

# - Identity Management -

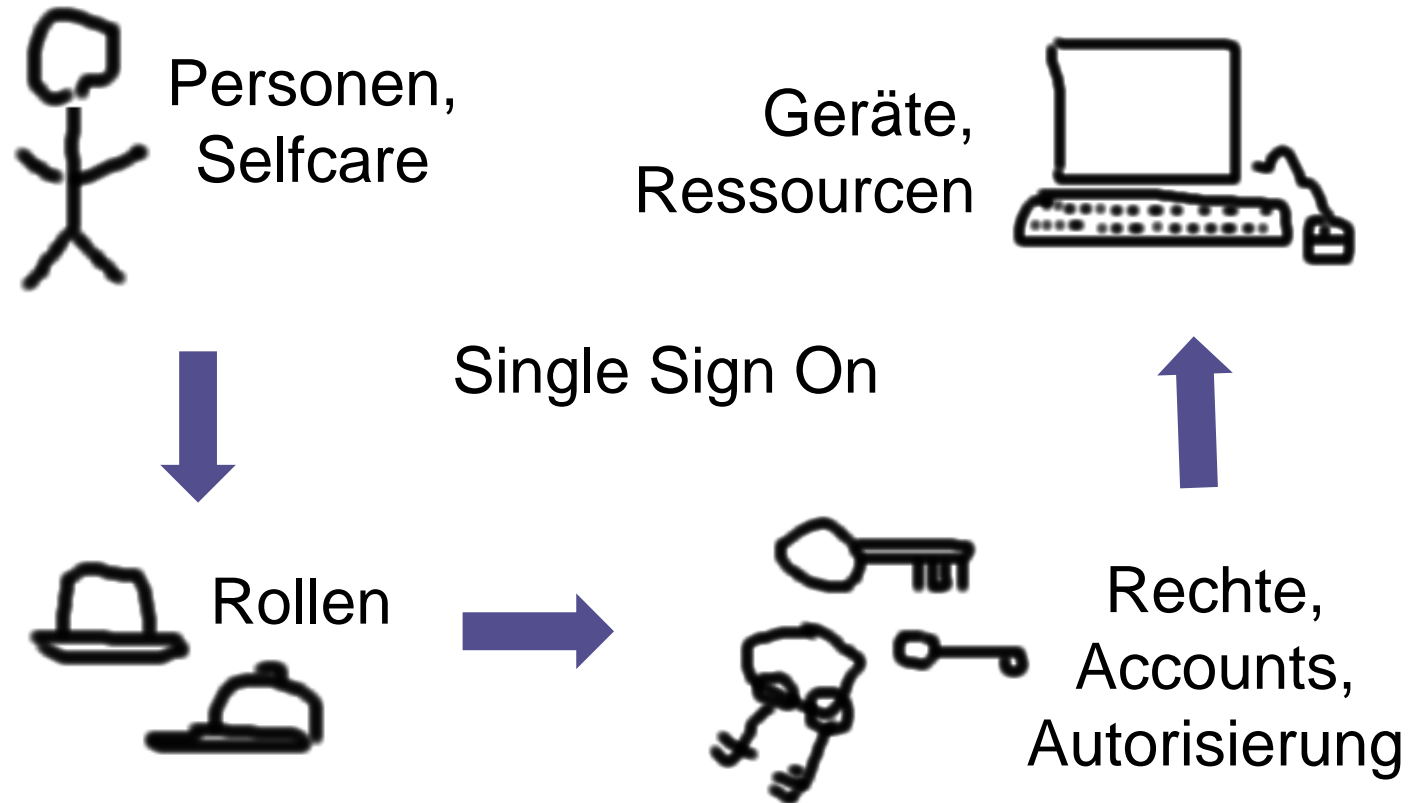
## Überblick und Entwicklungsstand Open Source Komponenten

