UNIVERSITÄT DUISBURG ESSEN

CampusSource Workshop 2007

# - Identity Management -

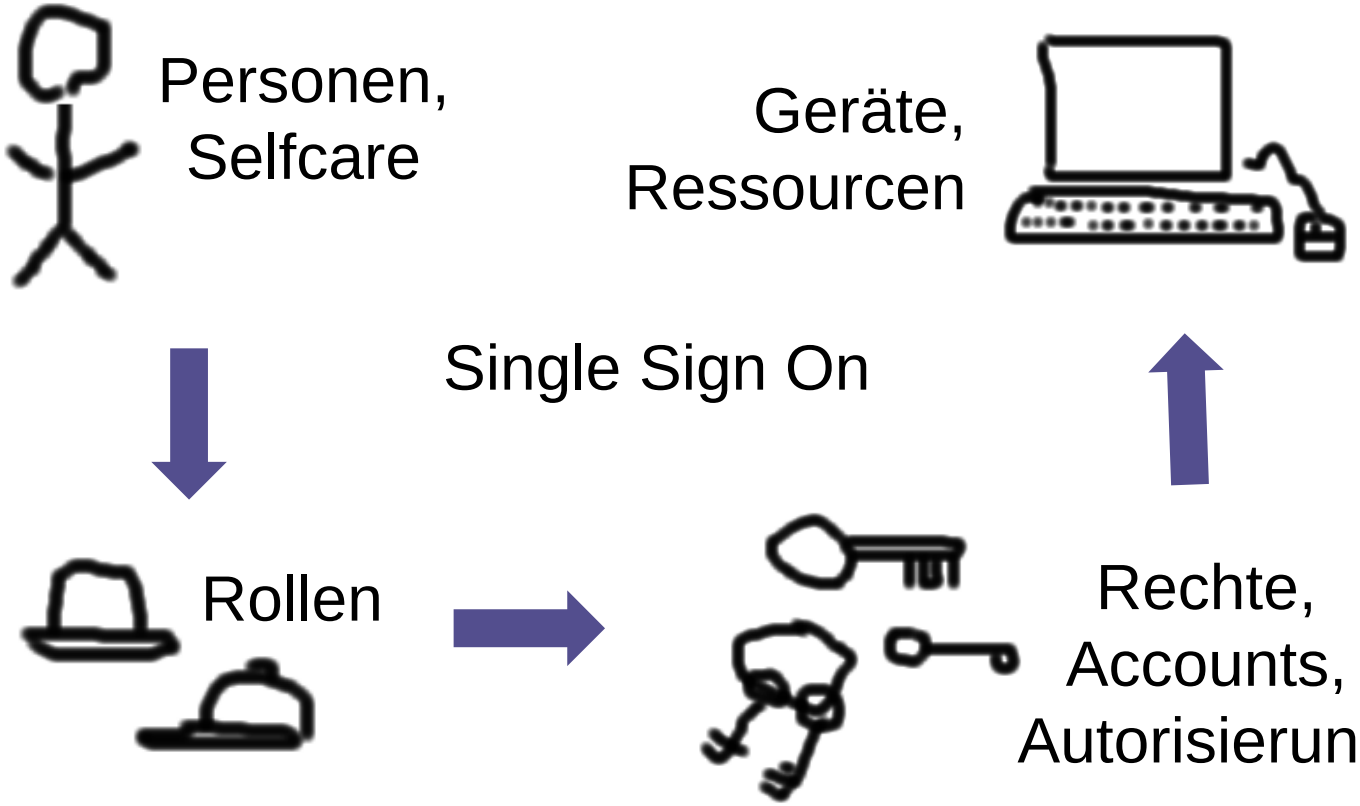
## Überblick und Entwicklungsstand Open Source Komponenten

Dipl.-Wirt.Inform. Frank Lützenkirchen
Universitätsbibliothek Duisburg-Essen
luetzenkirchen@ub.uni-duisburg-essen.de

# Agenda

- Identity Management (IDM):
  Begriff, Ziele, Architektur
- IDM und Dienstintegration
  an der Universität Duisburg-Essen
- Single Sign On
  Architekturen und Lösungen
- CAS: Central Authentication Service
- Shibboleth

