# Office 365 –
# Active Directory Federation Services –
# Shibboleth

**ZKI-Arbeitskreis Verzeichnisdienste**

**Kaiserslautern 17.09.2013**

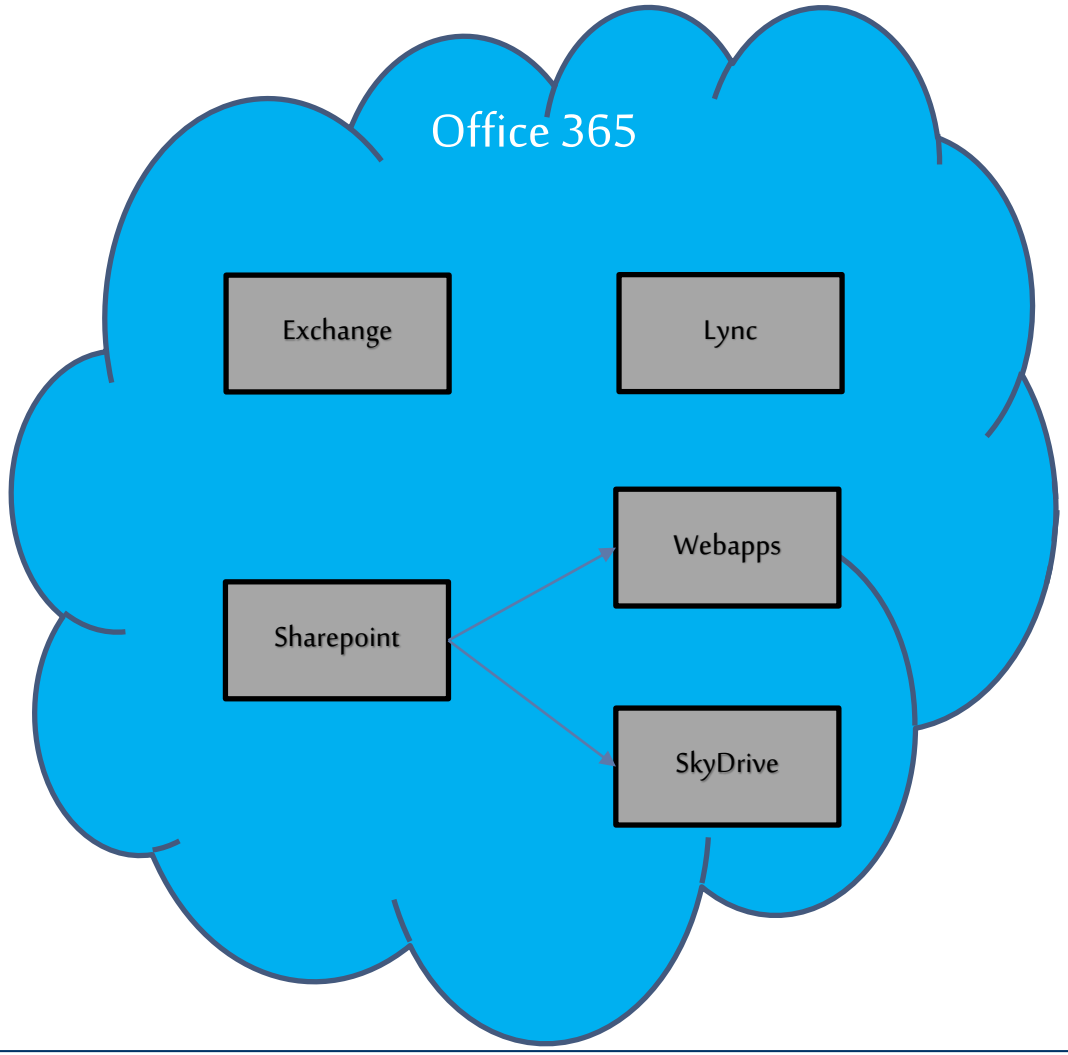
**Frank Schreiterer**

# Agenda

1. Office 365
2. ADFS (Active Directory Federation Services)
3. ADFS und Office 365
4. Kopplung Shibboleth und ADFS
5. Shibboleth – Authentifizierung an Office 365
6. Probleme und Lösungen
7. Live-Demo
8. Fragen

