Identity management in a university environment

respecting central and faculty needs and providing the identity to shibboleth

Gerhard Schneider

Rechenzentrum der Universität Freiburg

gerhard.schneider@rz.uni-freiburg.de

Historic background

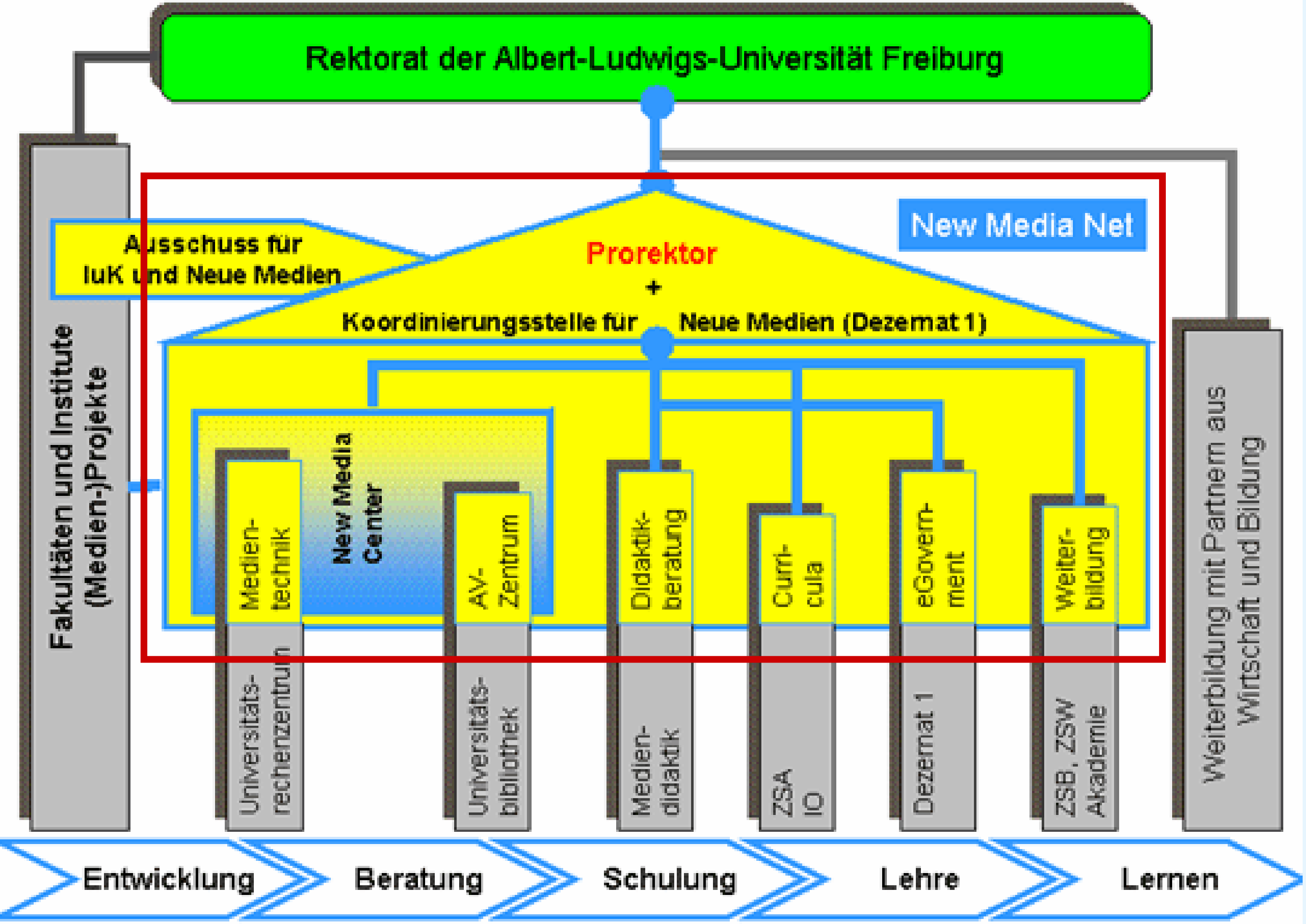
- **1995**: joint teleseminars between Freiburg and Karlsruhe
  - Ottmann – Stucky / organisation by GS (RZ-KA)
  - Using the existing fast Belwue Network
- media-hype → expensive media based lectures
  - The quest for alternatives
- Ottmann: Authoring on the Fly
  - Product „lecturnity“ available
- 1999: first BMBFprojects to adress eLearning
  - Mainly incompatible technical solutions
  - Not yet strategic for the universities
- 2000: DFG requests the CIO for universities
- This lead to a number of consequences …

New media deployment

- lesson: „New media“ is not just technology but also deployment
  - Deployment should affect the whole university
  - Including „early adopters“ and „the last line of defense“
- Successful deployment means:
  - Do not start every day with a new technology
  - But convert a new user every day – using existing technology
  - Financial incentives
  - „early adopters“ must approach users
    - And the users must not retreat ☺
- MEP „media development plant“ in 2001
  - Via university senate, all faculties involved

- http://www.newmedia.uni-freiburg.de/Profil/mep.html

New Media Net as core adress


Rektorat der Albert-Ludwigs-Universität Freiburg
New Media Net
Ausschuss für IuK und Neue Medien
Prorektor
+
Koordinierungsstelle für Neue Medien (Dezemat 1)
Fakultäten und Institute (Medien-)Projekte
New Media Center
Medien-technik
AV-Zentrum
Didaktik-beratung
Curri-cula
eGovern-ment
Weiter-bildung
Universitäts-rechenzentrum
Universitäts-bibliothek
Medien-didaktik
ZSA IO
Dezernat 1
ZSB, ZSW Akademie
Weiterbildung mit Partnern aus Wirtschaft und Bildung
Entwicklung
Beratung
Schulung
Lehre
Lernen

Financial boosters

- Catalytic effect: BMBF-initiative 2002
- *Faculty for applied sciences* presented (als consortial leader) the F-MoLL project
    - Involving all interested institutes and chairs
    - Oriental studies, music, political sciences, biology, etc
    - CC guaranteed the basic functionality
        - Notebook loan, organisation, deployment, server, etc
    - Computer science dept. Coordinated the development
    - 1,6 M€ - across all faculties
        - The only „revolutionary“ application

