



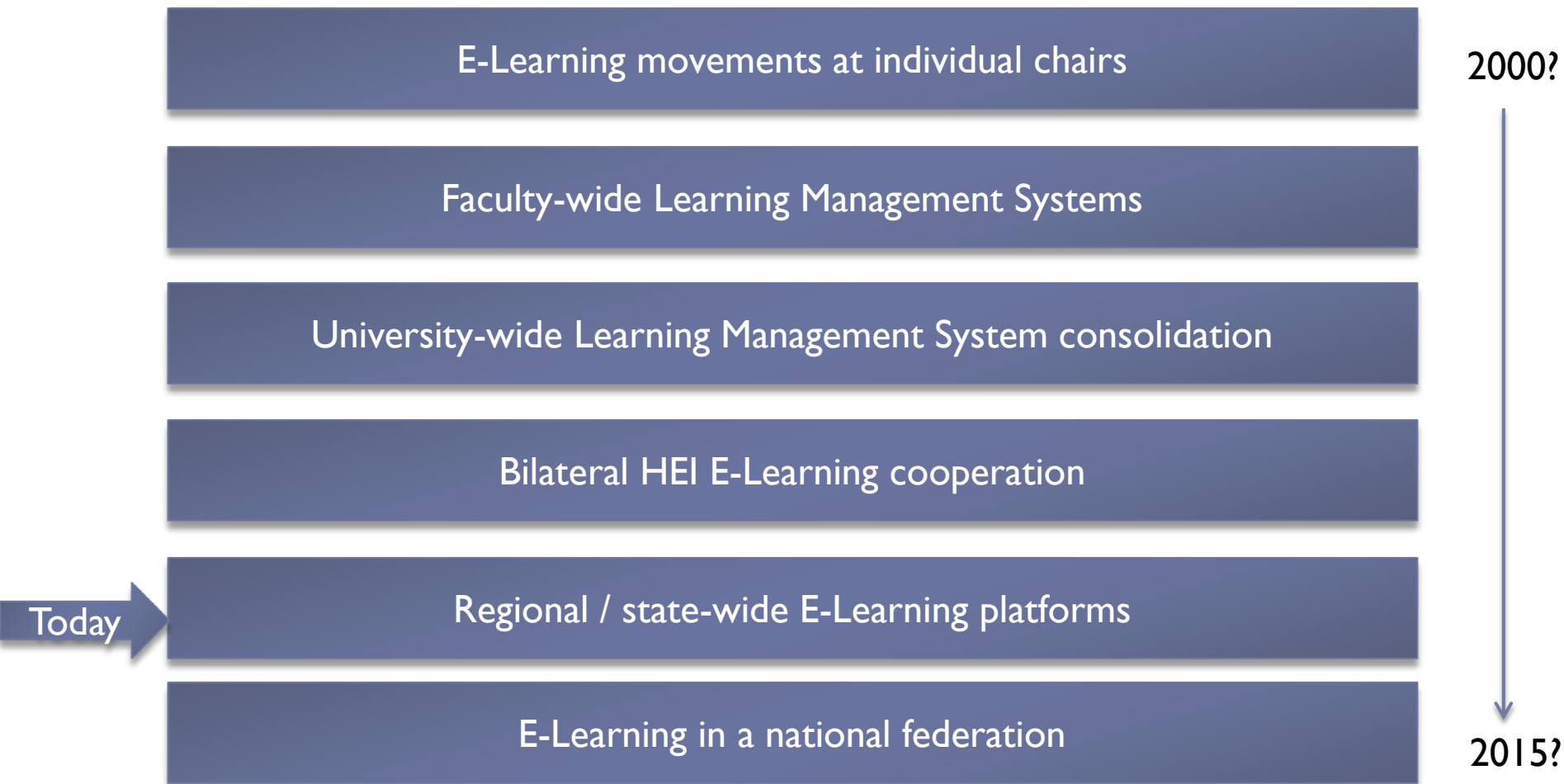
An identity management web service for privacy-preserving course authorization in federated E-Learning

EUNIS 2011

Ralf Ebner, Wolfgang Hommel
Leibniz Supercomputing Centre, Germany



► E-Learning milestones at German HEIs:



▶ Why?