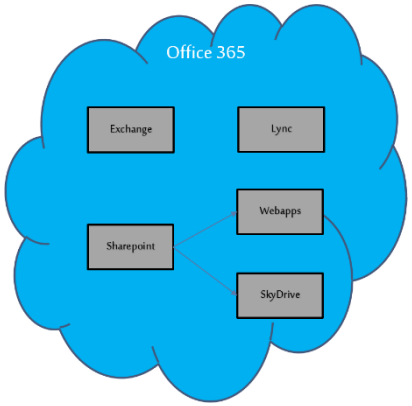
Universität Bamberg, Rechenzentrum, Frank Schreiterer
Feldkirchenstraße 21 | 96052 Bamberg | Tel. +49 (0)951 863-1356 | frank.schreiterer@uni-bamberg.de | www.uni-bamberg.de/rz/

# 1. Office 365




Universität Bamberg, Rechenzentrum, Frank Schreiterer
Feldkirchenstraße 21 | 96052 Bamberg | Tel. +49 (0)951 863-1356 | frank.schreiterer@uni-bamberg.de | www.uni-bamberg.de/rz/

# 1. Office 365 – Nutzerverwaltung




1. nicht automatisiert
   1. per Hand
   2. Massenimport per CSV

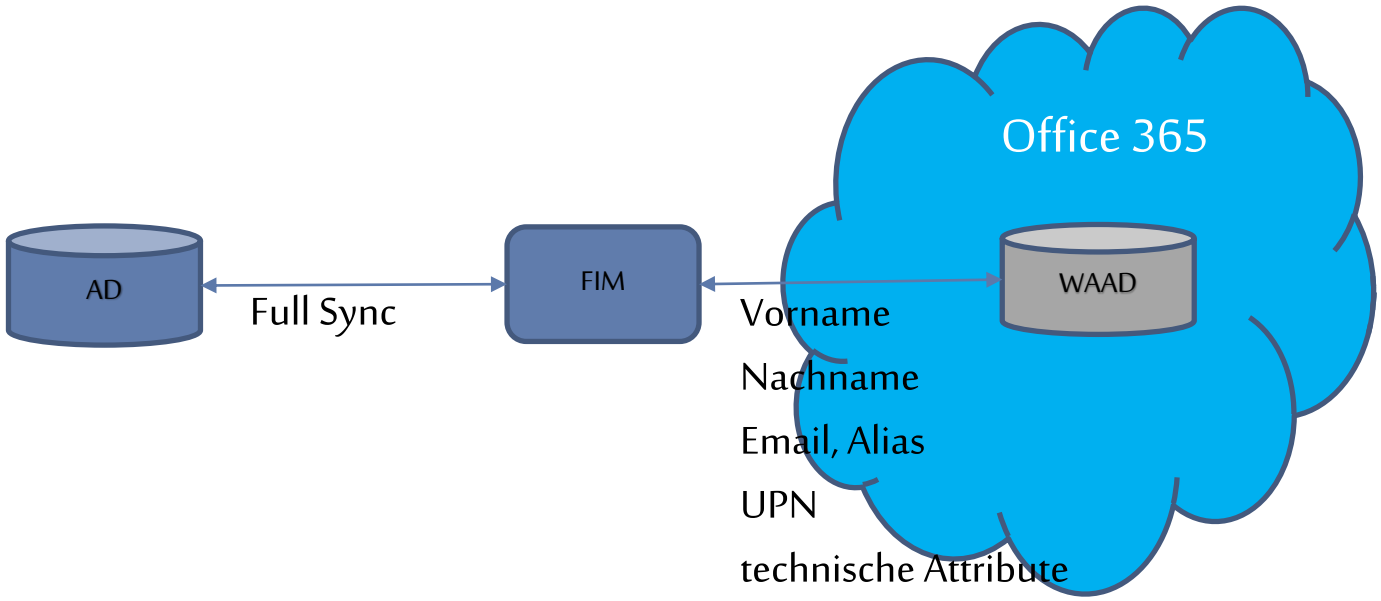
   Probleme: Synchronisation mit Nutzerverzeichnis und Passwortsynchronisation
2. automatisiert
   1. Synchronisation lokales AD mit WAAD, Passwort Cloud

      Problem: Passwörter ggf. asynchron
   2. Synchronisation lokales AD mit WAAD, Passwort lokal

      ABER: zusätzlich ADFS notwendig

Universität Bamberg, Rechenzentrum, Frank Schreiterer
Feldkirchenstraße 21 | 96052 Bamberg | Tel. +49 (0)951 863-1356 | frank.schreiterer@uni-bamberg.de | www.uni-bamberg.de/rz/