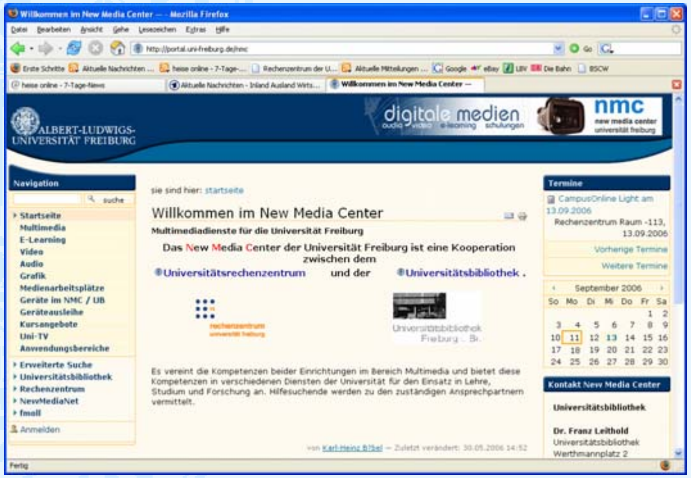
Money makes the world go round (and universities)

- Noticable effects:
  - Contract with the ministry forcing the university to continue with the implementation of New Media at all levels
  - Funding (2004-2006) of
    - Coordinating task force
    - New Media Centre
    - Media-based teaching in computer sciences

    with the (enforced) promise to continue after the end of the funding period
  - Total volume: 2,5 M€, i.e. 1M€ vom MWK
- University „media prize“
  - Rather than funding good promises
  - Better fund existing promising projects
    - 35 T€ p.a.

Structural consequences

- New Media Centre
  - Virtual centre as a truly existing „real“ cooperation of computer centre and library
  - Library director and CC director meet every 4 weeks for regular coordination
    - Both like good food…
  - „one face to the customer“
    - CC staff refers to library staff if necessary (and vice versa) customer does not have to search
    - Separate homepage referring to the services of the two institutions
- Competence is kept in its environment, yet the user has the notion of a single functional unit



sie sind hier: startseite

Willkommen im New Media Center

Multimediadienste für die Universität Freiburg

Das New Media Center der Universität Freiburg ist eine Kooperation zwischen dem Universitätsrechenzentrum und der Universitätsbibliothek .

Es vereint die Kompetenzen beider Einrichtungen im Bereich Multimedia und bietet diese Kompetenzen in verschiedenen Diensten der Universität für den Einsatz in Lehre, Studium und Forschung an. Hilfesuchende werden zu den zuständigen Ansprechpartnern vermittelt.

von Karl-Heinz Bißel — Zuletzt verändert: 30.05.2006 14:52

Termine

CampusOnline Light am 13.09.2006
Rechenzentrum Raum -113, 13.09.2006

Vorherige Termine

Weitere Termine

‹ September 2006 ›

So	Mo	Di	Mi	Do	Fr	Sa
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

Kontakt New Media Center

Universitätsbibliothek

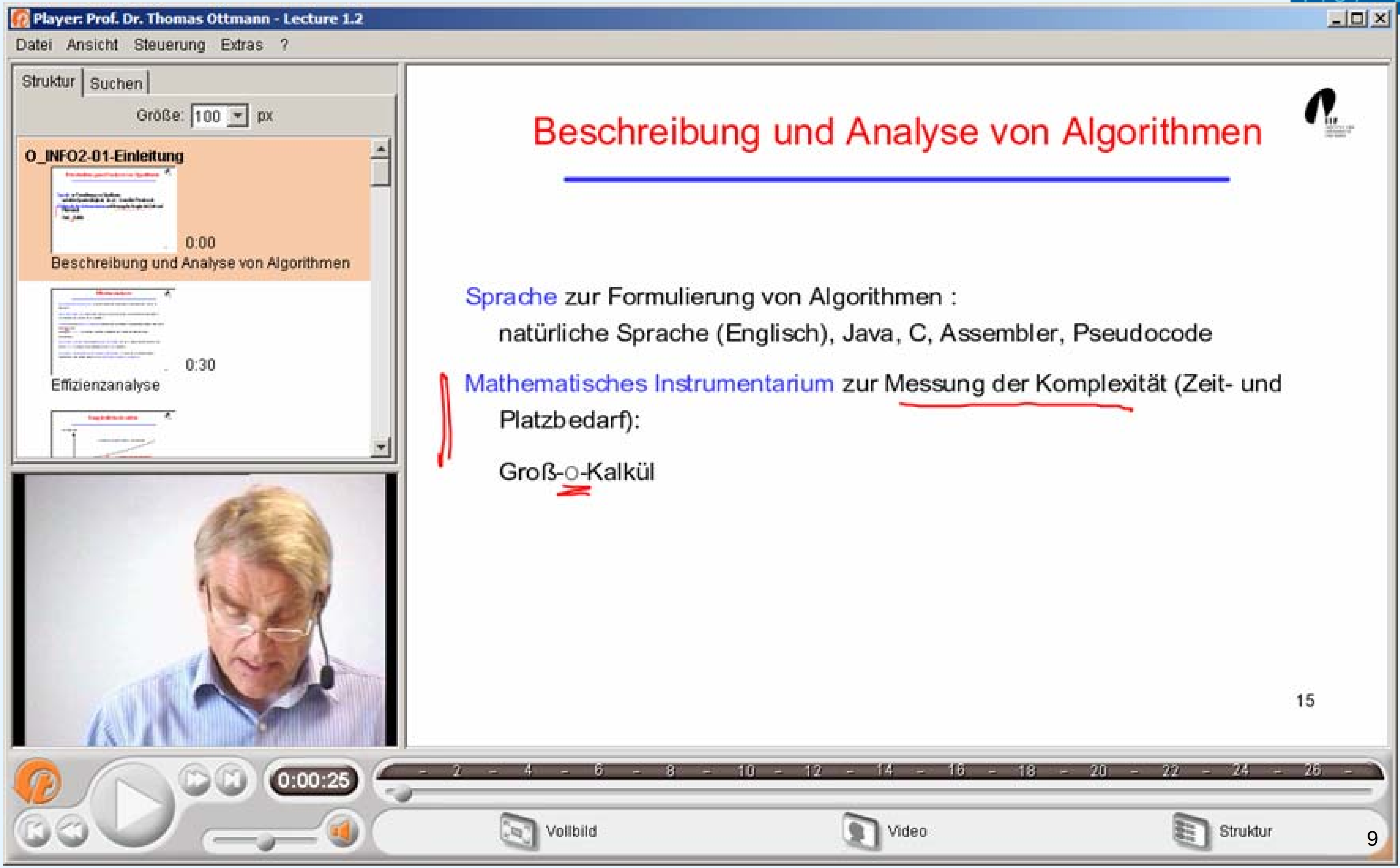
Dr. Franz Leithold
Universitätsbibliothek
Werthmannplatz 2