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



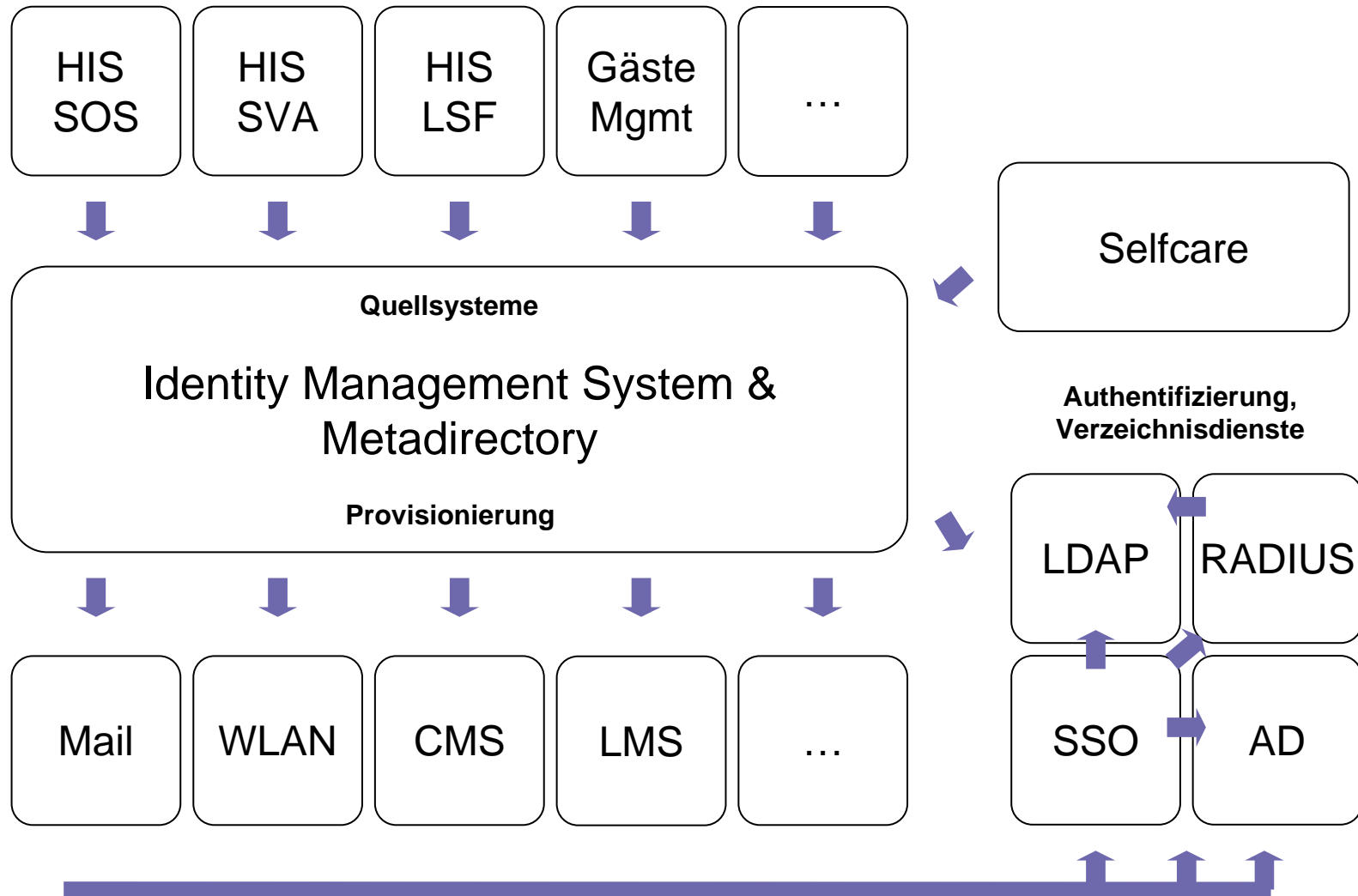
# Treibende Kräfte

- Leistungsfähige, kostengünstige, allorts 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

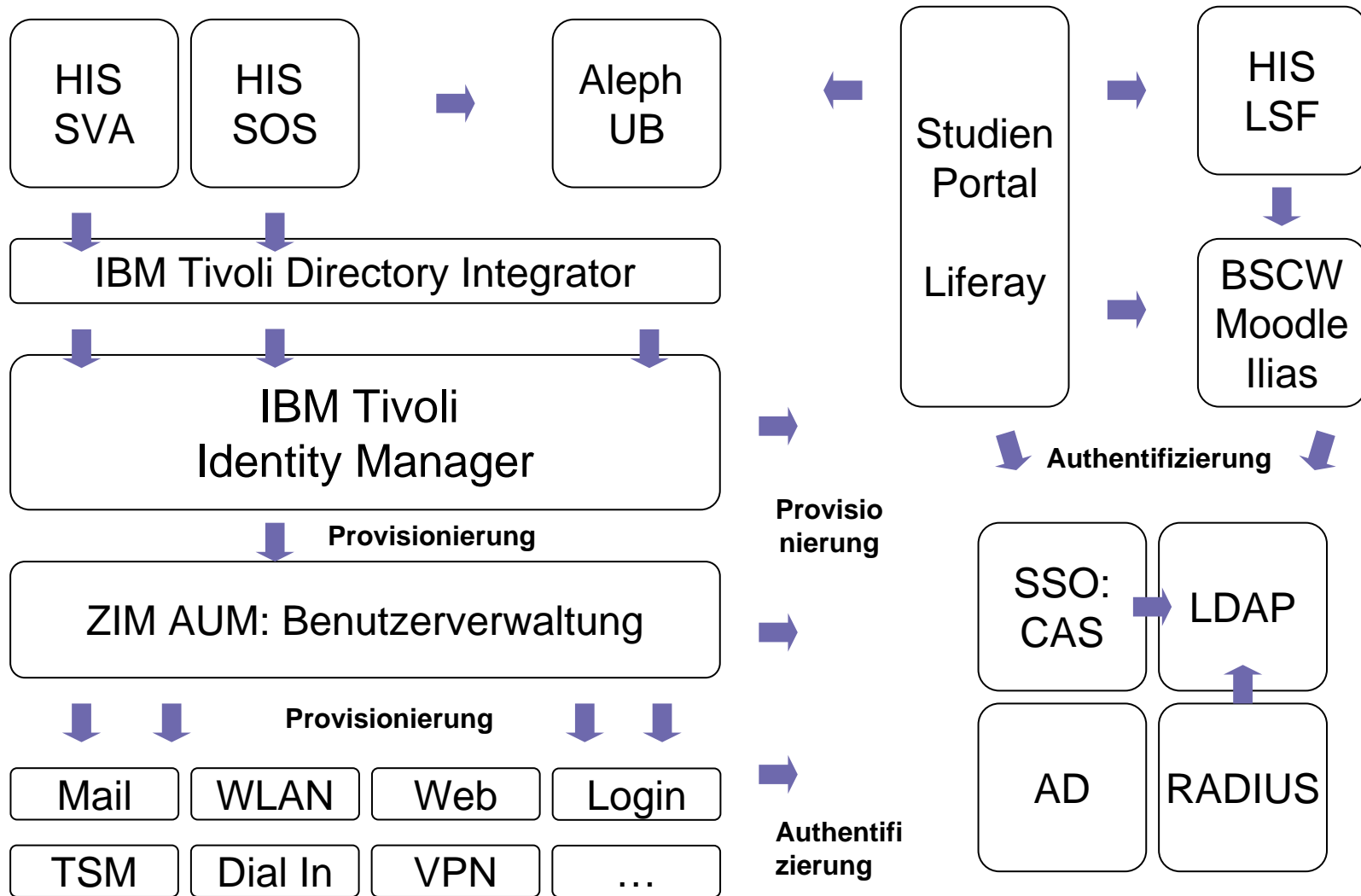
# Ziele

- 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

The screenshot displays the IBM Tivoli Directory Integrator (TDI) interface. The main window title is "IBM Tivoli Directory Integrator". The menu bar includes "Datei", "Objekt", "Speichern", "Fenster", "Tools", and "Hilfe". The toolbar contains various icons for file operations and help.