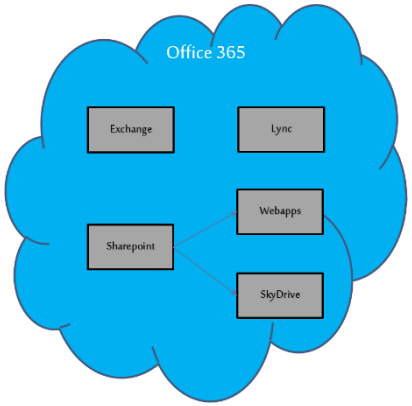
# 1. Office 365 – Nutzersynchronisation




Universität Bamberg, Rechenzentrum, Frank Schreiterer
Feldkirchenstraße 21 | 96052 Bamberg | Tel. +49 (0)951 863-1356 | frank.schreiterer@uni-bamberg.de | www.uni-bamberg.de/rz/

# 1. Office 365 – Authentifizierung

1. WAAD (Passwort in Cloud)
2. Shibboleth direkt (schlecht bis nicht unterstützt)
3. AD über ADFS lokal

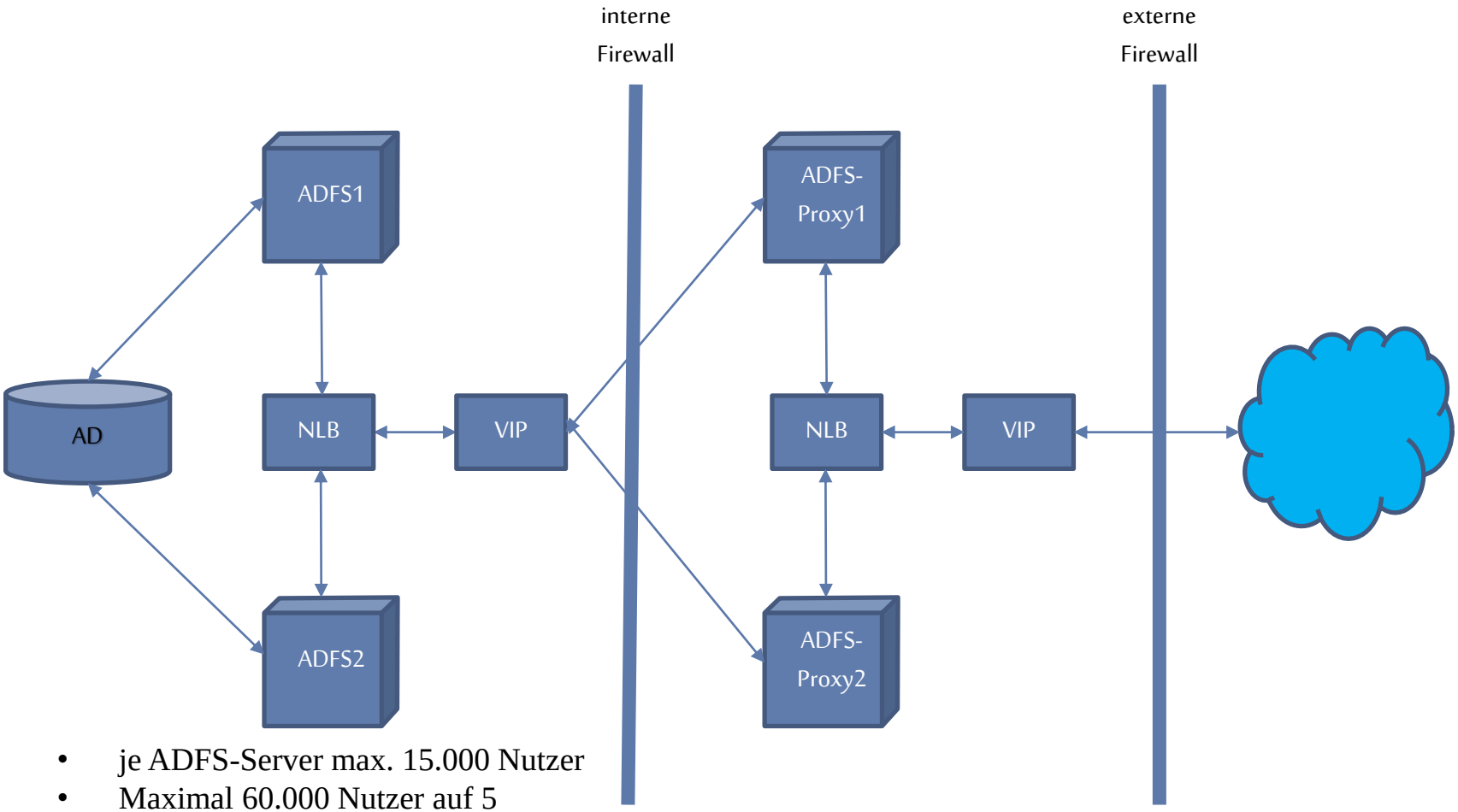



Universität Bamberg, Rechenzentrum, Frank Schreiterer
Feldkirchenstraße 21 | 96052 Bamberg | Tel. +49 (0)951 863-1356 | frank.schreiterer@uni-bamberg.de | www.uni-bamberg.de/rz/

# 2. ADFS (Active Directory Federation Services)

- Funktionsweise ähnlich Shibboleth
- Authentifizierung nicht nur per WWW möglich
- nicht plattformunabhängig (Windows Server 2012 bzw. 2008)
- Authentifizierungs- und Attributverzeichnis Active Directory (Standard)
- Datenbanken / LDAP als Attributspeicher einbindbar
- SAML-Anbieter als Anspruchsanbieter einbindbar (Authentifizierung und Attribute)