- ▶ Lecturers can reach a much larger audience
- ▶ Students can take courses not offered locally and obtain certificates of achievement
- ▶ E-Bologna & virtual mobility



Image source: TU Clausthal

▶ How?

- ▶ Integration of Shibboleth-enabled Learning Management Systems in national authentication / authorization infrastructures (AAI)
- ▶ German DFN-AAI provides a standardized data schema: Compatible syntax and semantics across German HEIs



Prototype implementation for the Virtual University of Bavaria (VUB)

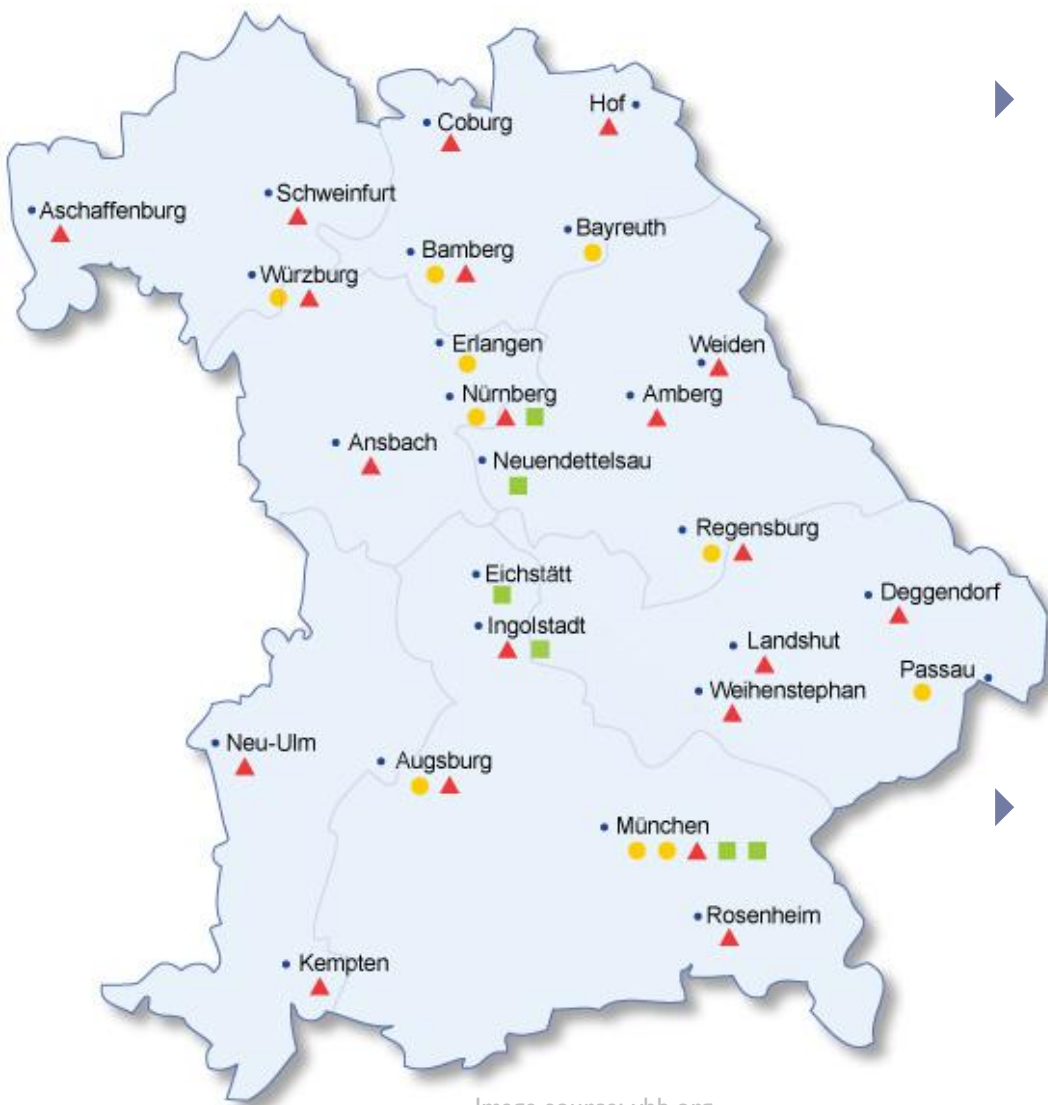


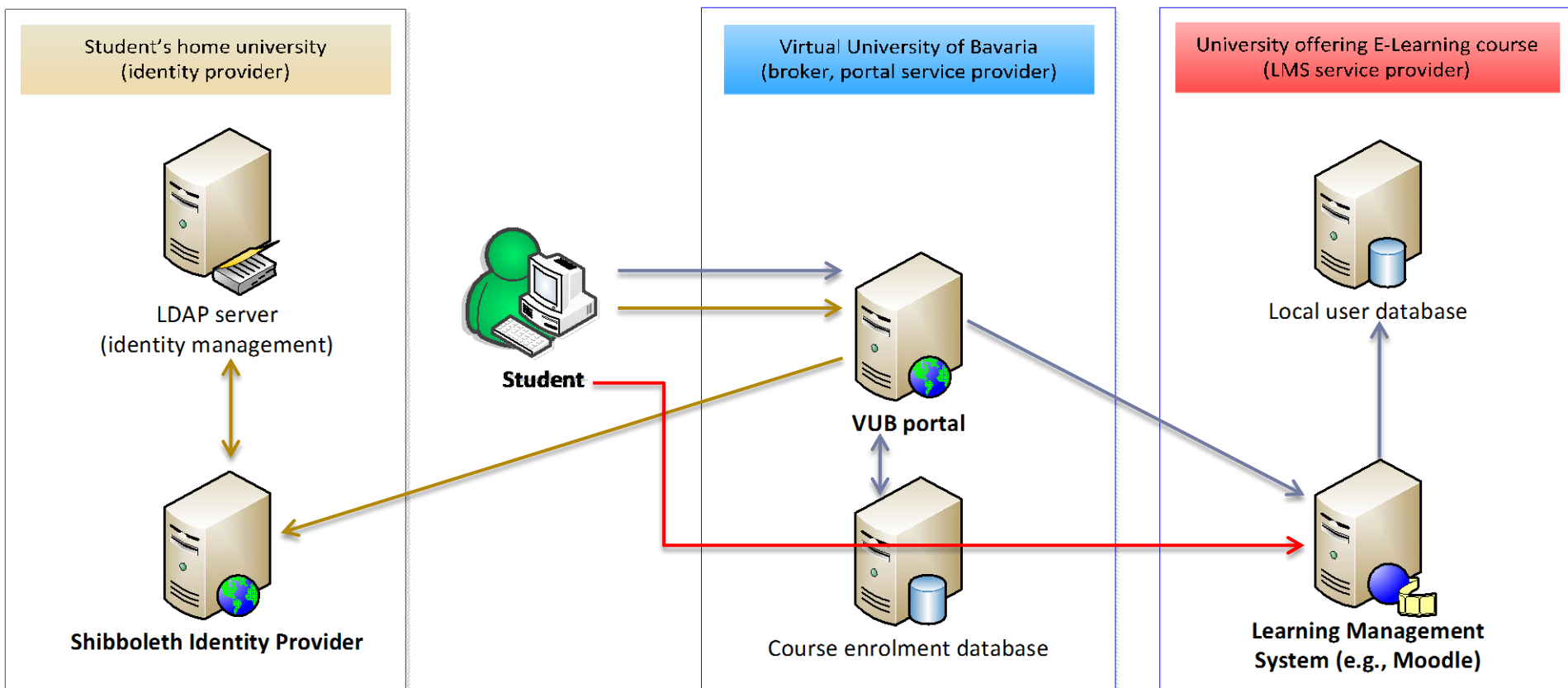
Image source: vhb.org

- ▶ VUB in figures:
 - ▶ Founded in 2000
 - ▶ 30+ member HEIs
 - ▶ ~20,000 students per semester
 - ▶ ~40,000 enrolments per sem.
 - ▶ 200+ courses offered per sem.