New Media coordination group

- Does the „dirty“ work for the sake of the university
  - No „I know better“ and no delivery of the orders of the rectroate
  - A bit like the New Media Centre, but going out to the user
    - Advertising technology, helping the user
  - With a clear mission of improving and pushing the use of New Media in teaching
    - To help students
    - Not just with a technology bias, but with proximity to technology
      - Office space in the CC
  - Optimization of workflows together with CC and administration
  - Big advantage(?): only one boss at all levels
- Who pays?
  - Up to now a strategic service of the university financed with third party money
  - Continuation thanks to student fees

Computer science

idea / environment=solution / commercial product



Beschreibung und Analyse von Algorithmen

Sprache zur Formulierung von Algorithmen :
natürliche Sprache (Englisch), Java, C, Assembler, Pseudocode

Mathematisches Instrumentarium zur Messung der Komplexität (Zeit- und Platzbedarf):

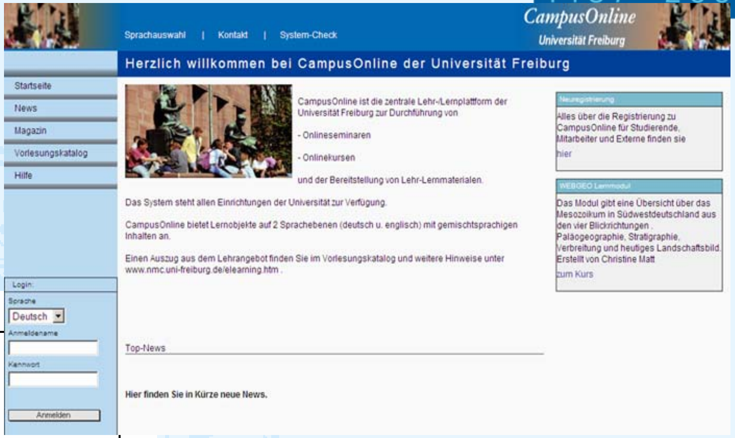
Groß-O-Kalkül

15

Common elearning platform

Campusonline

- currently about 170 lectures



Sprachauswahl | Kontakt | System-Check

CampusOnline
Universität Freiburg

Herzlich willkommen bei CampusOnline der Universität Freiburg

CampusOnline ist die zentrale Lehr-/Lernplattform der Universität Freiburg zur Durchführung von

- Onlineseminaren

- Onlinekursen

und der Bereitstellung von Lehr-Lernmaterialen.

Das System steht allen Einrichtungen der Universität zur Verfügung.

CampusOnline bietet Lernobjekte auf 2 Sprachebenen (deutsch u. englisch) mit gemischtsprachigen Inhalten an.

Einen Auszug aus dem Lehrangebot finden Sie im Vorlesungskatalog und weitere Hinweise unter www.nmc.uni-freiburg.de/elearning.htm .

Neuregistrierung

Alles über die Registrierung zu CampusOnline für Studierende, Mitarbeiter und Externe finden sie

hier

WEBGEO Lernmodul

Das Modul gibt eine Übersicht über das Mesozoikum in Südwestdeutschland aus den vier Blickrichtungen . Paläogeographie, Stratigraphie, Verbreitung und heutiges Landschaftsbild. Erstellt von Christine Matt

zum Kurs

Login:

Sprache: Deutsch

Anmeldename:

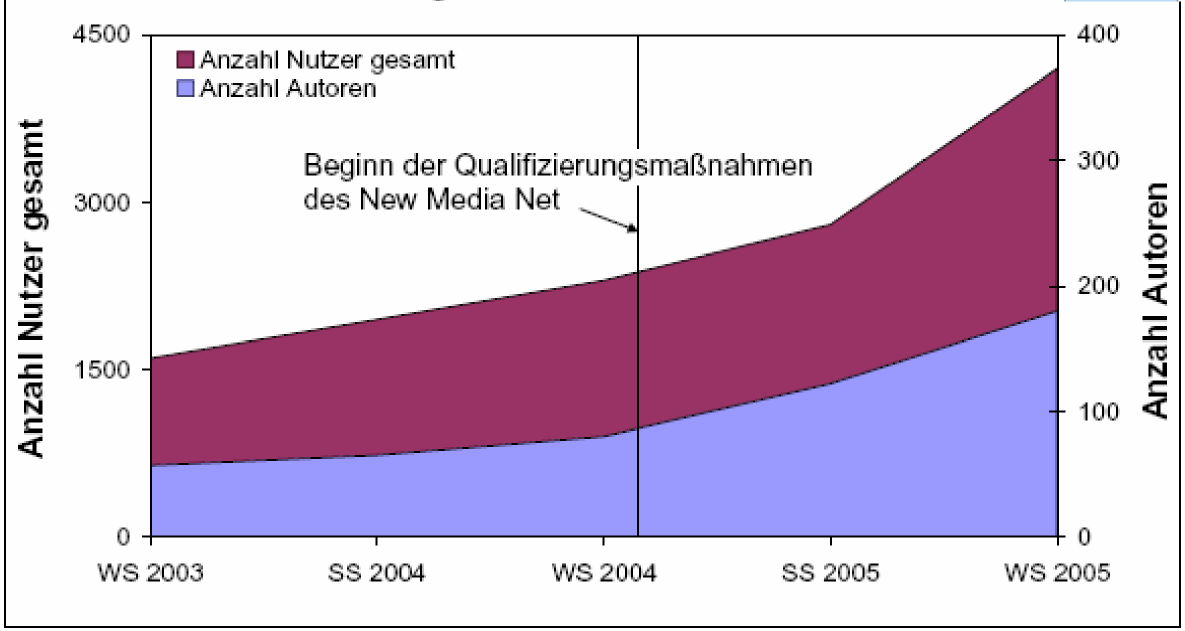
Kennwort:

Anmelden

Top-News

Hier finden Sie in Kürze neue News.

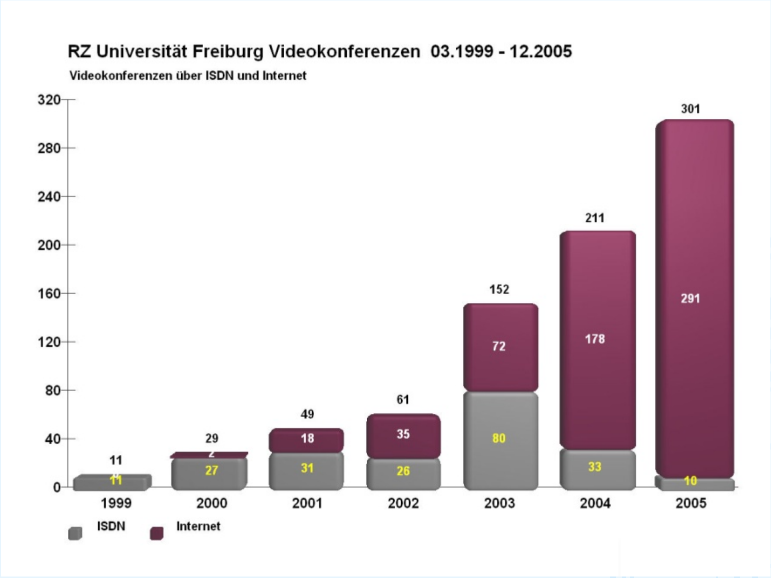
Entwicklung der Nutzer- und Autorenzahlen