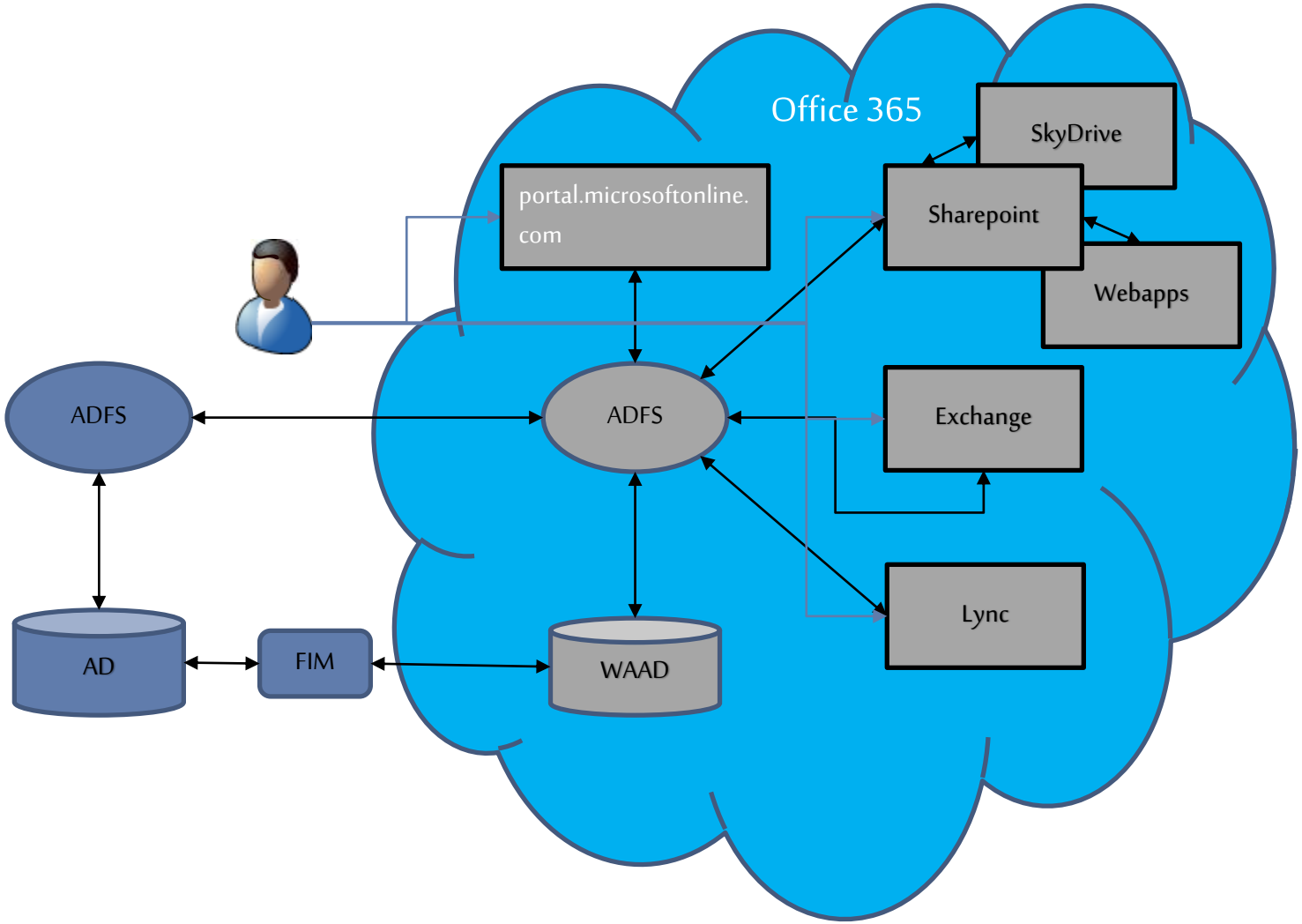
# 2. ADFS - Setup




- je ADFS-Server max. 15.000 Nutzer
- Maximal 60.000 Nutzer auf 5 Servern, dann zusätzlich MSSQL-Server-Lösung notwendig

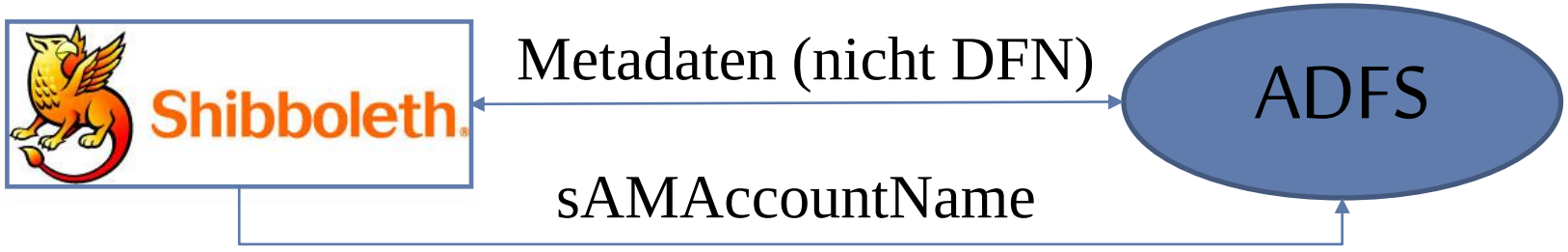
Universität Bamberg, Rechenzentrum, Frank Schreiterer
Feldkirchenstraße 21 | 96052 Bamberg | Tel. +49 (0)951 863-1356 | frank.schreiterer@uni-bamberg.de | www.uni-bamberg.de/rz/

# 3. ADFS und Office 365




Universität Bamberg, Rechenzentrum, Frank Schreiterer
Feldkirchenstraße 21 | 96052 Bamberg | Tel. +49 (0)951 863-1356 | frank.schreiterer@uni-bamberg.de | www.uni-bamberg.de/rz/