- ▶ Keynote by managing director Dr. Paul Rühl tomorrow noon

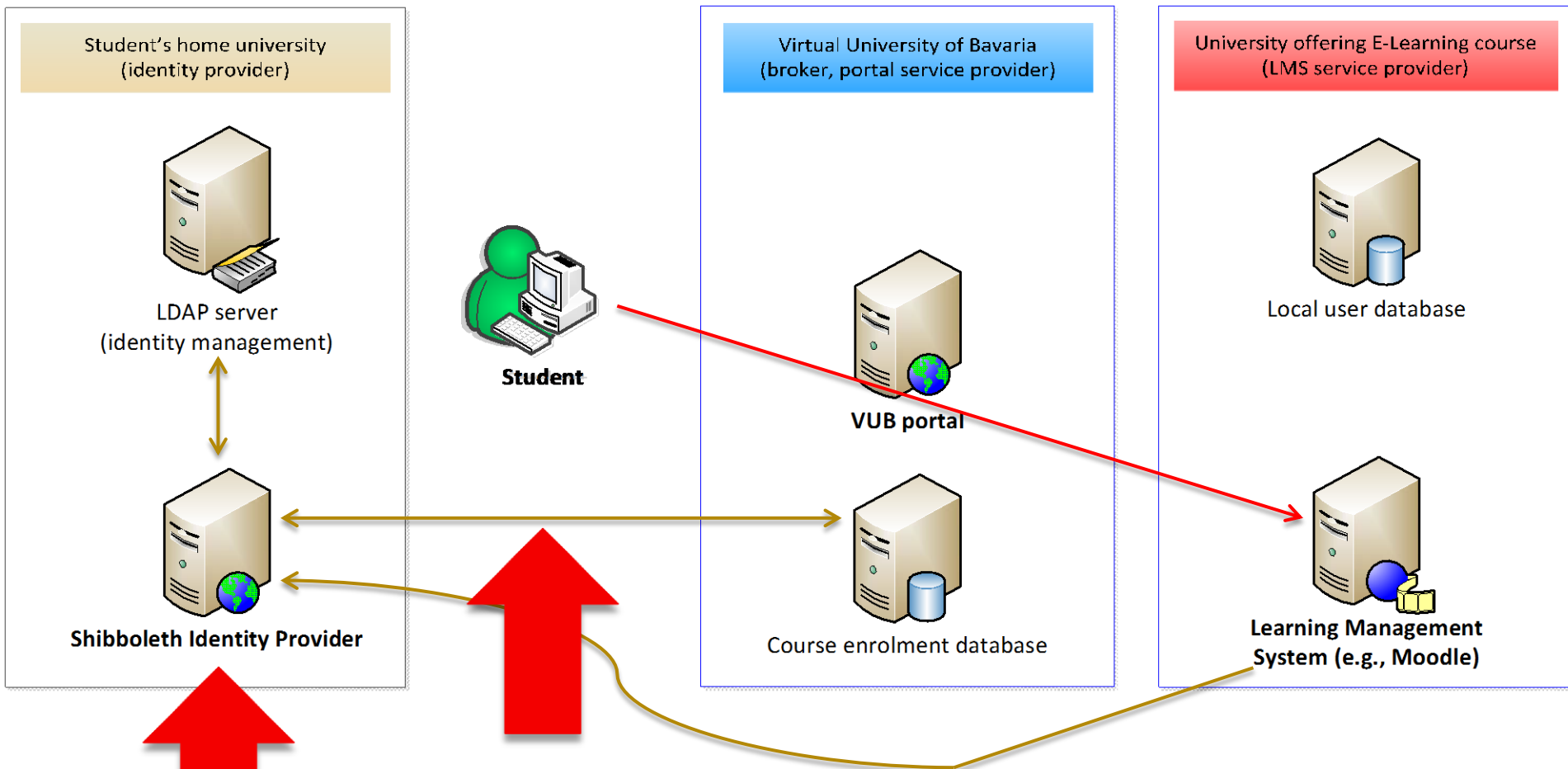


How VUB course enrolment works (logical view)





How we thought federation integration works (Shibboleth-based technical view, simplified)