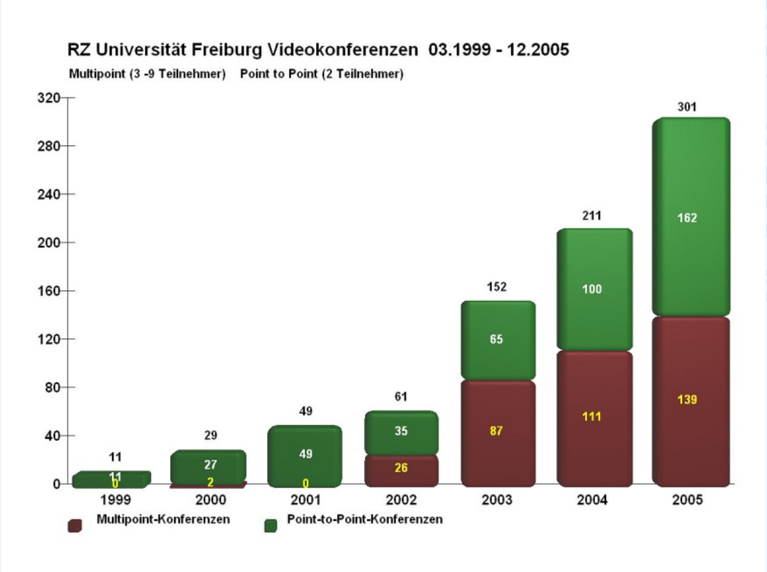


- Common = „keep talking to them“
- No support for those who want to run their own system
- Rectorate must be firm on this!!

550 Jahre
Albert-Ludwigs-Universität Freiburg
1457 – 2007

Video conferences





Videokonferenzraum

- Full support for complex conferences
  - Online exams with South Africa
- Permanent reservation for CERN conferences
  - Saves a few trips
- Joint seminars with the US (Harvard law)

Consequences at the „top level“

- All this will not run on its own
  - Even if all players are highly motivated
  - They still need cover from the rectorate
    - Especially when conquering new action fields
    - Example: is student administration allowed to decide a busines workflow on its own??
    - Necessary support rules must be put in action (senate)
  - Vice-president for „knowledge transfer and communication technology! (CIO)
    - Chief missionary – ultimate believer
    - **Requires a lot of spare time**
      - Work like a shepherd trying to direct the sheep into the right direction
      - Without finishing off orthogonal ideas of qualified people
        - Idea might be useful later
    - Without a permanent effort the system comes to a standstill

Media and more…

- You realize quickly, that a few initiatives alone are not enough
  - They sooner or later will run out of steam – especially when the funds dry out
- You can achieve a lokt of unexpected side effects
- And „New Media“ is a much wider issue than expected
  - If you look from above
  - The various departments/institutions can‘t see this

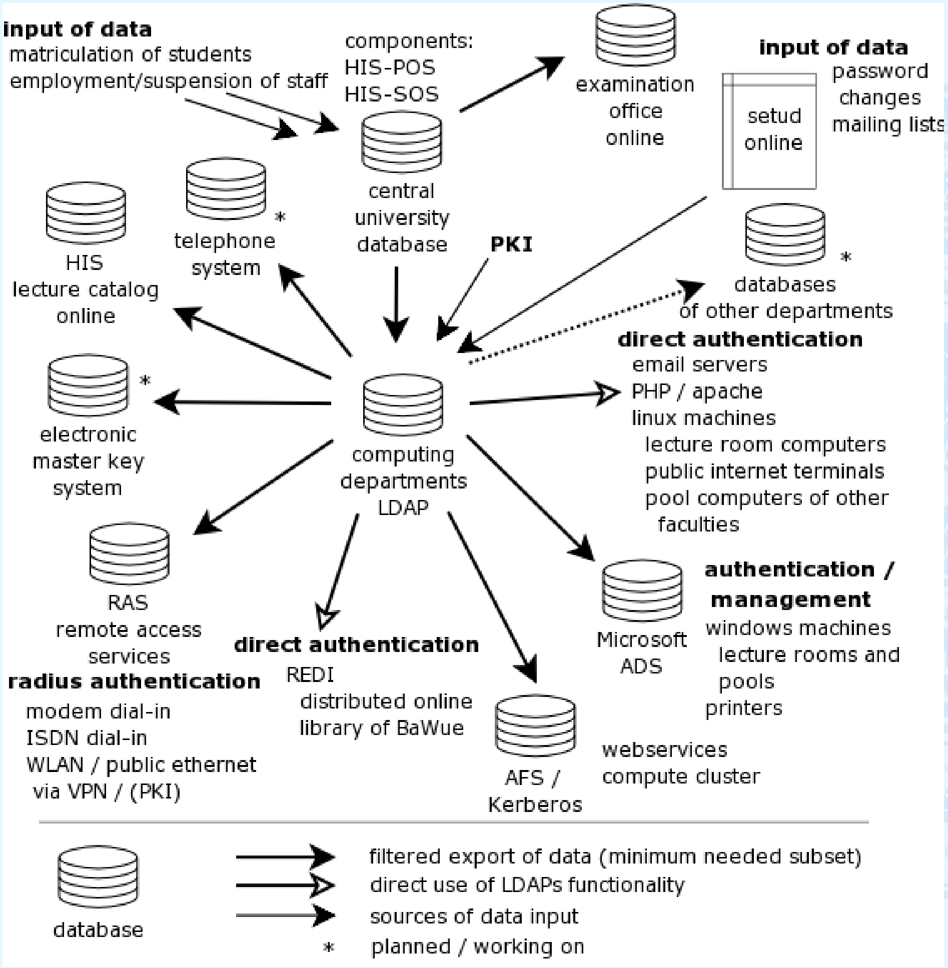
Consequences (1): Identity-Management

- Classical approach:
  complicated selection process of the „best“ system, modify your business processes to fit them to the system, do a lot of testing, migrate, update, etc…
  chaos and additional staff requirements.
- Our approach:
  - Who is in charge of the data – and who should be? Sort out the **organisational issues!**
  - How do the data items interact? And where are they needed? By whom? Sort out the **organisational dependencies**
  - What are the capabilities of your data management systems? And how can you improve the flow of data to achieve success?
  - And then develop/choose the necessary connecting system solutions using „good guesses“
    - After all a professional guess should not be too wrong