# 4. Kopplung Shibboleth und ADFS

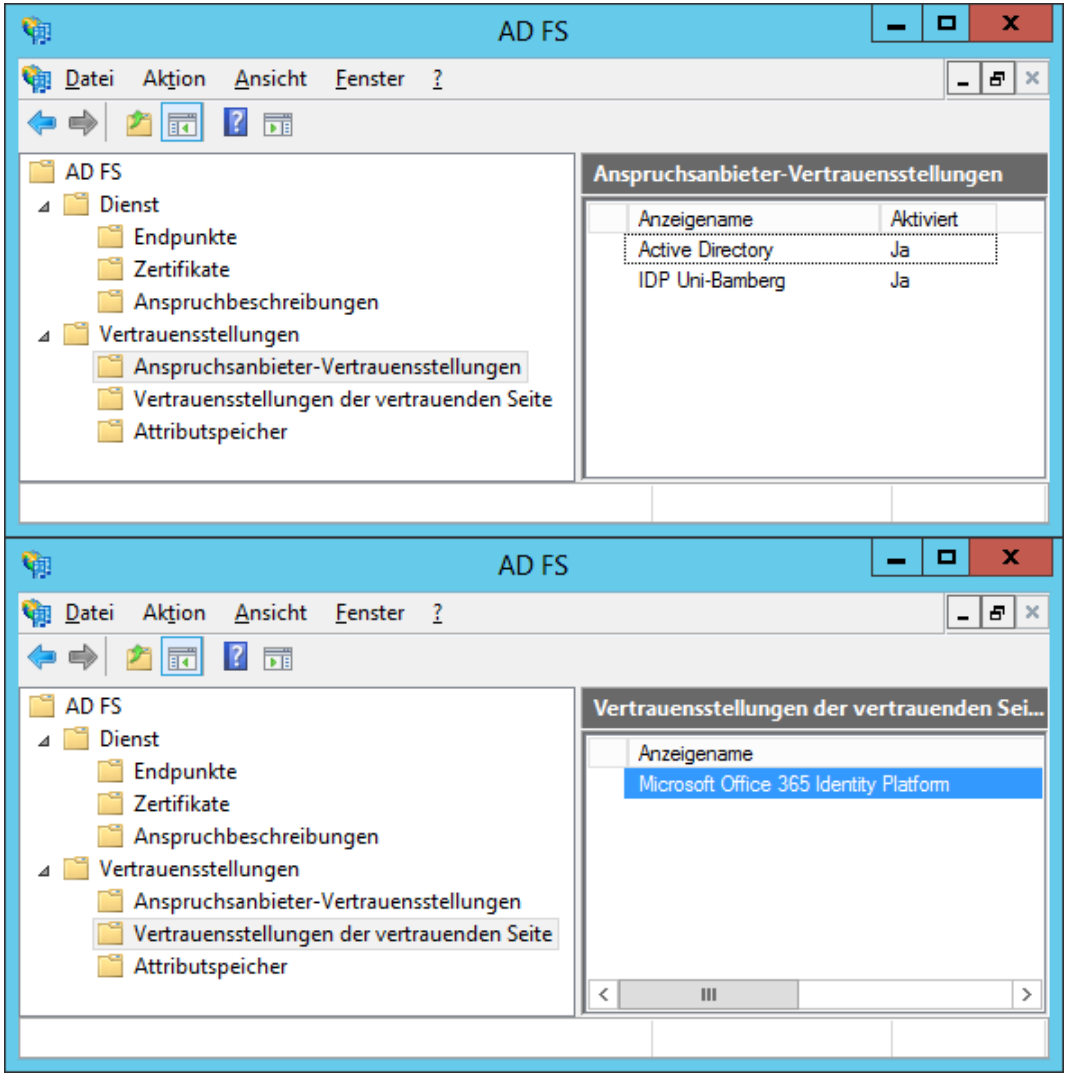



Rolle: IdP

Rolle: SP und IdP

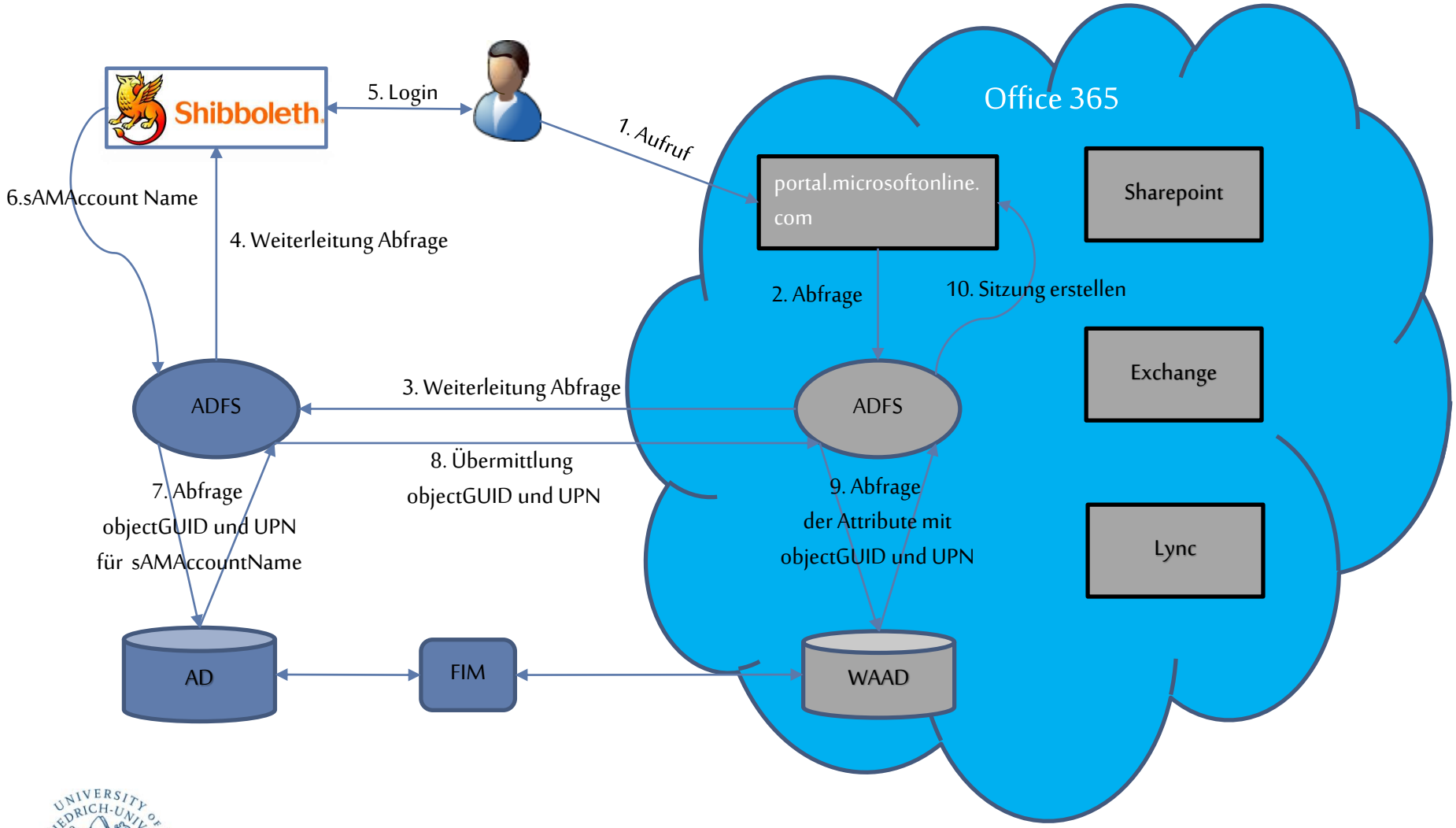
Universität Bamberg, Rechenzentrum, Frank Schreiterer
Feldkirchenstraße 21 | 96052 Bamberg | Tel. +49 (0)951 863-1356 | frank.schreiterer@uni-bamberg.de | www.uni-bamberg.de/rz/

# 4. Kopplung Shibboleth und ADFS




Universität Bamberg, Rechenzentrum, Frank Schreiterer
Feldkirchenstraße 21 | 96052 Bamberg | Tel. +49 (0)951 863-1356 | frank.schreiterer@uni-bamberg.de | www.uni-bamberg.de/rz/