# Identity Management



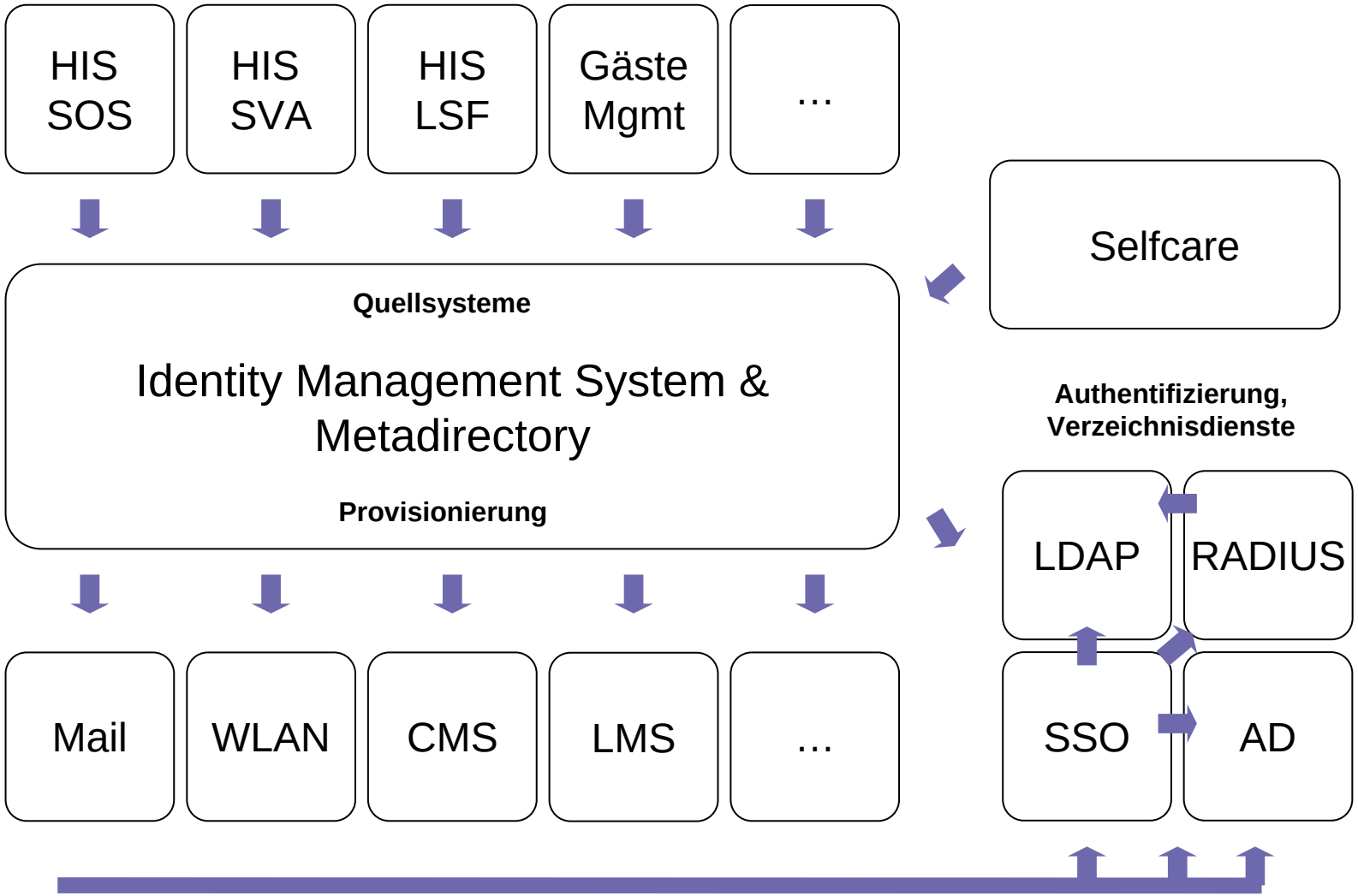
# Treibende Kräfte

- Leistungsfähige, kostengünstige, allenorts verfügbare Netze
  - DSL, Mobile Endgeräte, WLAN, …
- Integration und Konvergenz von Netzen, Services, Geräten
  - VoIP, Triple Play, IPhone, …
- Ubiquitous Computing
  - Allgegenwärtigkeit der Informationsverarbeitung
- Digital Lifestyle:
  - Web 2.0: Social Software, Blogs, Flickr, Wikipedia, Google
  - Anspruch, anstehende Aufgaben zeit- und ortsunabhängig online erledigen zu können
- Internet als primäre, einzig wahrgenommene Informationsquelle
  - Anforderungen an Aktualität und Qualität der Daten
- Wettbewerb um Studierende, Kundenorientierung: Services
- Hochschulreform, Bologna-Prozess: Komplexität des Wandels
- Kostendruck, sinkende Etats: Effiziente Prozesse

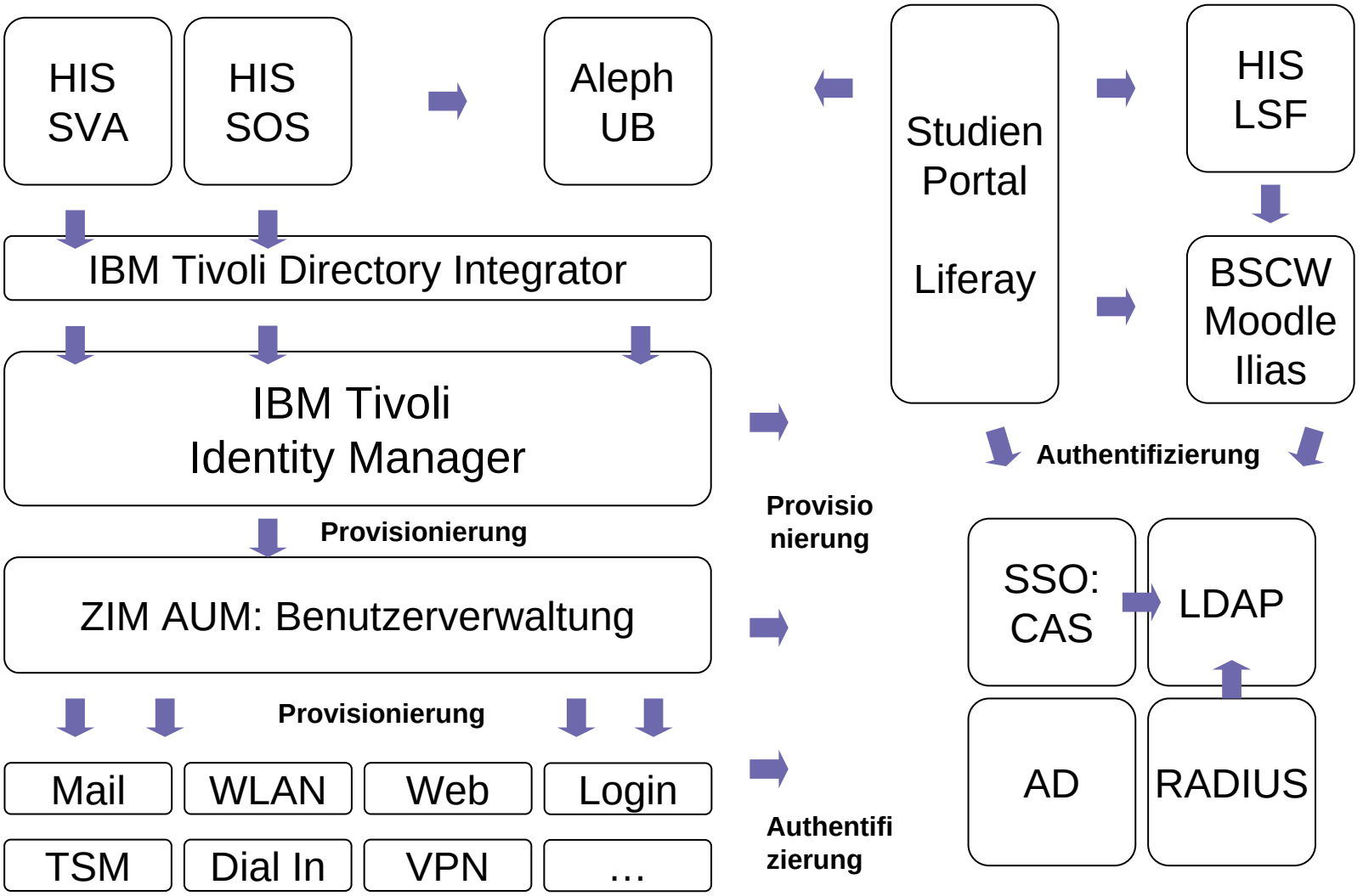
# Ziele

- Reduktion des Administrationsaufwands
  - Weg von der manuellen Benutzer- und Rechteverwaltung
  - Dublette Verwaltungsprozesse, Synchronisationsaufwand
- Integration von Diensten
  - Personalisierte Portale, Single Sign On
  - Interaktion von Diensten, auch hochschulübergreifend
- Aktualität und Qualität von Daten und Webauftritt
  - Kontaktinformationen im Internet: direkt, schnell, konsistent
- Informationelle Selbstbestimmung, Datensicherheit
  - Einsicht und Auskunft: Welche Daten wo und warum?
  - Datensparsamkeit, Verfolgung von Transaktionen
  - Selfcare-Funktionen
  - Potentielle Angriffspunkte eliminieren: unzugeordnete/abgelaufene Accounts, unnötige Datenhaltung