Consequences (1)
IdM - sketch of our solution

- HIS-SOS
  - „knows“, whether a student is matriculated or not
- LDAP
  - Imports the basic data
  - Checks regurlarly whether the person is still a member of the university
  - Does authentication (userid/passwd)
  - Allows for self-administration of user data
    - Preferred mail adress, student card id, etc
- Keycard door lock checks
  - Is the card still valid (→ LDAP)
  - Does the user have permission to open the door
    - Managment of these rights remains in the lock management software – administer user profiles in the system, decentral, use local competence!
- Wireless LAN (campus wide) „checks“
  - Is account still valid? (→ LDAP)

Consequences (1) architecture



- Only export data which is really necessary (privacy)
- Most ID-based decisions do not require a full view of all data
- It does work!
- We now see the real bottle necks!
  - A professional solution most likely will show the same bottlenecks – because they are of organisational origin

Consequences (2) mailing lists

- How do you find out the mail adresses of the members of the university??
  - By order
    - Each member gets a mail address - and nobody reads the mail or complains
    - „force“ never works in a (German) university environment)
  - Use honey pots….
    - Login to HIS-LSF requires central account and works only if mail adress is known
      - Special request to HIS (costs money)
      - As a reward send timetables and changes to this mail adress
    - Weekly newsletter with important infos to all known mail adresses
    - Self administration of list subscribtions
- **Be careful – do not spam**
  - We all have enough emails every day

Consequences (3) wireless LAN

- Perfect example for a central solution giving happiness to decentral institutions
- To succeed with a central and uniform approach, do not leave the playground to the faculties
  - „forbidden“ is not a promising concept
  - You have to be faster, have better ideas and offer additional features
    - Antennas placed on a highrise building provide connectivity for the home office
    - Provide good coverage in libraries
    - Wireless connectivity for (outside) places which students like
    - Provide roaming with other science institutions in the city, the state, the nation
    - Peering with a city wireless provider
    - Thus the „do it yourself people“ give up
- Access only possible with an account registered in the IdM

Lessons learnt (1)

- **If**
  - There is a central user base
    - The administration usually has one
  - The user basis is up to date
    - This is the administration‘s task
  - There are reliable central services (like mail)
    - The computer center should be able to deliver
  - And the users in general use them
    - Because alternatives are somewhat difficult or less functional

- **Then** you can use this for new services – making it more attractive
  - Central mailing lists to improve the flow of information
    - This requires „tender loving care“ – not spam
    - User self administration is necessary and must be respected
  - More services via self administration
    - Order semester tram ticket
    - Allow to collect money from the user bank account (authenticated) to pay for services

Lessons learnt (2)

- Process interaction is much deeper than originally expected
  - Would have been overlooked in a classical software approach
- Processes can be modernized so that they stay (or become) lean
  - But management has to work at the shop floor (from time to time)

- Stay mentally fresh and venture for new tasks:
  - Master Online:
    4 out of 26 applications were from Freiburg
    3 out of 5 successful applications are from Freiburg
    perhaps because they were not isolated plans, but part of a master plan of the university
- Make the right offers which suit faculties and institutes
  - Stop them from worrying about the present and the past
  - make them fly to the honey pot / lure them into the pot….
  - New Media leads to a working IdM

New targets…
in a digital information age

User

- Access to licenced contents should be possible **independent** of location and access method
- All licenced content should be accessible after only one single registration (**Single Sign-On**).
- If possible do not pass on personal data

Institutions (for example universities)

- The institution must be able to choose any which authentication system and whatever identity management

provider

- The licenced contents of a provider must be protected against illegal access

What is Shibboleth?

- Shibboleth is an **Internet2/MACE**-project (MACE = Middleware Architecture Committee for Education)
- Shibboleth consists of
  - **Architecture definition** (protokols and profiles),
  - **Deployment/usage guidelines**
  - **Open Source-Implementation**

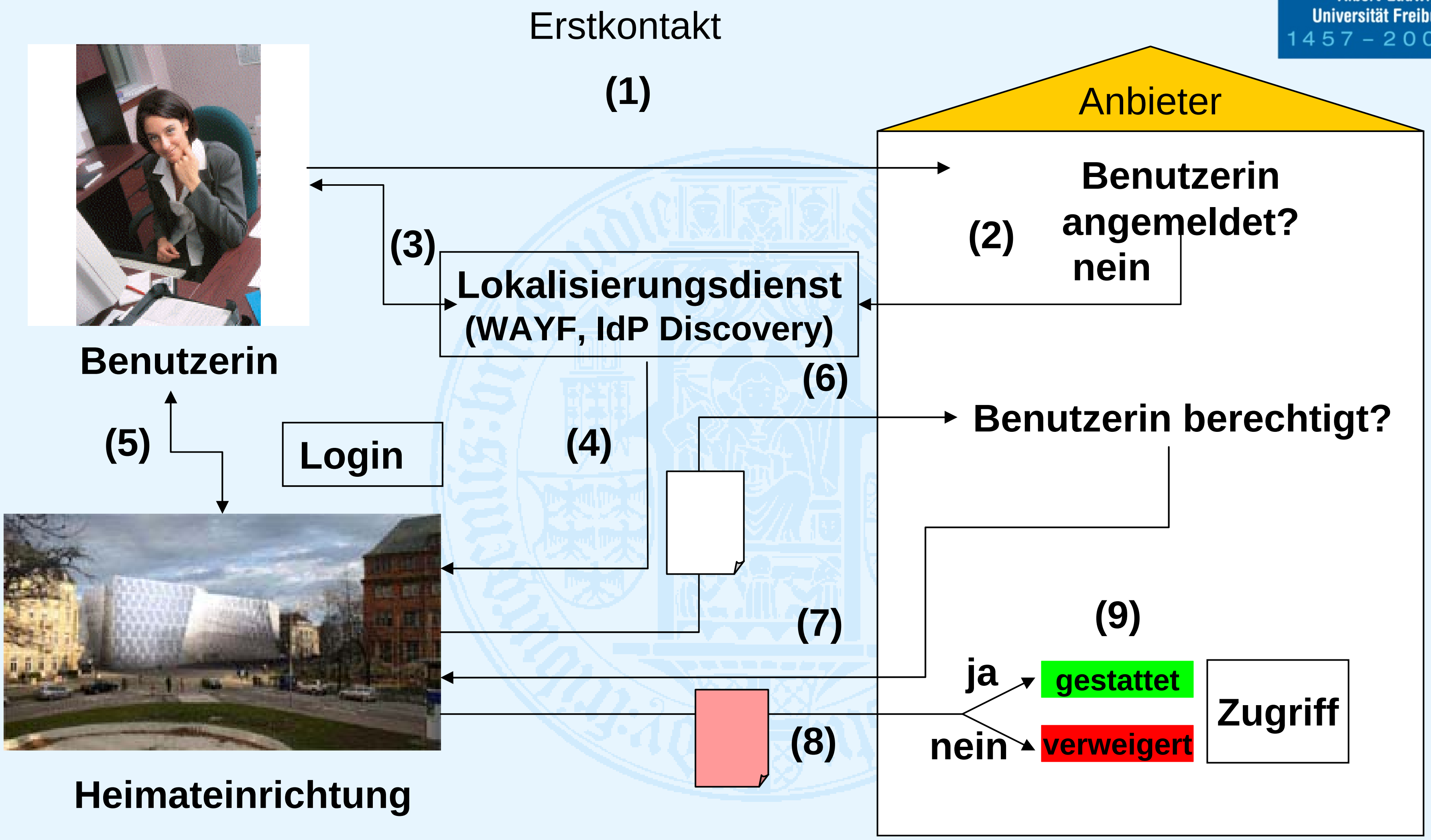
  to achieve access to web resources across insitutiones