The left sidebar shows a tree view of the project structure under "C:\Dokumente und Einstellungen\...". The "AssemblyLines" folder is expanded, showing a list of connectors including "SOSPER2TIM", which is currently selected.

The main workspace is titled "AssemblyLine: SOSPER2TIM". It features a toolbar with options like "Hooks", "Datenfluss", "Konfigurieren...", "Aufruf/Rückgabe", "Prüfpunkt", "Sandbox", "Protokollierung", and "Beschreibung". Below this, there are dropdown menus for "Modus" (set to "Update") and "Status" (set to "Aktiviert"). A checkbox for "Änderungen berechnen" is checked, and a "Delta" button is visible. A "Übernehmen von:" button is also present.

The central area shows a list of hooks for the selected connector. The "On Add" hook is selected, and its configuration is displayed in the right-hand pane. The configuration includes a checkbox for "Aktiviert" (checked) and "Debugunterbrechung" (unchecked). Below this, there is a code editor with the following script:

```
ADDED_NEW=true;
task.logmsg("INFO TIMMod,afterADD : "
+ work.getString("operationtype")
+ work.getString("registrationNumber")
);
```

At the bottom of the right pane, it says "Verfügbare Objekte: work, conn" and a "Übernehmen von: [parent]" button.

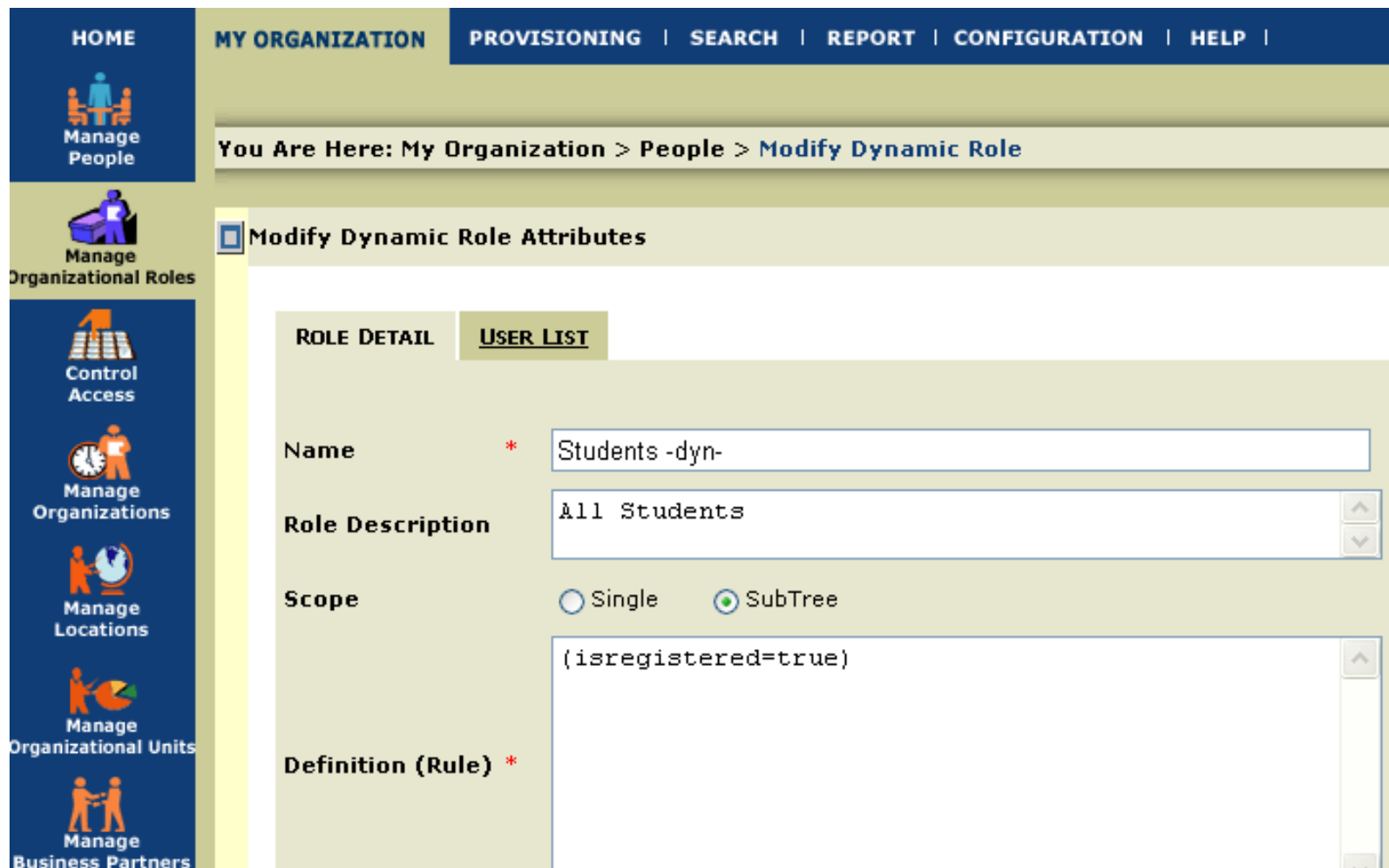
At the bottom left of the interface, there is a "Work-Eintrag" table with the following columns: "Name" and "Quelle".