# Identity Management Architektur



# Ist-Architektur Universität Duisburg-Essen



# Tivoli Directory Integrator: Konnektor SOS/ITIM

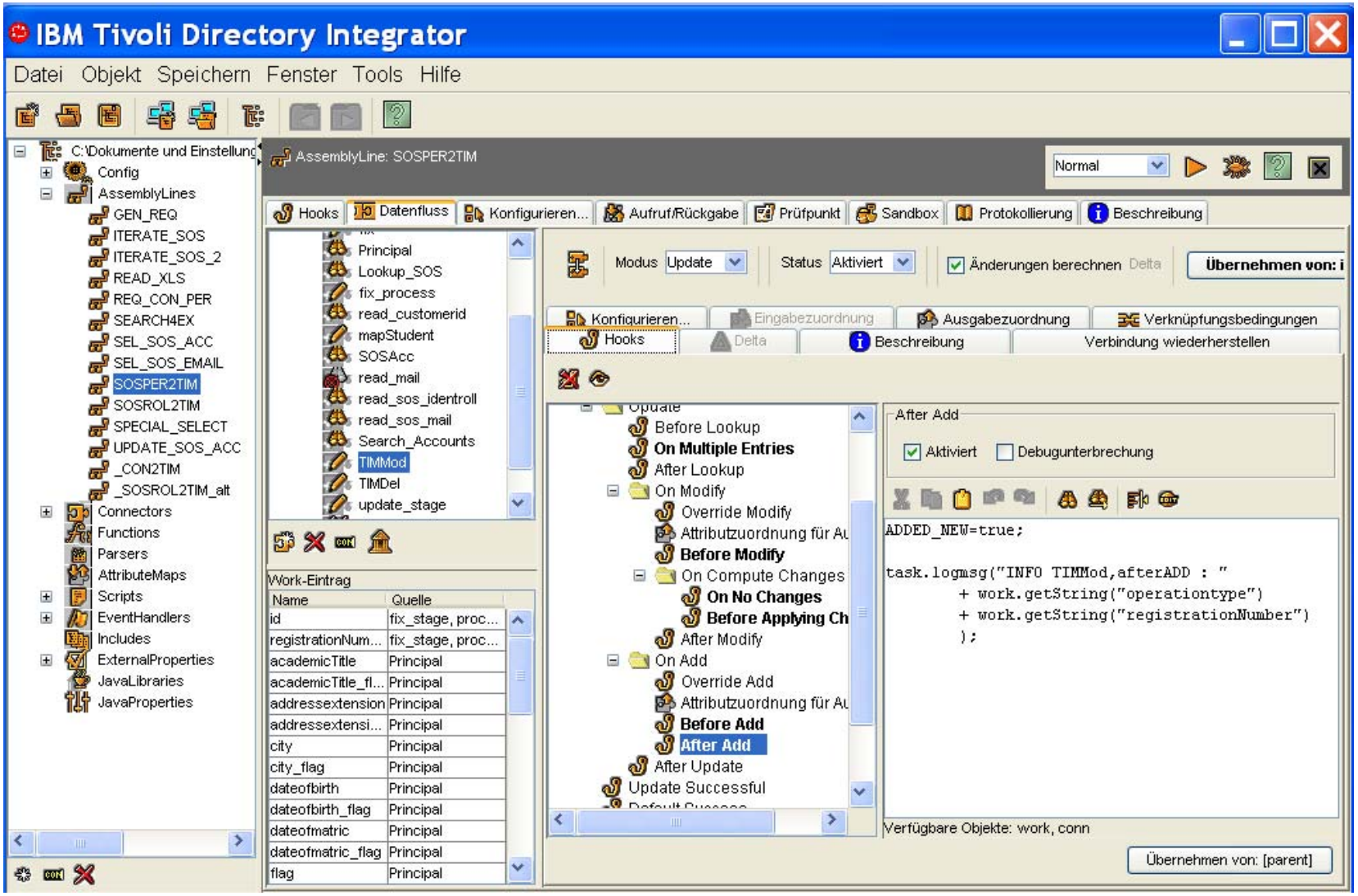



Abbildung: Dr. Burkhard Wald, Zentrum für Informations- und Mediendienste, Univ. Duisburg-Essen

# ITIM: Definition dynamische Rolle „Student“

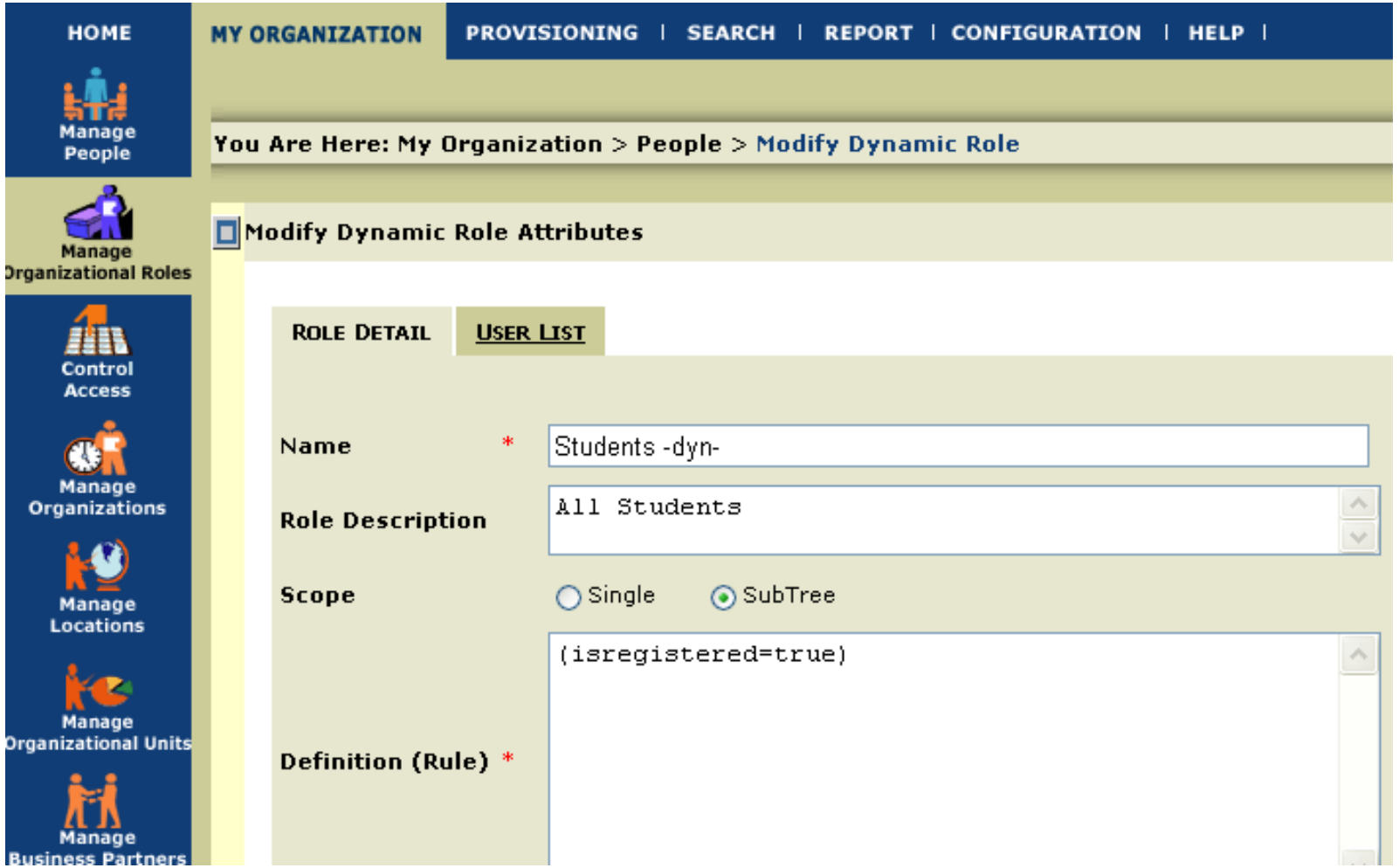



Abbildung: Dr. Burkhard Wald, Zentrum für Informations- und Mediendienste, Univ. Duisburg-Essen