  example: try to read your e-journals at anonther institution…
- Shibboleth uses a federated approach: Each institution manages and authenticates its own members and the information provider controls access to his resources

Five good reasons for Shibboleth

- **Single Sign-On across institutions**
- Authorisation and access control via **attributes** mit der Möglichkeit zur **anonymen/pseudonymen Nutzung** von Angeboten
- Based on **approved software und standards** (SAML: XML, SOAP, TLS, XMLsig, XMLenc)
- **Integration** with existing IdM and (web based) applications is **relatively easy**
- **High acceptance world wide,** even with (commercial) providers (Elsevier, JSTOR, EBSCO, Ovid, GBI, CSA, ...)

How does it work?



Erstkontakt

(1)

Anbieter

Benutzerin

(2) Benutzerin angemeldet? nein

(3)

Lokalisierungsdienst (WAYF, IdP Discovery)

(4)

Login

(5)

(6)

Benutzerin berechtigt?

(7)

(8)

(9)

ja gestattet

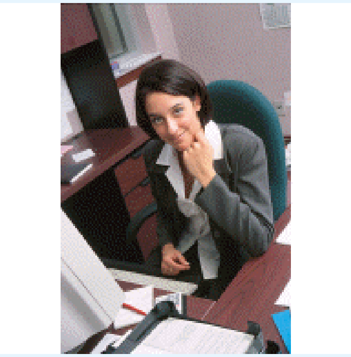
nein verweigert

Zugriff

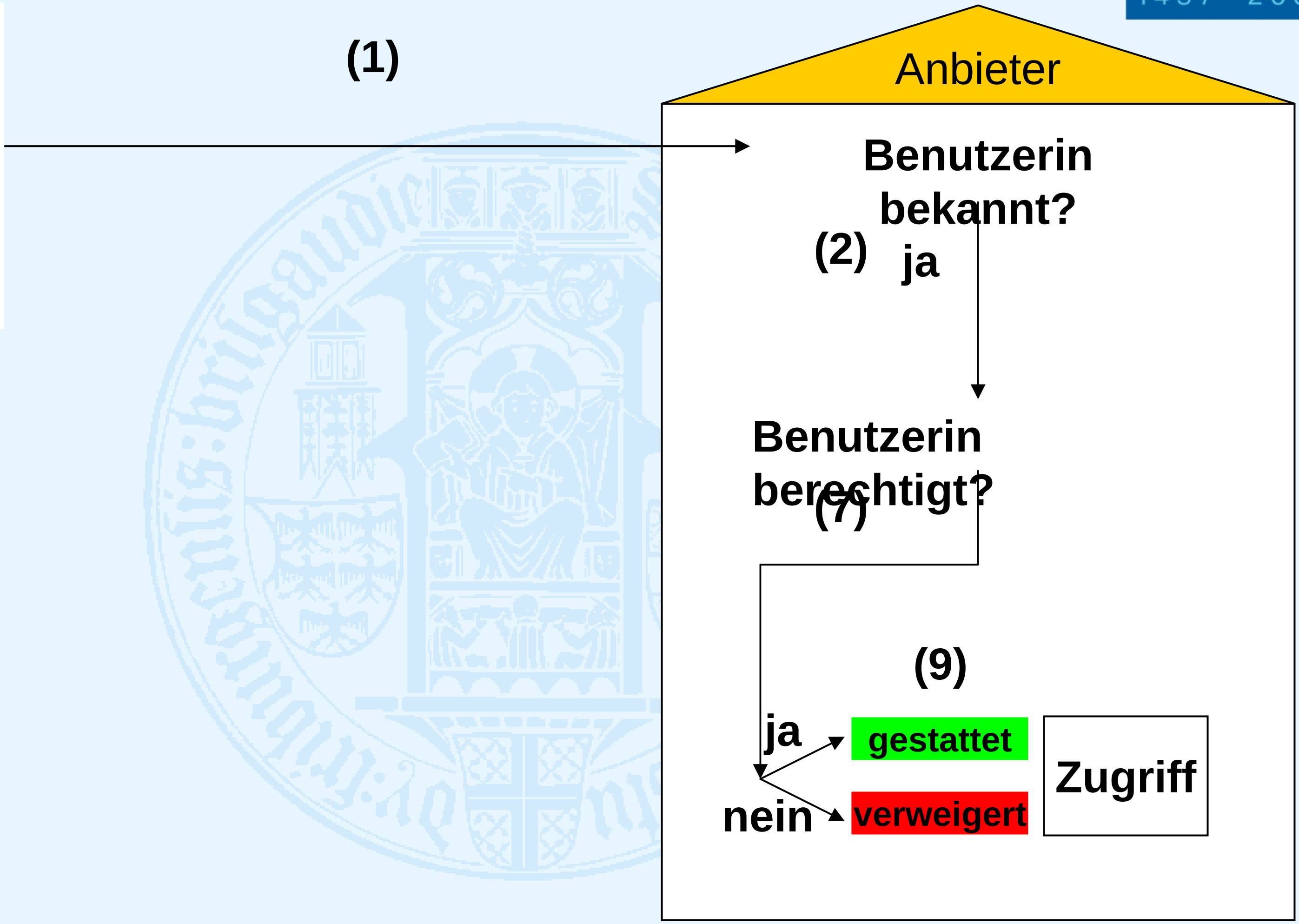
Heimateinrichtung

How does it work?

Folgekontakt (gleicher Anbieter)



Benutzerin



(1)

Anbieter

Benutzerin bekannt?

(2) ja

Benutzerin berechtigt?