Name	Quelle
id	fix_stage, proc...
registrationNum...	fix_stage, proc...
academicTitle	Principal
academicTitle_fl...	Principal
addressextension	Principal
addressextensi...	Principal
city	Principal
city_flag	Principal
dateofbirth	Principal
dateofbirth_flag	Principal
dateofmatric	Principal
dateofmatric_flag	Principal
flag	Principal

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



# ITIM: Definition dynamische Rolle „Student“



HOME | MY ORGANIZATION | PROVISIONING | SEARCH | REPORT | CONFIGURATION | HELP |

You Are Here: My Organization > People > Modify Dynamic Role

Modify Dynamic Role Attributes

ROLE DETAIL | USER LIST

Name \* Students -dyn-

Role Description All Students

Scope  Single  SubTree

Definition (Rule) \* (isregistered=true)

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

# ITIM: Provisionierungsregel definieren

The screenshot displays the ITIM Provisioning interface. The main navigation bar includes: HOME | MY ORGANIZATION | **PROVISIONING** | SEARCH | REPORT | CONFIGURATION | HELP |. The breadcrumb trail is: You Are Here: >> Provisioning AUM-Kundentabelle. A secondary breadcrumb trail shows: You Are Here: Universitaet Duisburg Essen > HRZ > Provisioning Policies > Provisioning AUM-Kundentabelle. A message states: Add a new Organizational Role or select an existing Organizational Role to remove. The current page title is: You Are Here: Provisioning AUM-Kundentabelle > Modify Entitlement > AUM-Kundentabelle. The form is titled 'View | Modify Entitlement Detail' and contains the following fields:

- Type: Automatic (dropdown)
- Target Type: Service (dropdown)
- Service Type: AUMProfile (dropdown)
- Service Name: AUM-Kundentabelle (dropdown)
- Provisioning Parameter List: [Get detail](#)
- Advanced Provisioning Parameter List: [Get detail](#)
- Process Definition: No workflow (text input) with Search and Clear buttons.

At the bottom of the form are Submit and Cancel buttons.

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

# ZIM Benutzerverwaltung: AUM (1)

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

[Telefonbuch abfragen](#)

# ZIM Benutzerverwaltung: AUM (2)

	ADRS1	SP2	UGE-HERMES	FS1	FS2	MAILBOX	Code-Schl.	Mail-Adresse	TSM	EXCHANGE	Freies Mail-Feld	RVNRW	GROUP	RADIUS	NIS	ZV	BB
<a href="#">hrz120</a>	<input checked="" type="checkbox"/>	yes	yes	<input type="checkbox"/>	yes	yes	<input type="checkbox"/>	yes	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	yes	yes	<input type="checkbox"/>	<input type="checkbox"/>
<a href="#">hrz120.hrz</a>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<a href="#">hy0231</a>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	yes	<input type="checkbox"/>	yes	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	yes	yes	<input type="checkbox"/>	<input type="checkbox"/>
<a href="#">icmcont</a>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<a href="#">lhrz300.hrz</a>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<a href="#">mcrfluet</a>	<input type="checkbox"/>	yes	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	yes	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<a href="#">mobile.ub</a>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<a href="#">mycore1.ub</a>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<a href="#">mycore2.ub</a>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	yes	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<a href="#">pcf1a.bibl</a>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<a href="#">wally.hrz</a>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<a href="#">Neuer Account</a>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## Accounts und Dienste des Benutzers

# ZIM Benutzerverwaltung: AUM (3)

SOFTQUOTA:	50000	
HARDQUOTA:	100000	
GECOS:	Frank Luetzenkirchen, HRZ	
<b>FS2</b>	jobonchange ▼	Y,YY
Home-Dirgruppe:	system	
Primaergruppe:	hrz	
Quota:	250000	
<b>SP2</b>	jobonchange ▼	Y,YY
Durchgefuehrte 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
<b>UGEHERMES</b>	jobonchange ▼	Y,YY
Durchgefuehrte 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:	<b>Domain Users; HRZ; Postbenutzer</b>	
Administratorgruppe:		Defaultwert
Anmeldescript:	benutzer.bat	

# ZIM Benutzerverwaltung: Selfcare-Portal



UNIVERSITÄT  
DUISBURG  
ESSEN

ZIM  
ZENTRUM FÜR INFORMATIONS- UND MEDIEDIENSTE

Sie sind eingeloggt als: hrz120  
[hrz120 ausloggen](#)

- ◆ Passwort ändern
- ◆ Mail-Funktionalitäten
- ◆ Webspaces für [www.uni-due.de](http://www.uni-due.de) verwalten
- ◆ Einen Rechner zum Backup- und Archivierungsservice anmelden
- ◆ Personendaten anzeigen
- ◆ Serviceprofile anzeigen

## E-Mail

- ◆ Den neuen Posteingangsserver aktivieren
- ◆ Abfragen, welche E-Mail-Adressen für Ihre Kennung geschaltet sind, und auf welchem Server Ihr Postfach liegt
- ◆ E-Mail-Weiterleitung (Forward) setzen oder löschen
- ◆ Abwesenheitsnachricht (vacation) für E-Mail setzen oder löschen
- ◆ SPAM-Schutzmaßnahmen einstellen
- ◆ Zentrale E-Mail-Listen der Universität abonnieren.
- ◆ E-Mails lesen oder schreiben. (Das ist eine Anwendung außerhalb dieses Portals und erscheint in einem eigenen Fenster.)
- ◆ Mehr zum Thema E-Mail erfahren. (Unsere Mailpolicy, Serveradressen, Anleitungen)