# ITIM: Provisionierungsregel definieren

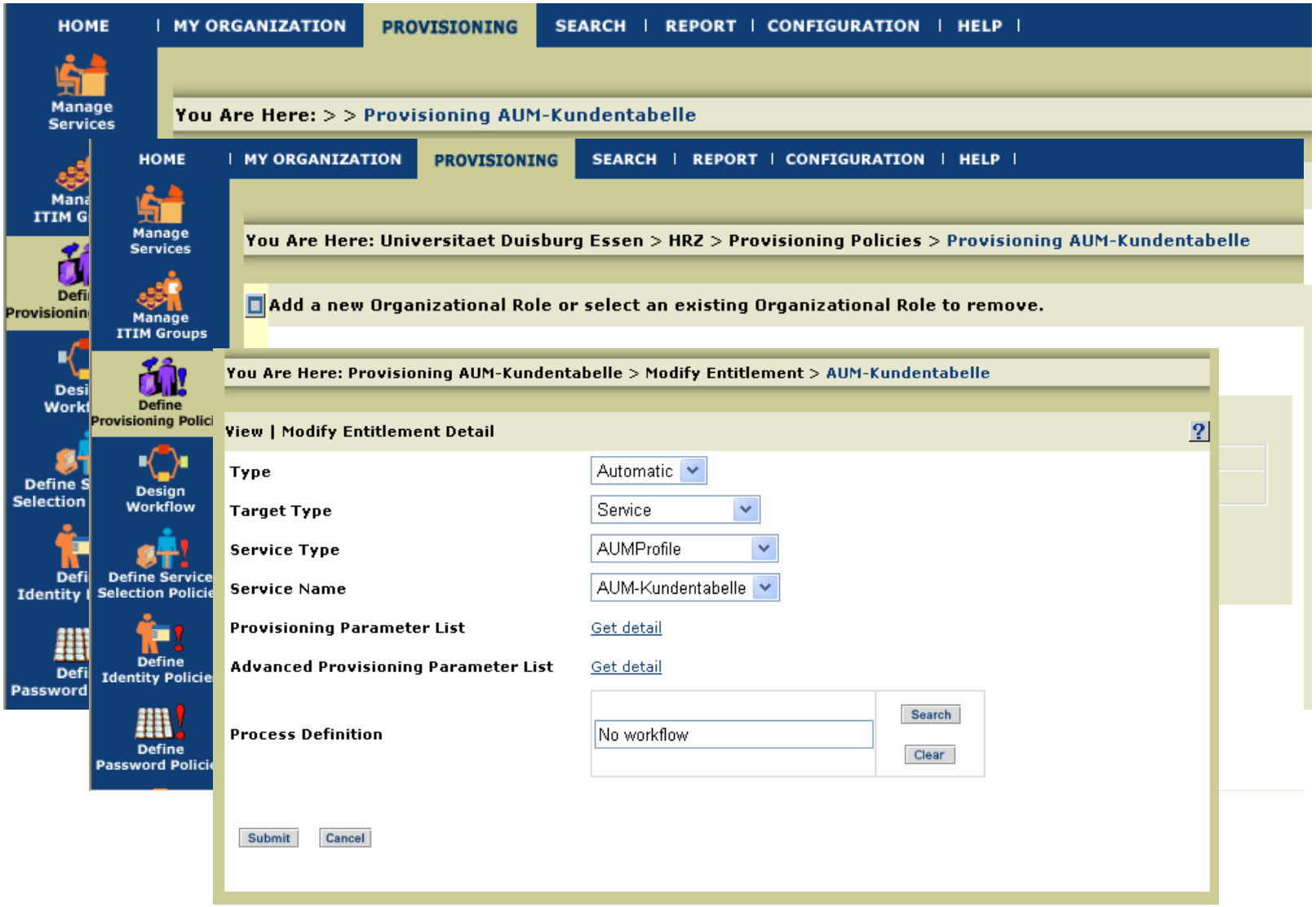



Abbildung: Dr. Burkhard Wald, Zentrum für Informations- und Mediendienste, Univ. Duisburg-Essen

# ZIM Benutzerverwaltung: AUM (1)

| | |
|---|---|
| Kunden_nr | 11505 |
| Eintragsdatum | 2001-07-18 |
| Austrittsdatum | |
| Name | Lützenkirchen |
| Vorname | Frank |
| Namenszusatz | |
| Titel | |
| Geschlecht | m |
| Alumni-Status | |
| Status | Wiss. Mitarbeiter/in |
| FB | Bibliothek |
| Institut | |
| Rechnungsstellung | Nein |
| Matrikelnummer | |
| Immatrikulations-Status | |
| Bemerkungen | |
| Telefon | 0201/183-2124 |
| Hauptaccount | hrz120 |
| E_mail | frank.luetzenkirchen@uni-due.de |
| Straße | |
| PLZ | |
| Ort | |
| Sprecher der Hochschulgruppe | |
| Austrittsgrund | |

Telefonbuch abfragen

Zeige alle Alias-Einträge

# ZIM Benutzerverwaltung: AUM (2)

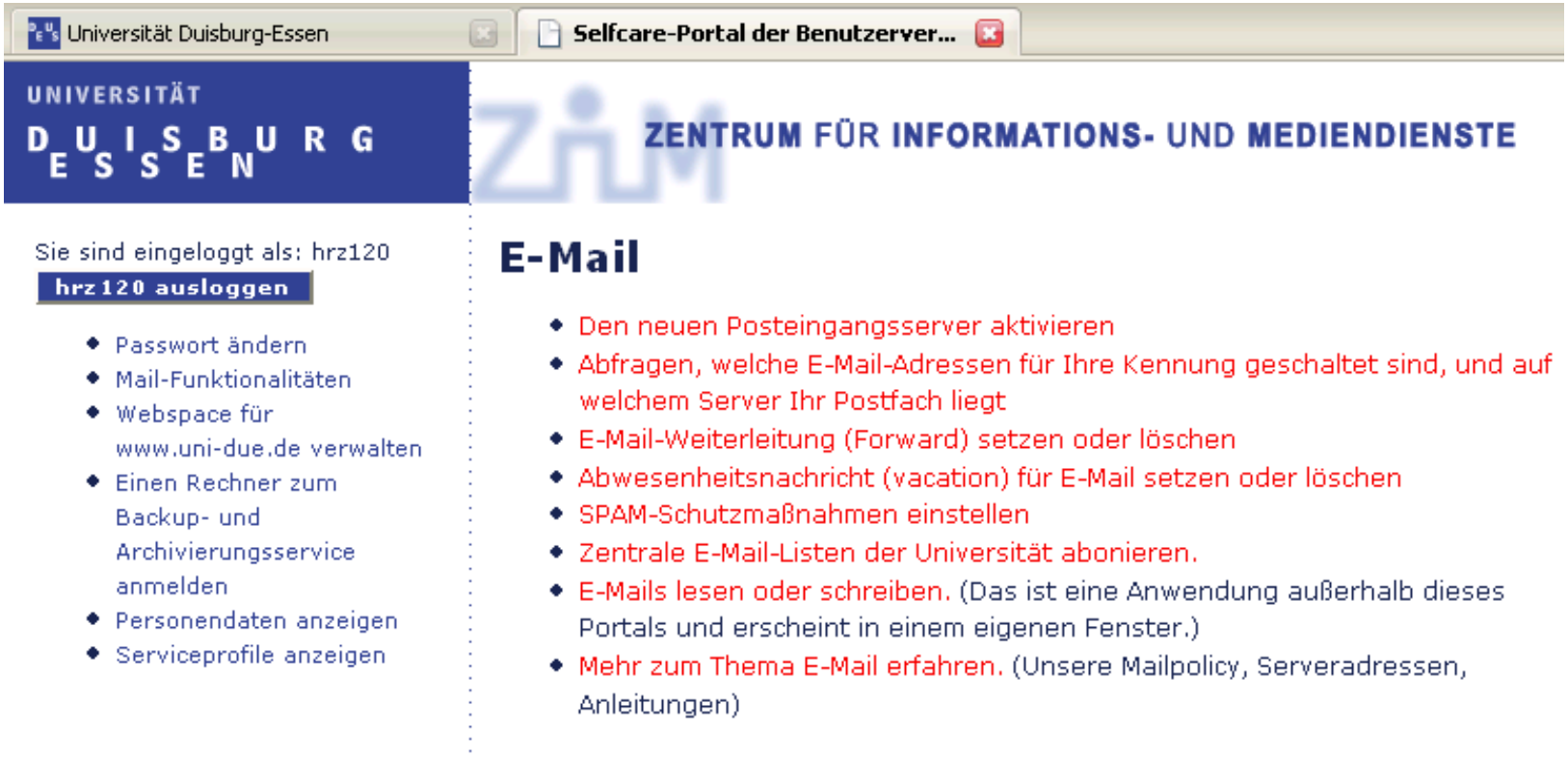
| | AIXRS1 | SP2 | UGE-HERMES | FS1 | FS2 | MAILBOX | Code-Schl. | Mail-Adresse | TSM | EXCHANGE | Freies Mail-Fach | RVNRW | GROUP | RADIUS | NIS | ZV | BB |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| hrz120 | ☑ | yes | yes | ☐ | yes | yes | ☐ | yes | ☐ | ☐ | ☐ | ☐ | ☐ | yes | yes | ☐ | ☐ |
| hrz120.hrz | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☑ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| hy0231 | ☐ | ☐ | ☐ | ☐ | ☐ | yes | ☐ | yes | ☐ | ☐ | ☐ | ☐ | ☐ | yes | yes | ☐ | ☐ |
| icmcont | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| lhrz300.hrz | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☑ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| mcrfluet | ☐ | yes | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | yes | ☐ | ☐ | ☐ |
| mobilue.ub | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☑ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| mycore1.ub | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☑ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| mycore2.ub | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | yes | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| pcfr1a.bibl | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☑ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| wally.hrz | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☑ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Neuer Account | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