(7)

(9)

ja

gestattet

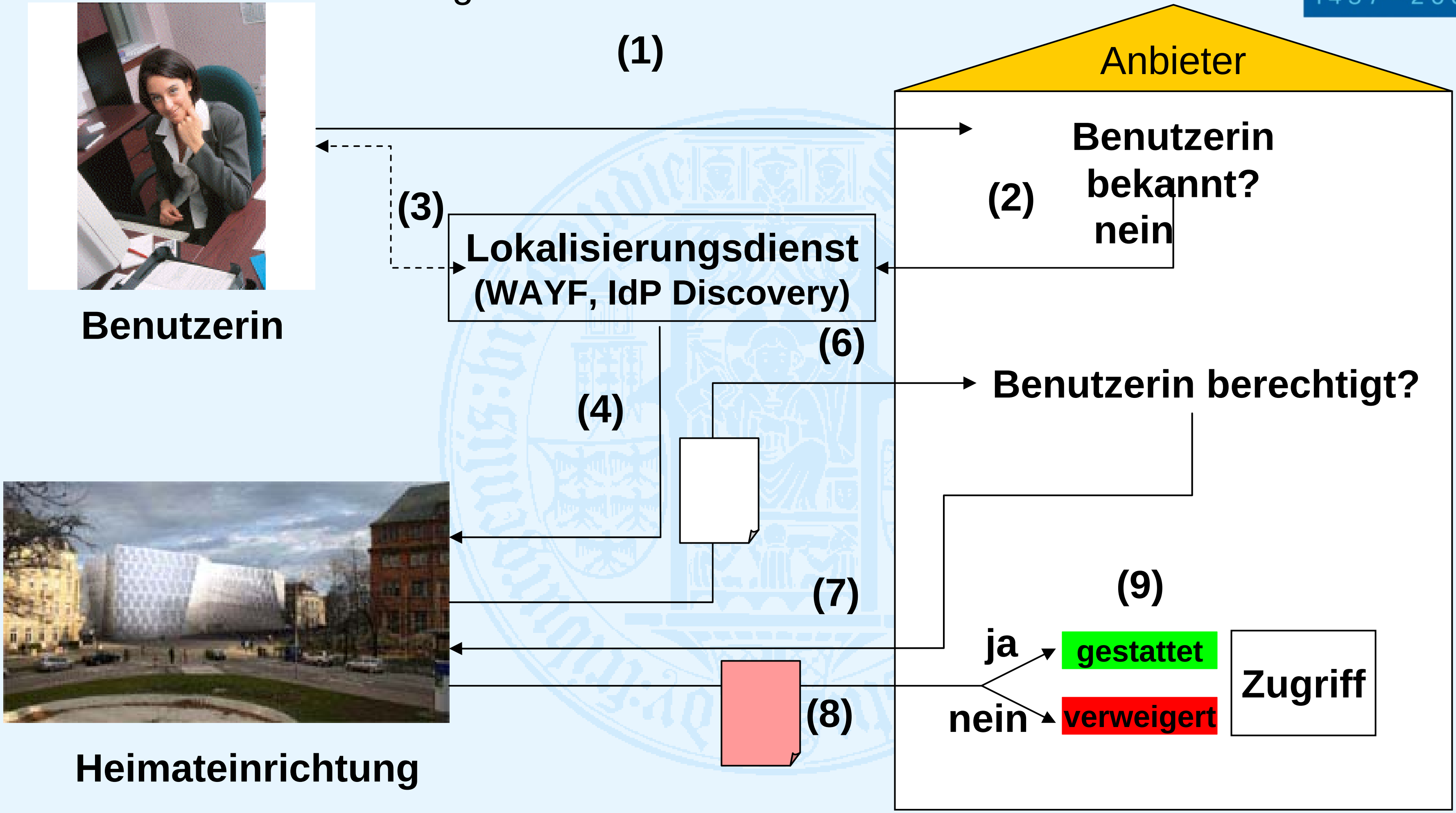
nein

verweigert

Zugriff

How does it work?

Folgekontakt anderer Anbieter



(1)

Anbieter

Benutzerin bekannt?

(2)

nein

Benutzerin

(3)

Lokalisierungsdienst
(WAYF, IdP Discovery)

(4)

(6)

Benutzerin berechtigt?

(7)

(9)

ja

gestattet

nein

verweigert

Zugriff

(8)

Heimateinrichtung

The federation DFN-AAI

- **Why is there a problem?**
  - Provider must trust the **user**
    - And the user is not known to them
  - After all there is **money** involved
  - **„Trust“** in business terms: **„contract“.**
  - Therefore we need **real** (bullet proof?)conventions
  - We need rules for the **technical operation**
- **DFN-AAI** is a service of the DFN-Vereins, both for scientific institutions as well as for (commercial) providers of (information) resources.
- **DFN-AAI** ensures the necessary **trust relationship** and the **organisatorial and technical framework** for an exchange of user information between many users and many providers