# Gästeverwaltung: Online-Anmeldung

<b>UNIVERSITÄT DUISBURG ESSEN</b>	<b>ZiM ZENTRUM FÜR INFORMATIONS- UND MEDIEDIENSTE</b>
<b>Hauptseite Neu registrieren</b>	<b>Online User Registrierung</b>
<b>Deutsch English</b>	Bitte geben Sie Ihre Daten ein. Fettgedruckte Felder sind verpflichtend.
	<b>Anrede :</b> Herr ▾
	Akademischer Titel : <input type="text"/>
	<b>Name :</b> <input type="text"/>
	<b>Vorname :</b> <input type="text"/>
	<b>Geburtsdatum :</b> TT ▾ MM ▾ JJJJ ▾
	<b>E-Mail-Adresse :</b> <input type="text"/>
	<b>Einrichtung der Hochschule : ?</b> ▾
	<b>Grund der Registrierung ? :</b> <input type="text"/>
	<b>Telefon :</b> <input type="text"/>
	<b>Weiterer Kommentar :</b> <input type="text"/>
<b>(Nur für Gastwissenschaftler) :</b>	<input type="checkbox"/> Ja, ich möchte meine persönliche Daten an die Pressestelle weitergeben. (Info zur Pressestelle)
	<input type="checkbox"/> Ja, ich möchte eine Multifunktionkarte beantragen. (Info zur Multifunktionkarte)
	Passfoto hochladen <input type="text"/> <input type="button" value="Durchsuchen..."/>

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

# HIS LSF: Lehre, Studium, Forschung

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

The screenshot displays the HIS LSF web application interface. At the top, the logo for 'UNIVERSITÄT DUISBURG ESSEN' and 'DIE CAMPUS UNIVERSITÄT' is visible. Below the logo, a navigation bar contains links for 'Startseite', 'Abmelden', and user information: 'Herr Frank Lützenkirchen | Sie sind angemeldet als: hrz120 | in der Rolle: Lehrender für Gemeinsame Projekte von UB und ZIM | Semester: WS 2007/08 | Hilfe | Sitemap'. A main navigation menu includes 'Meine Funktionen', 'Veranstaltungen', 'Einrichtungen', 'Studium', 'Personen', 'Forschung', 'Studentisches Leben', and 'Räume und Gebäude'. The 'Veranstaltungen' section is active, showing a search results page titled 'Suchen nach Veranstaltungen'. The search results show 2 hits for 'Dozent(-in) - Lützenkirchen, Frank Dipl.-Wirt.Inform. Semester - WS 2007/08'. The page includes a 'Suche nach Veranstaltungen' section with a 'markierte Termine merken' button. Two event entries are listed: 'E-Publishing' and 'Informatik', both for the semester 'WS 2007/08' and 'Zentrale Einrichtung Universitätsbibliothek'. The interface also features a 'Fullscreen: on off' toggle and a 'Fertig' status indicator at the bottom left.



# Personensuche: WebServices Integration

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

**Personensuche**

Nachname

**Kontakt** | Lehre | Dokumente | Publikationen

**Dipl.-Wirt.Inform. Frank Lützenkirchen**

Adresse

Anschrift: Universitätsstr. 9  
45141 Essen  
Universitätsbibliothek

Telefon: +49 203 379 2124 (D: 0203/379-\*, E: 0201/183-\*)

Fax: +49 203 379 3231

E-Mail: [luetzenkirchen \[at\] ub.uni-duisburg-essen.de](mailto:luetzenkirchen@ub.uni-duisburg-essen.de)

- Wiss. Mitarbeiterinnen/Mitarbeiter Universitätsbibliothek
- Mitarbeiter/in Gemeinsame Projekte von UB und ZIM

Telefon: E 21 24 (D: 0203/379-\*, E: 0201/183-\*)

E-Mail: [luetzenkirchen \[at\] ub.uni-duisburg-essen.de](mailto:luetzenkirchen@ub.uni-duisburg-essen.de)

# Studienportal: Liferay, Portlets, CAS

UNIVERSITÄT  
**D U I S B U R G**  
**E S S E N**

STUDIENPORTAL

Welcome, Michael Kerres! ▾

Startseite
Lehre ▾
Bibliothek
Informationen
Weblinks
Kommunikation
Hilfe

**Details**

**Online-Tutor Training**  
Diese Veranstaltung in LSF  
**Bitte aktivieren Sie die Belegfunktionalität in LSF, Studierende können sich sonst nicht für diesen Kurs anmelden!**

Dozent: Kerres, Michael

Termin: Mo, 14:00 - 17:00, wöch.  
Raum: LC 030

Verwendete Werkzeuge:  
keine

Verfügbare Werkzeuge:

**Veranstaltungssuche**

Suche nach Veranstaltungen

Veranstaltungsnummer:

Titel der Veranstaltung:

Veranstaltungs-Art:

Einrichtung:

Lehrender:

Raum:

von (Uhrzeit):

bis (Uhrzeit):

Wochentag:

Elearning:

Unterrichtssprache:

Semester:

**Liste Ihrer Veranstaltungen**

Michael Kerres hat im WS 2007/08 folgende Veranstaltungen belegt:

VeranstaltungsID	Titel	erster Termin
101445	edu media	
96110	Zusatzveranstaltung: Konzeption und Evaluation von Computer- und Lernspielen	
90906	Einführung in die Didaktik/Mediendidaktik	
95981	Praxisprojekt: Konzeption und Evaluation von Computer- und Lernspielen	
90897	Forschungskolloquium Bildung und Medien	
90911	Vorbereitung auf das Praktikum	
90894	Online-Tutor Training	

**Stundenplan**

**Stundenplan für Michael Kerres**

Montag	Online-Tutor Training 14:00-17:00 LC 030
Dienstag	Einführung in die Didaktik/Mediendidaktik 10:00-12:00 R.12 R03 A69
Mittwoch	keine Veranstaltungen
Donnerstag	keine Veranstaltungen
Freitag	Praxisprojekt: Konzeption und Evaluation von Computer- und Lernspielen 10:00-12:00 R.12 R03 A69 edu media 12:00-18:00 LC 026
keine Angaben	Vorbereitung auf das Praktikum --- R.12 R03 A69