Accounts und Dienste des Benutzers

# ZIM Benutzerverwaltung: AUM (3)

| | | |
|---|---|---|
| SOFTQUOTA: | 50000 | |
| HARDQUOTA: | 100000 | |
| GECOS: | Frank Luetzenkirchen, HRZ | |
| **FS2** | jobonchange | Y,YY |
| Homedirgruppe: | system | |
| Primaergruppe: | hrz | |
| Quota: | 250000 | |
| **SP2** | jobonchange | Y,YY |
| Durchgeführte Jobs | 13.02.2006 14:09 update_sp2 | |
| HOME: | /u/ | |
| SHELL: | /bin/ksh | |
| PGROUP: | hrz | |
| GROUPS: | hrz, cisco | |
| SOFTQUOTA: | 200000 | |
| HARDQUOTA: | 250000 | |
| GECOS: | Frank Luetzenkirchen, | |
| NO_PASSWORD: | | Defaultwert |
| **UGEHERMES** | jobonchange | Y,YY |
| Durchgeführte Jobs | 03.04.2006 19:30 update_ugehermes | |
| Adminkennung: | | Defaultwert |
| Beschreibung: | Mitarbeiter | |
| Profilepfad: | \\hrzcluster\profile$\Hrz\Mitarbeiter | |
| Home-Verzeichnis: | \\hrzcluster\home$\Hrz\Mitarbeiter | |
| Home-Platte: | Z: | |
| Gruppen: | **Domain Users; HRZ; Postbenutzer** | |
| Administratorgruppe: | | Defaultwert |
| Anmeldescript: | benutzer.bat | |

# ZIM Benutzerverwaltung: Selfcare-Portal



# Gästeverwaltung: Online-Anmeldung

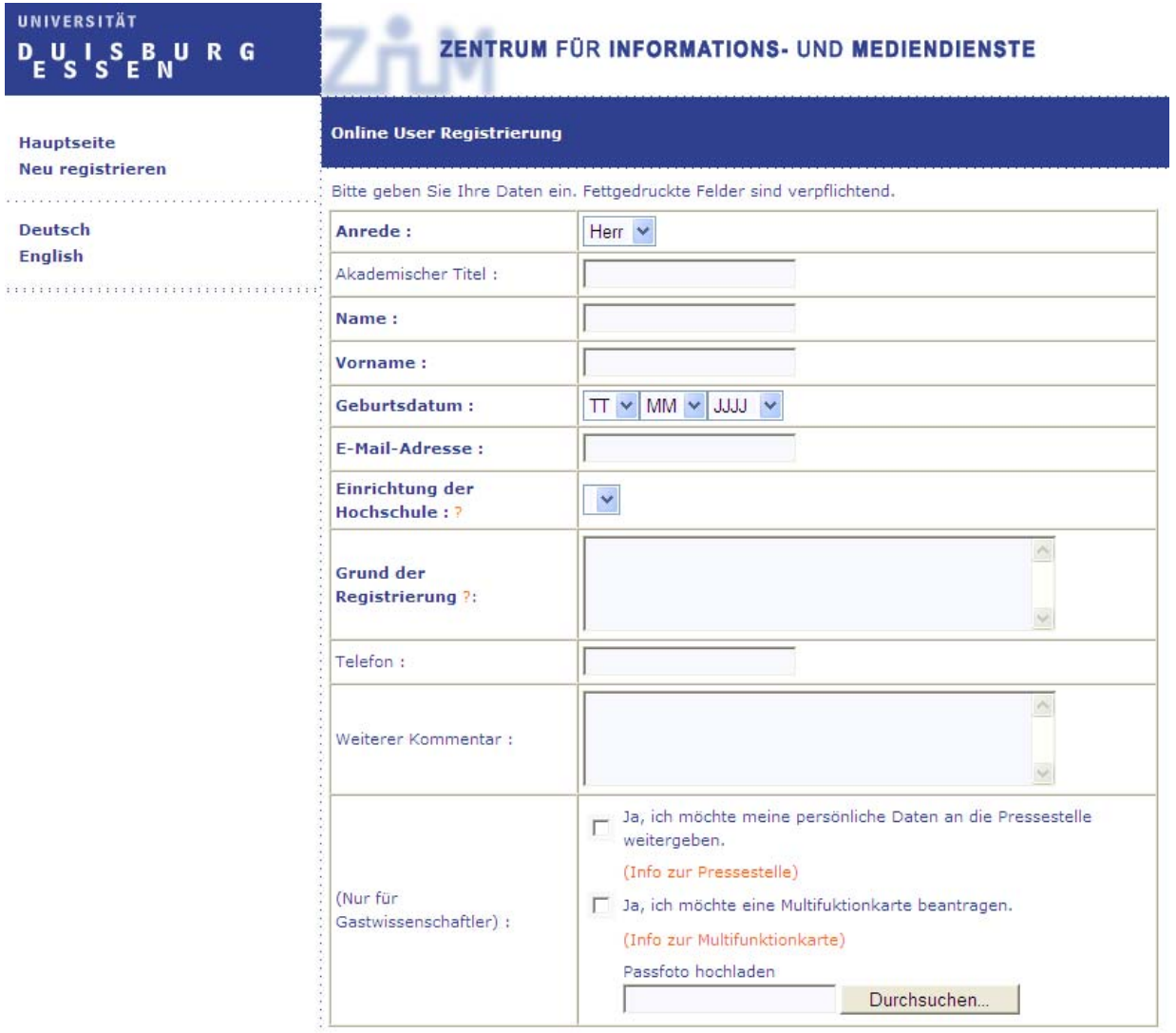



Abbildung: Dr. Burkhard Wald, Zentrum für Informations- und Mediendienste, Univ. Duisburg-Essen

# HIS LSF: Lehre, Studium, Forschung

- Online-Personenverzeichnis
- Online-Veranstaltungsverzeichnis
- Selfcare: Veranstaltungen, Kontaktinformationen

# Personensuche: WebServices Integration

- Suche nach Personen in HIS LSF über WebServices
- Kontaktinformationen, Lehrveranstaltungen aus LSF
- Publikationslisten, Volltextdokumente aus DuEPublico