# 5. Shibboleth – Authentifizierung an Office 365

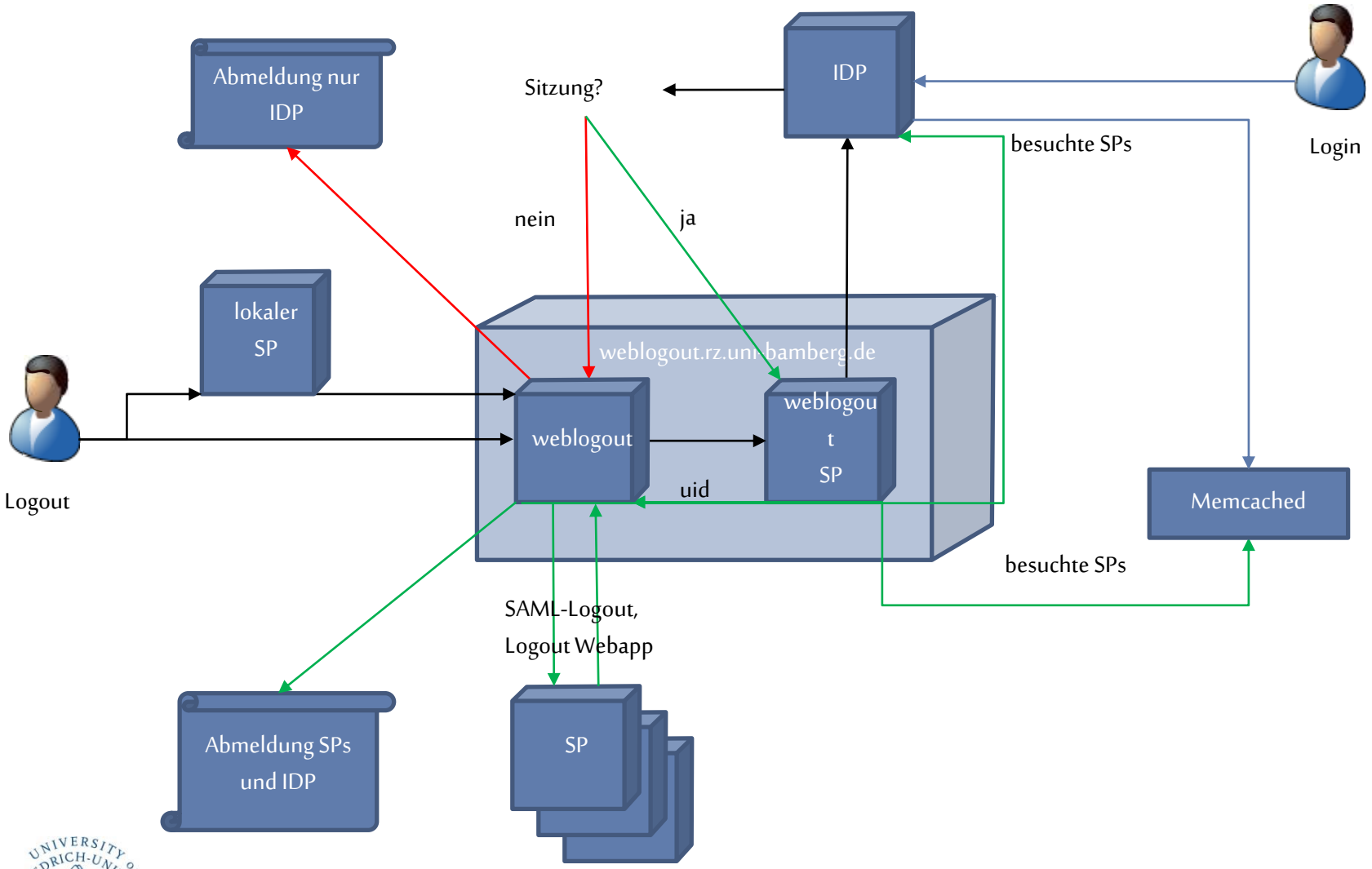



Universität Bamberg, Rechenzentrum, Frank Schreiterer
Feldkirchenstraße 21 | 96052 Bamberg | Tel. +49 (0)951 863-1356 | frank.schreiterer@uni-bamberg.de | www.uni-bamberg.de/rz/

# 6. Probleme und Lösungen

- portal.microsoftonline.com und Shibboleth: zweimalige Eingabe des Nutzernamens erforderlich
  - ✓ Einrichtung einer Umleitung mit URL auf lokales ADFS und Einrichtung eines DNS-Eintrags o365.uni-bamberg.de
- ADFS-Login-Seite zeigt Anspruchsanbieter Vertrauensstellungen als Auswahldialog beim Login an, Active Directory kann nicht als Anspruchsanbieter deaktiviert werden
  - ✓ Überschreiben der Collection der Anspruchsanbieter mit Shibboleth-IdP → ADFS leitet ohne Zwischenanzeige an Shibboleth-IdP weiter
- Logout in Office 365 wirkungslos, da Shibboleth-Sitzung nur für ADFS abgemeldet wird
  - ✓ Logout-Dienst für Shibboleth auf SAML-Basis (und Anwendungsebene)
  - ✓ URL-Rewrite für Logout-URLs auf ADFS-Proxy-Servern

# 6. Probleme und Lösungen – Weblogout Universität Bamberg




Universität Bamberg, Rechenzentrum, Frank Schreiterer
Feldkirchenstraße 21 | 96052 Bamberg | Tel. +49 (0)951 863-1356 | frank.schreiterer@uni-bamberg.de | www.uni-bamberg.de/rz/

# 7. Live-Demo


Universität Bamberg, Rechenzentrum, Frank Schreiterer
Feldkirchenstraße 21 | 96052 Bamberg | Tel. +49 (0)951 863-1356 | frank.schreiterer@uni-bamberg.de | www.uni-bamberg.de/rz/

# 8. Fragen


Vielen Dank!

Universität Bamberg, Rechenzentrum, Frank Schreiterer
Feldkirchenstraße 21 | 96052 Bamberg | Tel. +49 (0)951 863-1356 | frank.schreiterer@uni-bamberg.de | www.uni-bamberg.de/rz/