Druckansicht

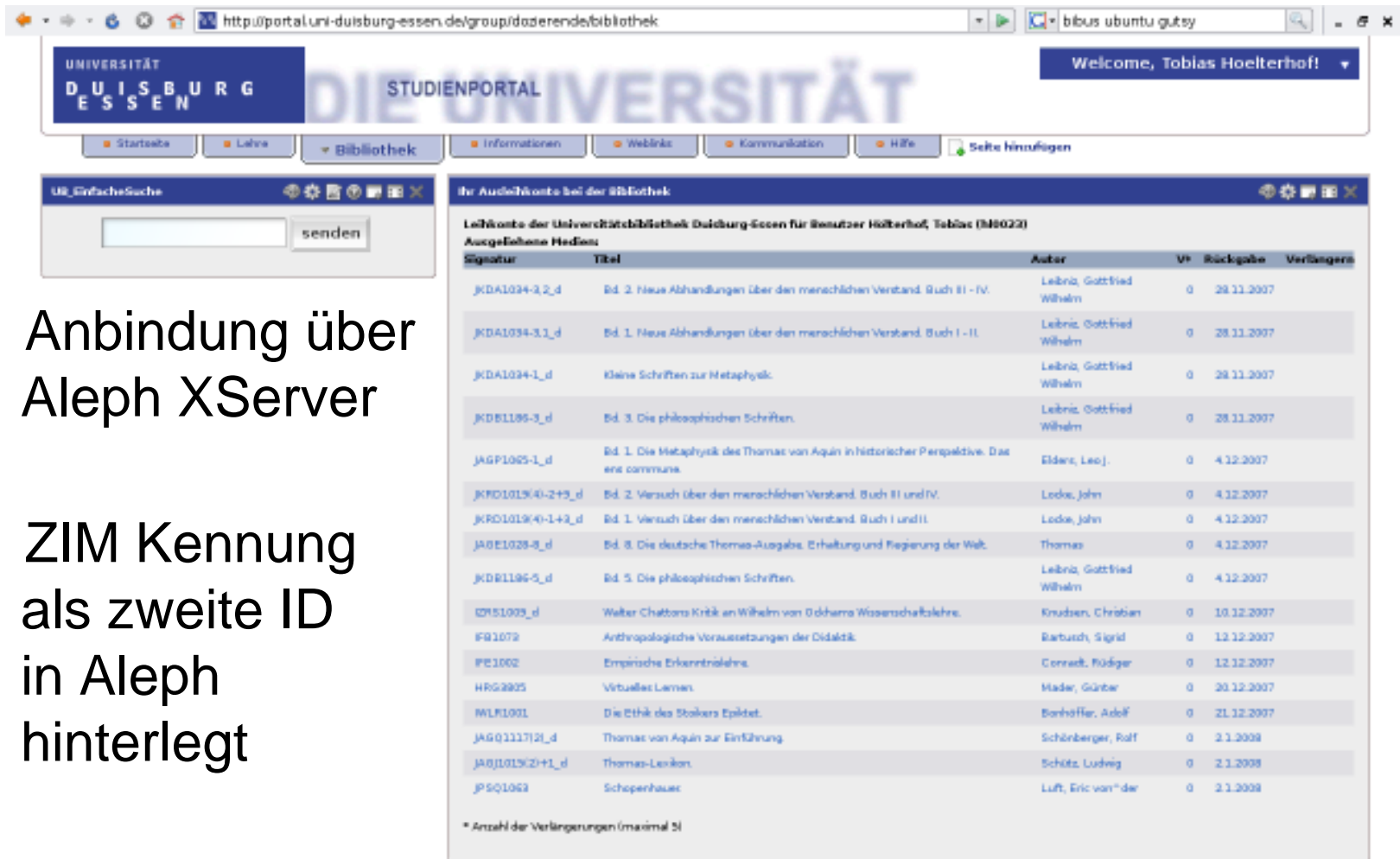
**Semesterapparat**

Verfügbare Semesterapparate für den Dozenten: Kerres, Michael

Titel	letzte Änderung
Didaktisches Design für mediengestützte Lernangebote	30.3.2007

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

# Studienportal: Ausleihkonto Bibliothek



The screenshot shows a web browser window with the URL <http://portal.uni-duisburg-essen.de/group/doi/erende/bibliothek>. The page header includes the University of Duisburg-Essen logo and the text "STUDIENPORTAL". A navigation menu contains links for "Startseite", "Lehre", "Bibliothek", "Informationen", "Weblinks", "Kommunikation", and "Hilfe". A search box labeled "UB\_einfacheSuche" is visible. The main content area is titled "Ihr Ausleihkonto bei der Bibliothek" and displays a table of borrowed books for user Tobias Hoelterhof (ID M8022).

Signatur	Titel	Autoren	VP	Rückgabe	Verlängerung
JKDA1034-3_2_d	Bd. 2. Neue Abhandlungen über den menschlichen Verstand. Buch III - IV.	Leibniz, Gottfried Wilhelm	0	28.11.2007	
JKDA1034-3_1_d	Bd. 1. Neue Abhandlungen über den menschlichen Verstand. Buch I - II.	Leibniz, Gottfried Wilhelm	0	28.11.2007	
JKDA1034-1_d	Kleine Schriften zur Metaphysik.	Leibniz, Gottfried Wilhelm	0	28.11.2007	
JKDB1185-3_d	Bd. 3. Die philosophischen Schriften.	Leibniz, Gottfried Wilhelm	0	28.11.2007	
JAGP1025-1_d	Bd. 1. Die Metaphysik des Thomas von Aquin in historischer Perspektive. Das erste commune.	Elders, Leo J.	0	4.12.2007	
JKFD1019/40-2+3_d	Bd. 2. Versuch über den menschlichen Verstand. Buch III und IV.	Lodde, John	0	4.12.2007	
JKFD1019/40-1+2_d	Bd. 1. Versuch über den menschlichen Verstand. Buch I und II.	Lodde, John	0	4.12.2007	
JA0E1028-8_d	Bd. 8. Die deutsche Thomas-Ausgabe. Erhaltung und Regierung der Welt.	Thomas	0	4.12.2007	
JKDB1186-5_d	Bd. 5. Die philosophischen Schriften.	Leibniz, Gottfried Wilhelm	0	4.12.2007	
IDP51005_d	Walter Chatters Kritik an Wilhelm von Ockhams Wissenschaftslehre.	Knudsen, Christian	0	10.12.2007	
FB1079	Anthropologische Voraussetzungen der Didaktik.	Barbusch, Sigrid	0	12.12.2007	
PE1002	Empirische Erkenntnislehre.	Conrath, Rüdiger	0	12.12.2007	
HRG2905	Virtuelles Lernen.	Mader, Günter	0	20.12.2007	
MLR1001	Die Ethik des Stoikers Epiktet.	Bonhöffer, Adolf	0	21.12.2007	
JAGQ1117/21_d	Thomas von Aquin zur Einführung	Schönberger, Ralf	0	2.1.2008	
JA0J1019/2+1_d	Thomas-Lexikon.	Schütz, Ludwig	0	2.1.2008	
JPSQ1063	Schopenhauer.	Luft, Eric van der	0	2.1.2008	