# Studienportal: Liferay, Portlets, CAS

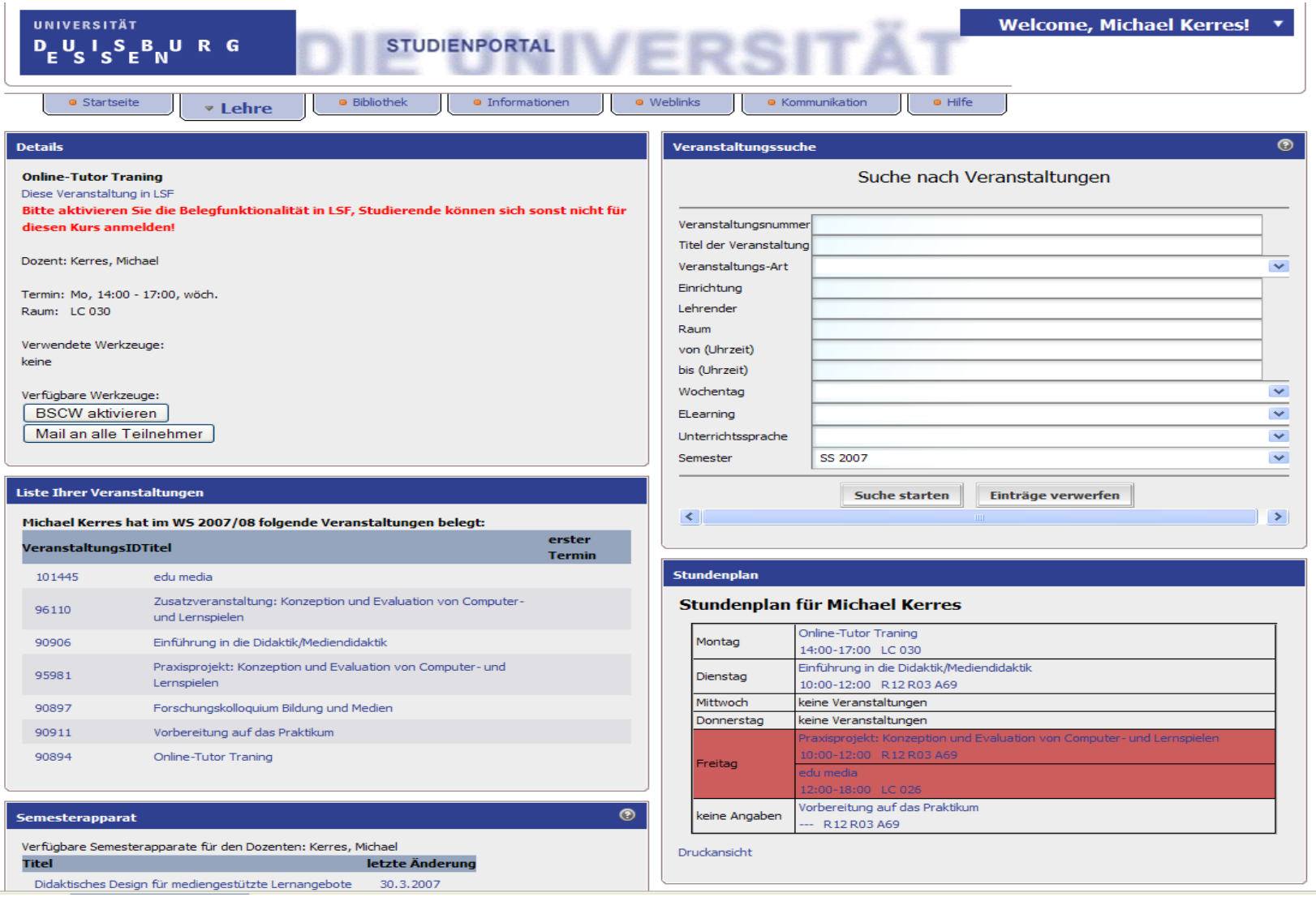
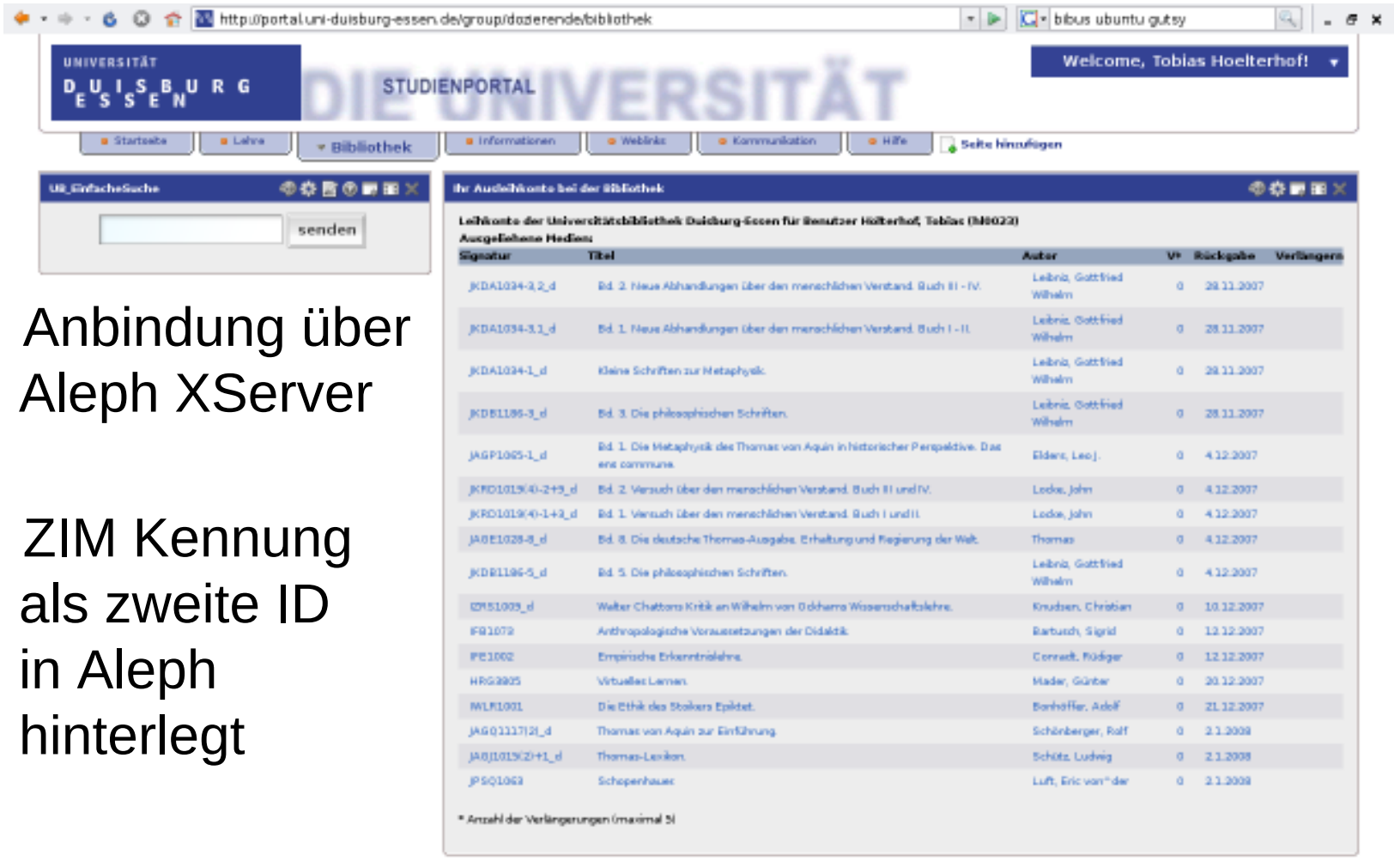



Abbildung: Prorektorat Information, Kommunikation, Medien, Prof. Kerres, Univ. Duisburg-Essen

# Studienportal: Ausleihkonto Bibliothek




- Anbindung über Aleph XServer
- ZIM Kennung als zweite ID in Aleph hinterlegt

# Single Sign On: SSO

- Einmalige Authentifizierung je Sitzung
- Danach Zugriff auf alle Dienste und Rechner, zu deren Nutzung der Anwender autorisiert ist