Usage scenarios

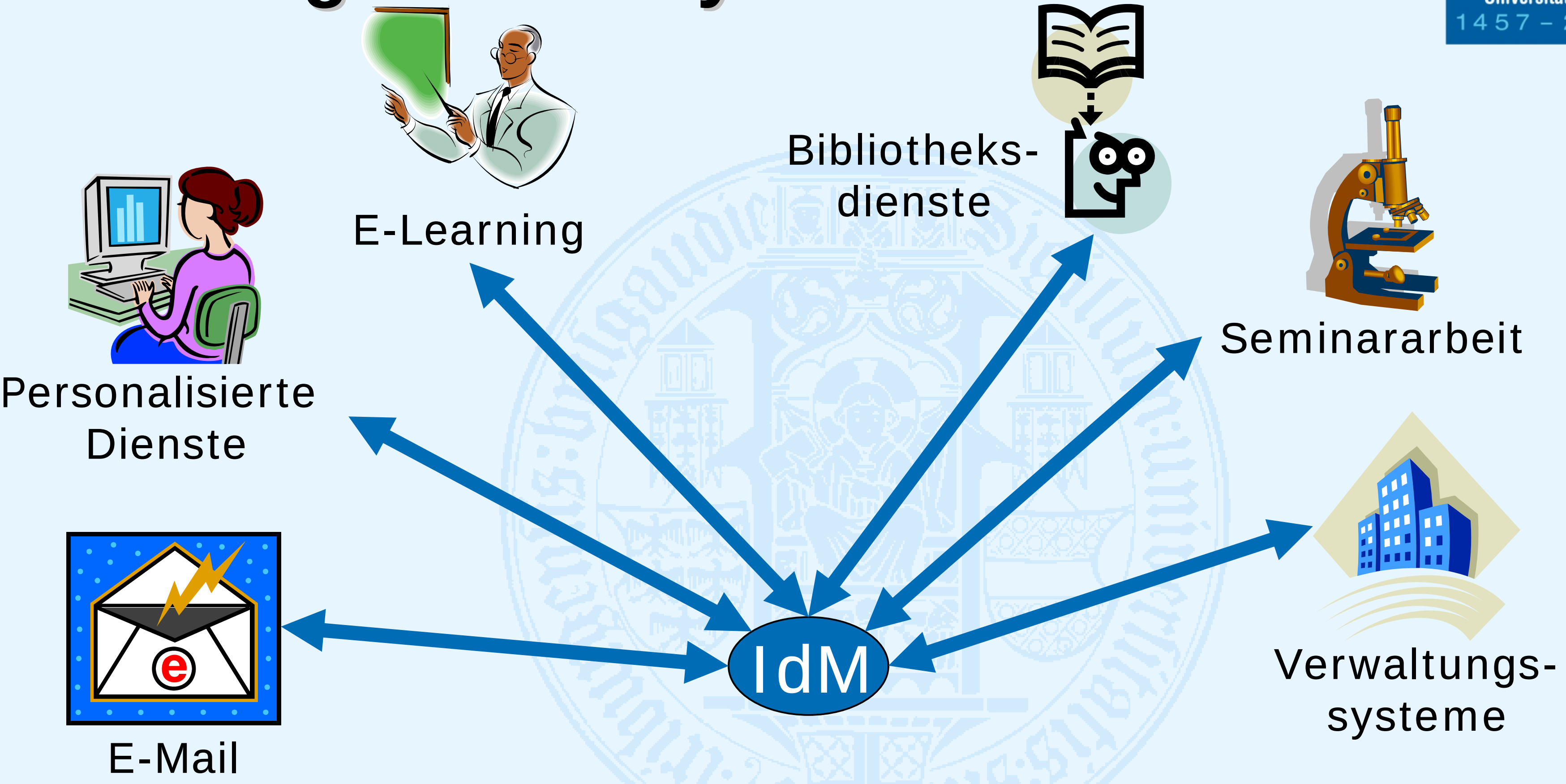
- Access to protected (esp. Commercial) electronic information
  - E-journals, data bases, e-books, ...
  - Portals (e.g. vascoda, ReDI)
  - DFG sponsored national licences
  - Repositories
- e-Learning
- e-Science
- Even administration systems
  - student grades
- Grid-Computing

The myLogin project of Freiburg University

- basis:
  - The existion **IdM-system** of the **myAccount** allows self administering your own account
  - Many (internal) applications already use the central IdM (LDAP)
- target:
  - **Single Sign-On** for these applications
  - Uniform authentication and authorisation process
  - „hide“LDAP via an intermediate layer (IdP)
  - No login data can be kept in decentral application
- partners:
  - University library (AAR): operates Shibboleth und VHO
  - University computing centre (URZ): operates LDAP
  - Hospital computing centre (KRZ): operates KRZ-LDAP
  - Rectorate: IdM-provider (they know…)
- Time frame:
  - Started March 2007
  - In operation since 1.9.2007
  - Continuously expanded to new services

550 Jahre
Albert-Ludwigs-Universität Freiburg
1457 – 2007

Status before myLogin project of Freiburg University



E-Learning

Bibliotheks-dienste

Seminararbeit

Personalisierte Dienste

E-Mail

IdM

Verwaltungs-systeme

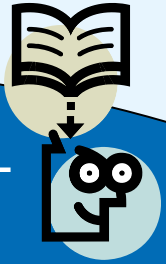
Ato Ruppert

myLogin project of Freiburg University – current and planned status

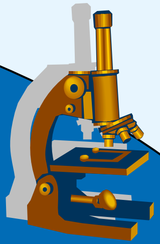
550 Jahre
Albert-Ludwigs-Universität Freiburg
1457 – 2007

E-Learning

Bibliotheksdienste

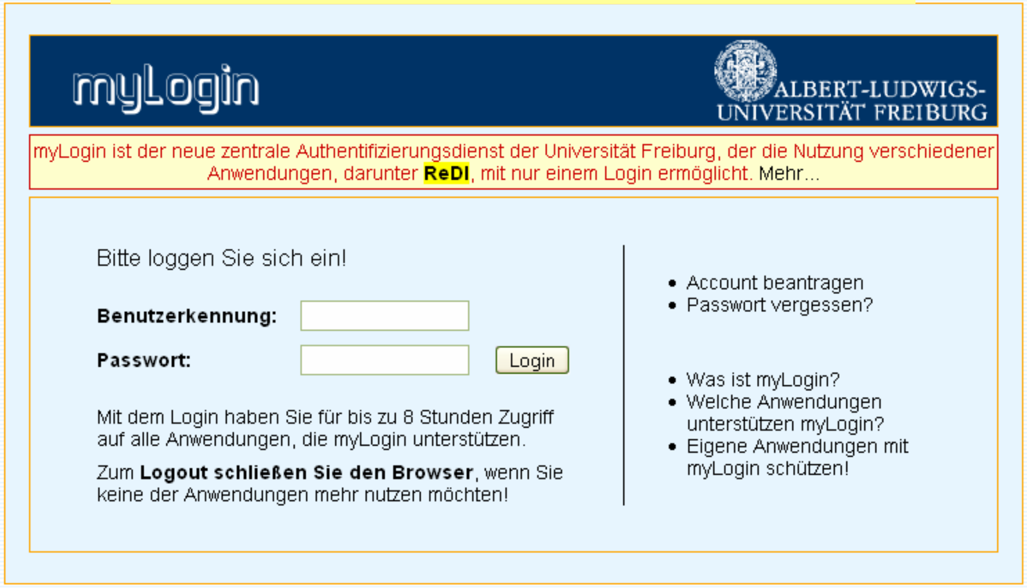


Personalisierte Dienste



Seminararbeit

Single-SignOn mit Shibboleth, ein Login für alle Dienste



myLogin

ALBERT-LUDWIGS-UNIVERSITÄT FREIBURG

myLogin ist der neue zentrale Authentifizierungsdienst der Universität Freiburg, der die Nutzung verschiedener Anwendungen, darunter **ReDI**, mit nur einem Login ermöglicht. Mehr...

Bitte loggen Sie sich ein!

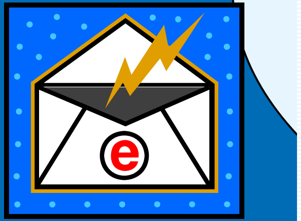
Benutzerkennung:	
Passwort:	

Mit dem Login haben Sie für bis zu 8 Stunden Zugriff auf alle Anwendungen, die myLogin unterstützen.

Zum **Logout schließen Sie den Browser**, wenn Sie keine der Anwendungen mehr nutzen möchten!

- Account beantragen
- Passwort vergessen?

- Was ist myLogin?
- Welche Anwendungen unterstützen myLogin?
- Eigene Anwendungen mit myLogin schützen!



E-Mail

Verwaltungssysteme