\* Anzahl der Verlängerungen (maximal 5)

- Anbindung über Aleph über 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

UNIVERSITÄT  
DUISBURG  
ESSEN

## Central Authentication Service der UDE (CAS)

**Bitte geben Sie Ihre Uni-Kennung und Ihr Passwort ein.**

Uni-Kennung:

Passwort:

Ich möchte gewarnt werden, bevor ich mich in einen anderen Bereich einlogge.

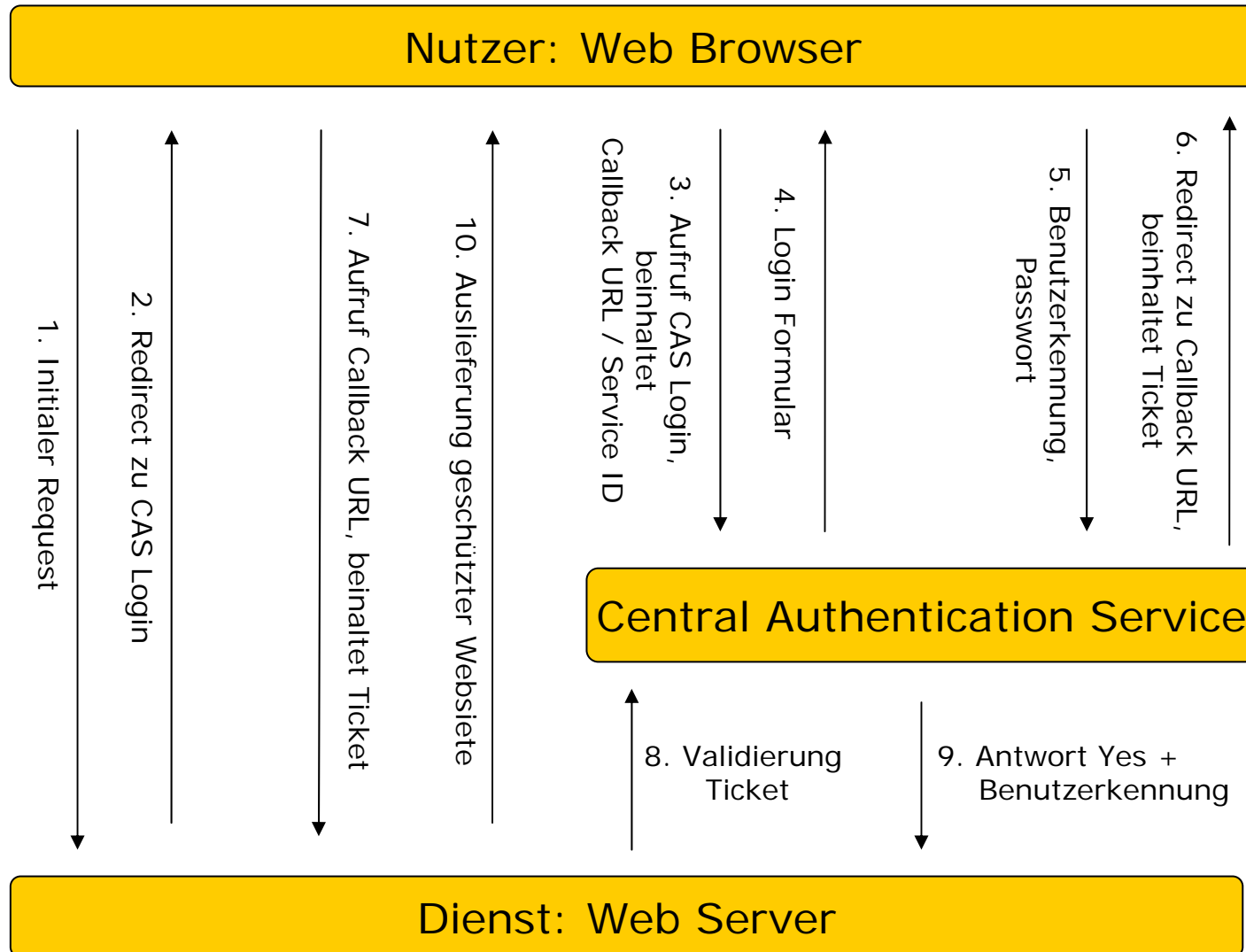
Aus Sicherheitsgründen sollten Sie bei Verlassen der passwortgeschützten Bereiche sich explizit ausloggen und Ihren Webbrowser schliessen!