- Vorteile
  - Zeitersparnis, bequemere, einheitliche Nutzung
  - Sicherheitsgewinn im Passwort-Handling, in der Benutzerverwaltung
- Nachteile
  - Verfügbarkeit des SSO Service: Single Point of Failure
  - Ausspähen einer einzigen Benutzeridentität ermöglicht Zugriff auf sämtliche Dienste und Rechner

# Single Sign On: Brauche ich das überhaupt?

- „Wozu Single Sign On?
  Mein Browser hat doch einen Passwort-Manager.“

- Benutzer speichert alle Benutzerkennungen und Passwörter lokal auf dem eigenen Rechner oder im Netzwerk
- Lokaler Dienst meldet den Benutzer ggf. an

- Auch für proprietäre Systeme geeignet

# SSO Architektur: Zentraler SSO Server

- Authentifizierung wird an einen dedizierten, zentralen Server ausgelagert
- Benutzer wird zunächst an SSO Server umgeleitet
- Benutzer meldet sich beim SSO Server an und wird dort authentifiziert
- SSO Server erzeugt Ticket für Dienstserver
- Dienstserver prüft Ticket, kennt aber nicht das Passwort

- CAS
- Shibboleth

Screenshots: Dr. Burkhard Wald, Zentrum für Informations- und Mediendienste

# CAS: Central Authentication Service

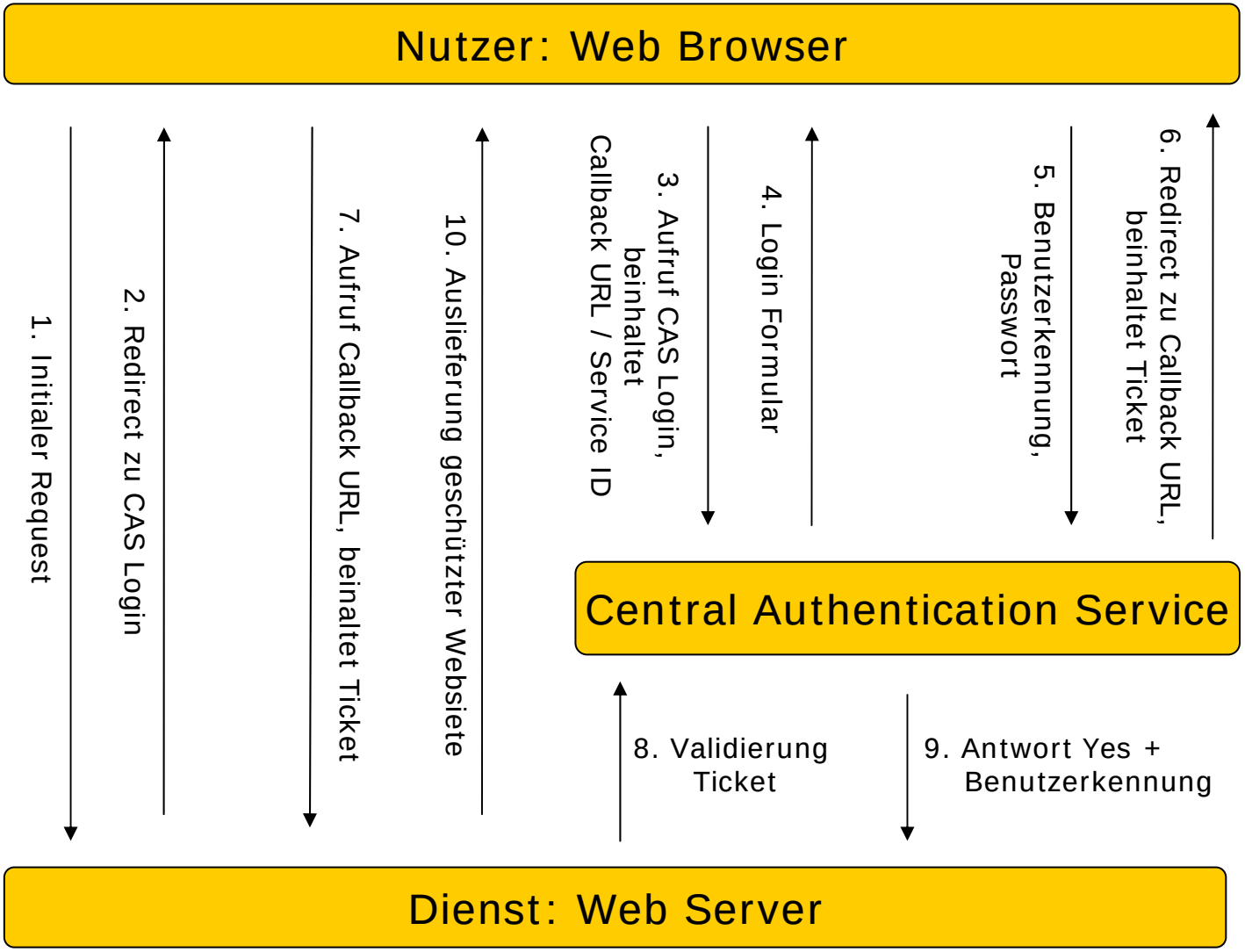
- Ursprünglich 2001 entwickelt von der Yale University
- Seit 2005:
  JA-SIG Java in Administration Special Interest Group
- Zentraler, webbasierter Authentifizierungsservice
- Server-Implementierung in Java
- Clients für Java, .NET, PHP, Perl, Apache, …
- Unterstützung in Moodle, Ilias, Stud.IP,
  BSCW, Zope, uPortal, Liferay, …
- Single Sign On realisierbar


http://www.ja-sig.org/products/cas/

# CAS Login: Universität Duisburg-Essen

- Single Sign On für
  Studienportal, Moodle, BSCW, ((Aleph)), weitere

# CAS Architektur



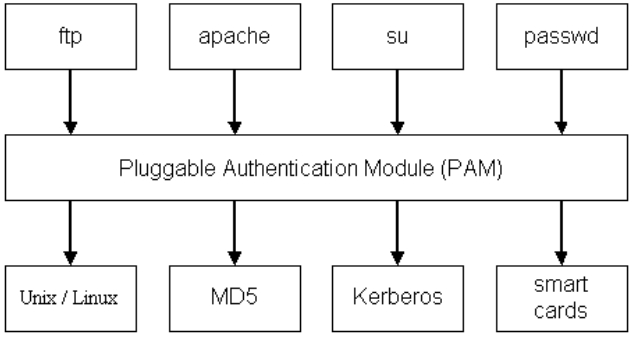
# CAS: Authentifizierung

- *Authentication Handler*: implementiert Authentifizierung
- *Principal*: Zu authenifizierender Nutzer
- *Credentials*: Identitätsbeweis, z. B. Kennung & Passwort
- Authentication Handler Implementierungen für
  LDAP, Kerberos, SPNEGO, MS Active Directory,
  Radius, JDBC (Datenbank), JAAS, X.509 Zertifikate

- CAS 2 Architektur unterstützt Proxy Agenten,
  die anstelle des ursprünglichen Nutzers Dienste aufrufen
- Optional XML-basiertes Protokoll
- CAS 3.1 unterstützt Single Sign Out:
  Aktive Benachrichtigung der registrierten Systeme
- CAS unterstützt OpenID und SAML 2.0

# JAAS: Java Authentication and Authorization Service

- Standard Java API, ermöglicht eine Anwendung unabhängig von der Authentifizierungsmethode zu implementieren, die über eine Konfigurationsdatei anpassbar ist
- LoginModule Implementierungen für LDAP, Kerberos, NT Lan Manager, Unix
- JAAS orientiert sich am Pluggable Authentication Module Framework (PAM)
- JAAS-PAM-Bridge ermöglicht Nutzung von PAM-Modulen auf Unix-Servern, darüber z. B. RADIUS




