.

Rei...	Regelname	Ausgegebene Ansprüche
1	WebUntisIDs	um:oid:2.5.4.3;um:oid:0.9...
2	Lehrer	um:oid:1.3.6.1.4.1.5923....
3	Schueler	um:oid:1.3.6.1.4.1.5923....
4	UPN als NameID	Namens-ID

Regel hinzufügen... | Regel bearbeiten... | Regel entfernen...

Regel bearbeiten - WebUntisIDs

Diese Regel kann so konfiguriert werden, dass sie die Werte von LDAP-Attributen als Ansprüche sendet. Wählen Sie einen Attributspeicher aus, aus dem die LDAP-Attribute extrahiert werden sollen. Geben Sie an, wie die Attribute den von der Regel ausgestellten ausgehenden Anspruchstypen zugeordnet werden.

Anspruchsregelname:
WebUntisIDs

Regelvorlage: LDAP-Attribute als Ansprüche senden

Attributspeicher:
Active Directory

Zuordnung von LDAP-Attributen zu ausgehenden Anspruchstypen:

	LDAP-Attribut (weitere können durch Auswahl oder Eingabe hinzugefügt werden)	Ausgehender Anspruchstyp (weitere können durch Auswahl oder Eingabe hinzugefügt werden)
▶	Title	um:oid:2.5.4.3
	E-Mail-Addresses	um:oid:0.9.2342.19200300.100.1.3
	User-Principal-Name	UPN
*		

Regelsprache anzeigen... | OK | Abbrechen

Regel bearbeiten - Lehrer

Diese Regel kann so konfiguriert werden, dass sie einen Anspruch auf Grundlage der Active Directory-Gruppenmitgliedschaft eines Benutzers sendet. Geben Sie die Gruppe an, deren Mitglied der Benutzer ist, und geben Sie den ausgehenden Anspruchstyp sowie -wert an, der ausgestellt werden soll.

Anspruchsregelname:
Lehrer

Regelvorlage: Gruppenmitgliedschaft als Anspruch senden

Gruppe des Benutzers:
BGBAB\lehrer

Ausgehender Anspruchstyp:
um:oid:1.3.6.1.4.1.5923.1.1.1.1

Ausgehendes ID-Format des Namens:
Nicht angegeben

Ausgehender Anspruchswert:
lehrer

Regelsprache anzeigen...

OK Abbrechen

Regel bearbeiten - Schueler

Diese Regel kann so konfiguriert werden, dass sie einen Anspruch auf Grundlage der Active Directory-Gruppenmitgliedschaft eines Benutzers sendet. Geben Sie die Gruppe an, deren Mitglied der Benutzer ist, und geben Sie den ausgehenden Anspruchstyp sowie -wert an, der ausgestellt werden soll.

Anspruchsregelname:
Schueler

Regelvorlage: Gruppenmitgliedschaft als Anspruch senden

Gruppe des Benutzers:
BGBAB\schueler

Ausgehender Anspruchstyp:
um:oid:1.3.6.1.4.1.5923.1.1.1.1

Ausgehendes ID-Format des Namens:
Nicht angegeben

Ausgehender Anspruchswert:
schueler

Regelsprache anzeigen...

OK Abbrechen

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

Regel bearbeiten - UPN als NameID

Diese Regel kann so konfiguriert werden, dass sie einen eingehenden Anspruchstyp einem ausgehenden Anspruchstyp zuordnet. Optional kann auch ein eingehender Anspruchswert einem ausgehenden Anspruchswert zugeordnet werden. Geben Sie den eingehenden Anspruchstyp an, der dem ausgehenden Anspruchstyp zugeordnet werden soll, und legen Sie fest, ob der Anspruchswert einem neuen Anspruchswert zugeordnet werden soll.

Anspruchsregelname:

Regelvorlage: Eingehenden Anspruch transformieren

Eingehender Anspruchstyp:

Eingehendes ID-Format des Namens:

Ausgehender Anspruchstyp:

Ausgehendes ID-Format des Namens:

☒ Alle Anspruchswerte zulassen

☐ Eingehenden Anspruchswert durch einen anderen ausgehenden Anspruchswert ersetzen

Eingehender Anspruchswert:

Ausgehender Anspruchswert:

☐ Eingehende E-Mail-Suffix-Ansprüche durch ein neues E-Mail-Suffix ersetzen

Neuer E-Mail-Suffix:

Beispiel: fabrikam.com

Shibboleth IDP
(Java, Tomcat)

LDAP Zugriff

Active Directory

```
<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>
```

```
<!-- 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>
```

```
<!-- 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>
```

```
<!-- 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/AttributeName>

DN: CN=Gerald.Stachl,OU=Store 1-Rektorat,OU=Mitarb

Name: givenName
Wert: Gerald
Typ: Attribut
Größe: 6 Bytes

Eigenschaften:

Name	Wert
OID	2.5.4.42
Einzelwertig	WAHR
Kollektiv	FALSCH
Vom Benutzer nicht g...	FALSCH
Verwendung	Anwendungen des Benutzers
Syntax	Directory String
Guid	{F0F8FF8E-1191-11D0-A060-0...

Buttons: OK, Abbrechen, Übernehmen, Hilfe

```
<!-- 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>
```

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

- ☐ phoMatriculationNumber
- ☐ phoOrgEinheiten
- ☐ phoPersonNr
- ☐ phoPersonOBF
- ☐ phoSapPersNr
- ☐ phoStaffEmail
- ☐ phoStaffMifareID
- ☐ phoStudentEmail
- ☐ phoStudentNr
- ☐ phoStudentOBF
- ☐ phoUniqueID
- ☐ phoUsergroup

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](http://oid-info.com)

First Registration Authority

[Wolfgang Uebermasser](#)

Brothers (48142)

```
<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
BAMTBmlvb2R5ZTAeFw0xNzAyMTkyMTI0NTVaFw0yNzAyMTcyMTI0NTVaMBExDzAN

          yFVMOCFzmy5U/BkTeIRnT0npfVK6FRLrcT1aLYh9f0oT5zJsmShQrjvE05hQE3oy
          5QXd5MUgw4mYK9dPyatif8QUckw+enon6dpr7oz7wZ1WMVramXMFxhYdwK4bz2pF
          Jpz14Zbk99WdVmE1tQ==
        </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>
```

```
<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>
```

- 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)