Languages:  
[English](#) | [Spanish](#) | [French](#) | [Russian](#) | [Nederlands](#) | [Svenskt](#) | [Italiano](#) | [Urdu](#) | [Chinese \(Simplified\)](#) | [Deutsch](#) | [Japanese](#)

Fertig demoportal.uni-duisburg-essen.de



# CAS Architektur

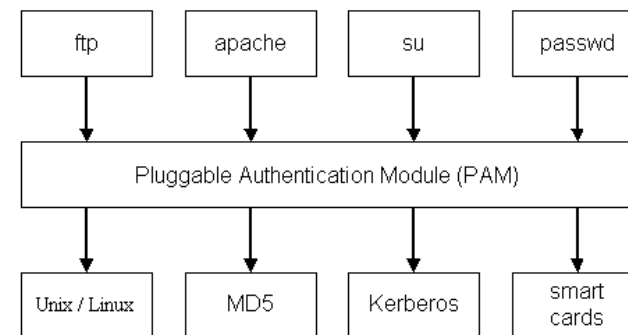


## CAS: Authentifizierung

- *Authentication Handler*: implementiert Authentifizierung
- *Principal*: Zu authentifizierender 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";
};
```

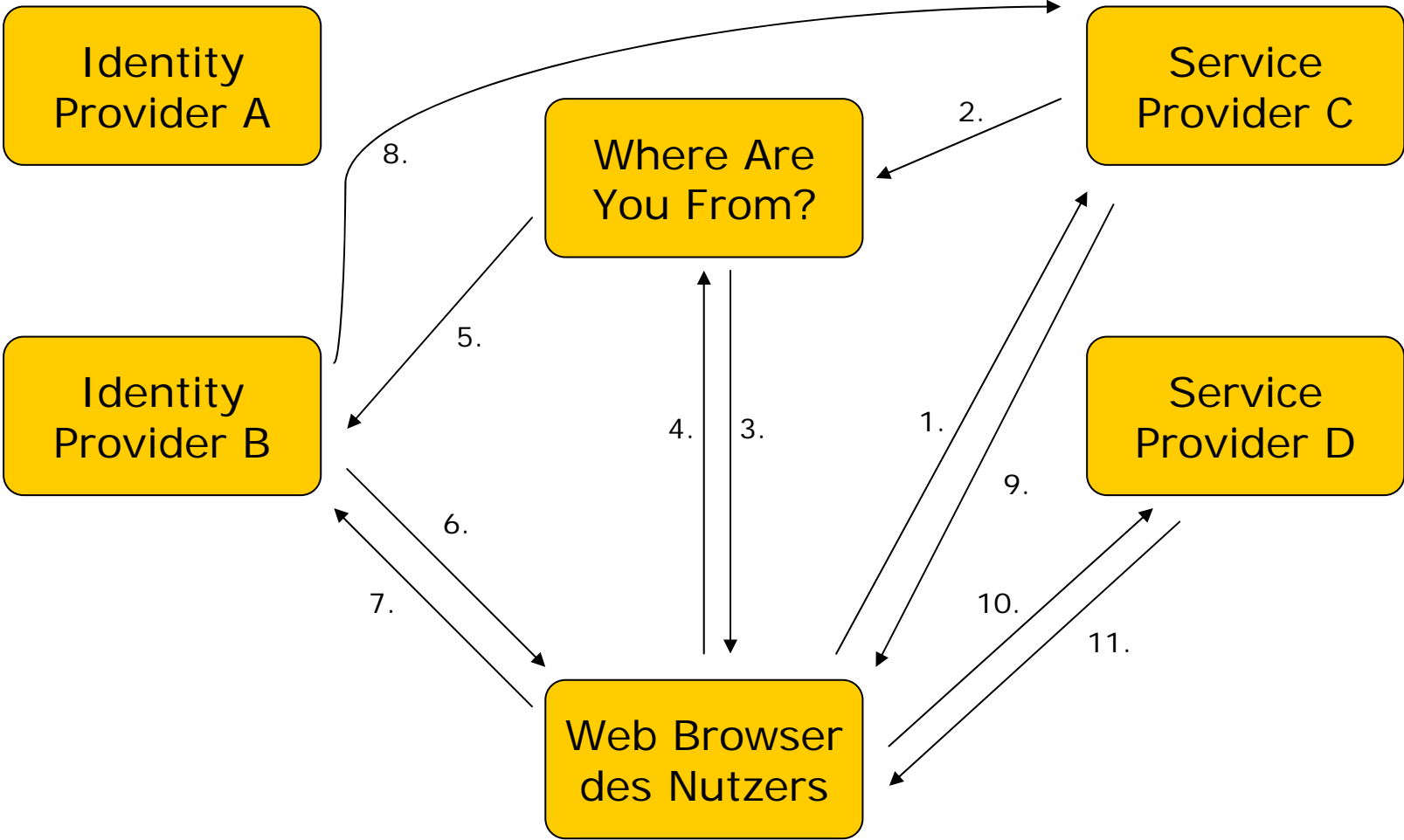
Quelle: Beispiel-Konfiguration aus der CAS Dokumentation

# 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



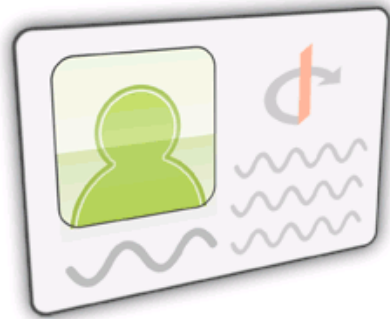
# Shibboleth Architektur



## 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

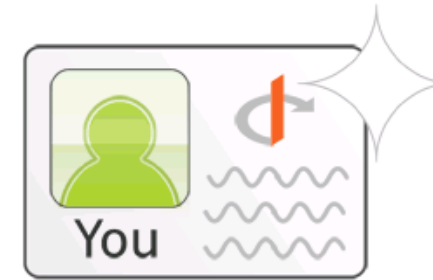
# OpenID



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 Authentifizierungsmethoden 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!**