Quelle: Wikipedia

# JAAS Konfiguration: Stacked Authentication

```
/**
* Login Configuration for JAAS. First try Kerberos, then LDAP, then AD
* Note that a valid krb5.conf must be supplied to the JVM for Kerberos auth
* -Djava.security.krb5.conf=/etc/krb5.conf
*/
CAS {
com.ibm.security.auth.module.Krb5LoginModule sufficient
debug=FALSE;

edu.uconn.netid.jaas.LDAPLoginModule sufficient
java.naming.provider.url="ldap://ldap.my.org:389/dc=my,dc=org"
java.naming.security.principal="uid=cas,dc=my,dc=org"
java.naming.security.credentials="password"
Attribute="uid"
startTLS="true";

edu.uconn.netid.jaas.LDAPLoginModule sufficient
java.naming.provider.url="ldaps://ad.my.org:636/dc=ad,dc=my,dc=org"
java.naming.security.principal="cas@ad.my.org"
java.naming.security.credentials="password"
Attribute="sAMAccountName";
};
```

Quelle: Beispiel-Konfiguration aus der CAS Dokumentation

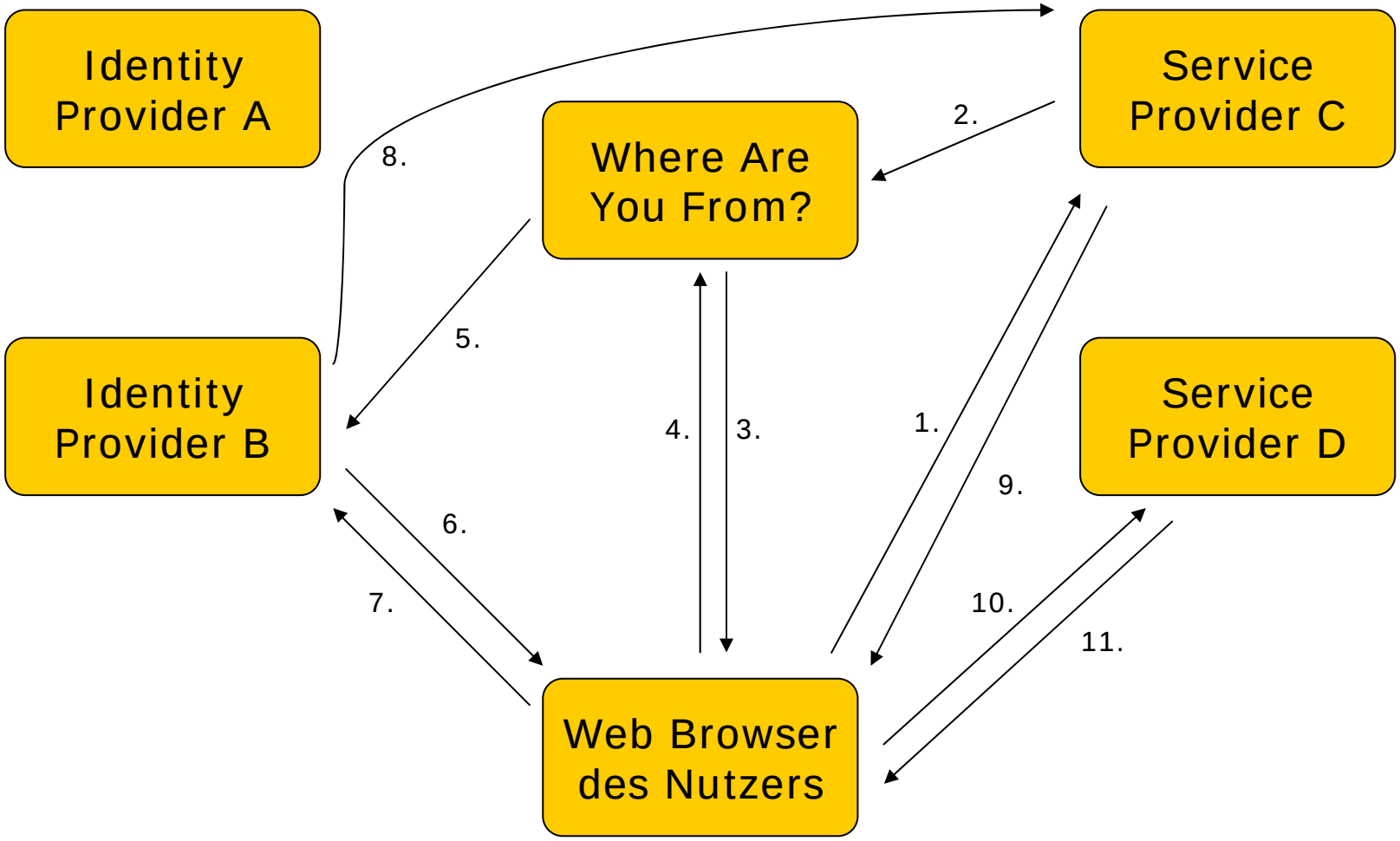
# Shibboleth

- Entwicklung der Internet2-Initiative
- Verteilte Authentifizierung und Autorisierung im Web
- Single Sign On


- SP: Service Provider, Dienst mit Shibboleth Unterstützung
- IP: Identity Provider in Heimateinrichtung, authentifiziert
- WAYF: Lokalisierungsdienst, Where are you from?

- IP kann Attribute an SP weitergeben:
  Rollenbasierte Autorisierung
- Unterstützung verteilter Architekturen, Föderationen

# Shibboleth Architektur



# DFN AAI: Deutsches Forschungsnetz Authentifizierungs- und Autorisierungsinfrastruktur

- Bundesweite Shibboleth Föderation, Dienst des DFN
- Organisatorischer, technischer Rahmen für den Austausch von Benutzerinformationen zwischen
  - wissenschaftlichen Einrichtungen (Universitäten, Institute)
  - Anbietern (kommerziell und nicht kommerziell)
- Anwendungen
  - Bibliotheksanwendungen: Recherche-Datenbanken, Verlagsangebote, DFG Nationallizenzen
    Ablösung IP-basierter Autorisierung
  - Grid Computing, Portale, E-Learning Anwendungen
- DFN AAI schafft das notwendige Vertrauensverhältnis
  - Betrieb, Richtlinien, Vertragsgestaltung, Rahmenverträge

# OpenID


OpenID is a free and easy way to use a **single digital identity** across the Internet.

With one OpenID you can login to all your **favorite websites** and forget about online paperwork!

Now, you get to choose the login that's right for you. **Get an OpenID** today!

Quelle: http://www.openid.net/

- Dezentrales, internetweites Identifizierungssystem
- Benutzer kann sich auf OpenID-unterstützten Websites anmelden, ohne dort eigenes Benutzerkonto zu haben
- Kontoverwaltung über verschiedene OpenID-Provider
- URL-basierte Identität: Informationen abrufbar

# Zusammenfassend

- Ein Identity Management ist die Basis für eine sichere, kundenorientierte, effiziente Integration von Diensten
- Rollenbasierte, automatische Autorisierung wird ermöglicht
- Dabei unterstützt die CampusSource Engine die Synchronisation, Provisionierung und Integration von Systemen
- Alle gängigen Authentifizierungmethoden wie LDAP, Kerberos, Active Directory, Radius sind z. B. über JAAS leicht in Open Source Anwendungen integrierbar bzw. in der Regel durch diese schon unterstützt
- Mit CAS und Shibboleth sind leistungsfähige, weit verbreitete Open Source Lösungen für Single Sign On (SSO) verfügbar
- Shibboleth spielt durch bundesweite Föderation zunehmend eine wichtige Rolle
- Viele CampusSource Systeme unterstützen bereits SSO und Datenübernahme aus Verzeichnisdiensten

# Vielen Dank für Ihre Aufmerksamkeit!