2. **Enrolment data only transported** to LMS, but not stored at home university

1. Privacy issue: Login by **anyone** to **any SP** implicitly “reported” to VUB



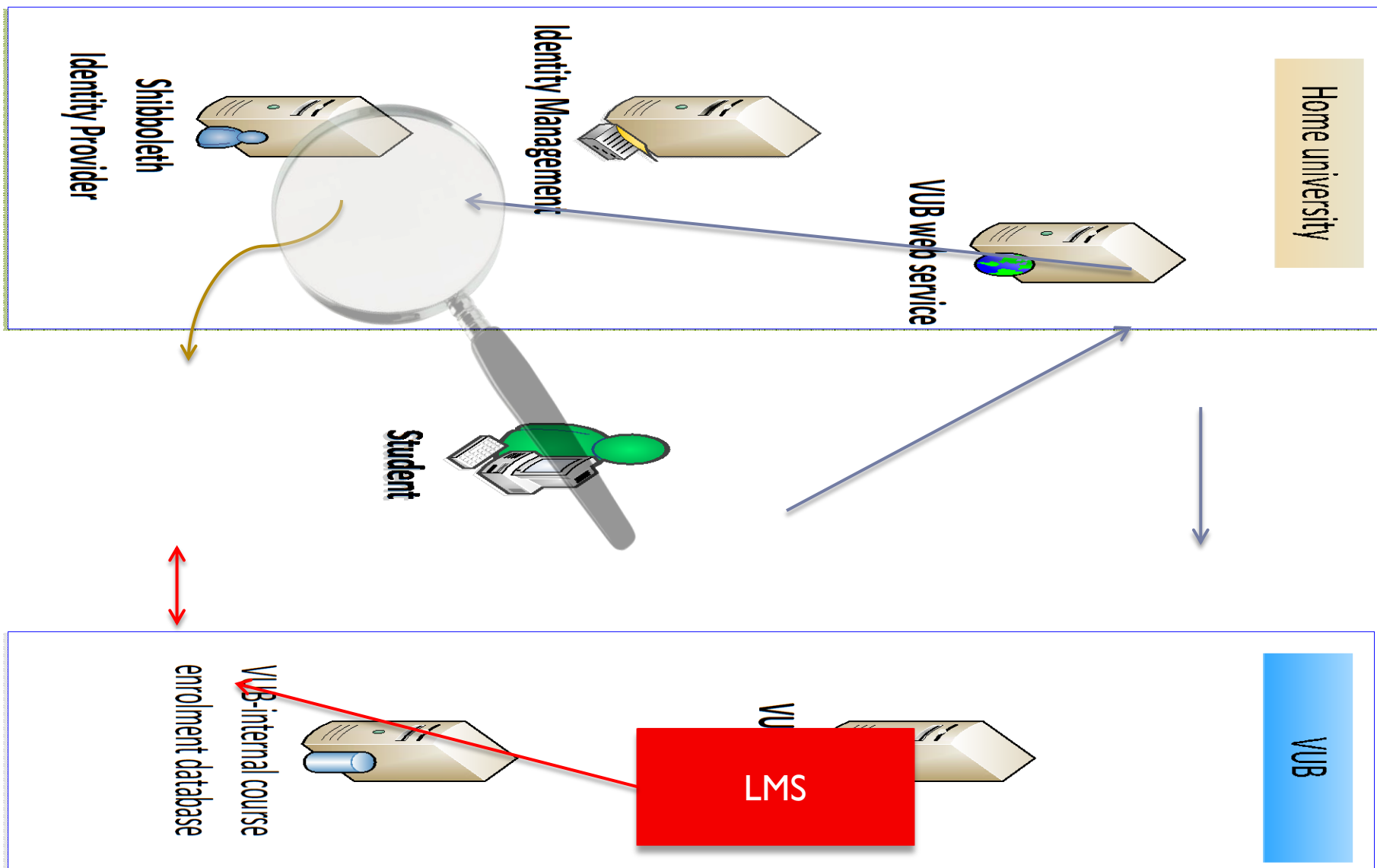
Issues that needed to be addressed



- ▶ 1. Privacy issue
- ▶ 2. Home university's enrolment overview issue
- ▶ 3. Stability issue:
 - ▶ Temporary unavailability (e.g., network failure or maintenance) of VUB course enrolment database results in technical error message
- ▶ 4. Incomplete Shibboleth coverage:
 - ▶ Not all of Bavaria's HEIs have a working Shibboleth IDP yet
 - ▶ Organizational issue, various solution strategies are available, e.g., IDP hosting as a DFN service



Basic workflow with the new solution

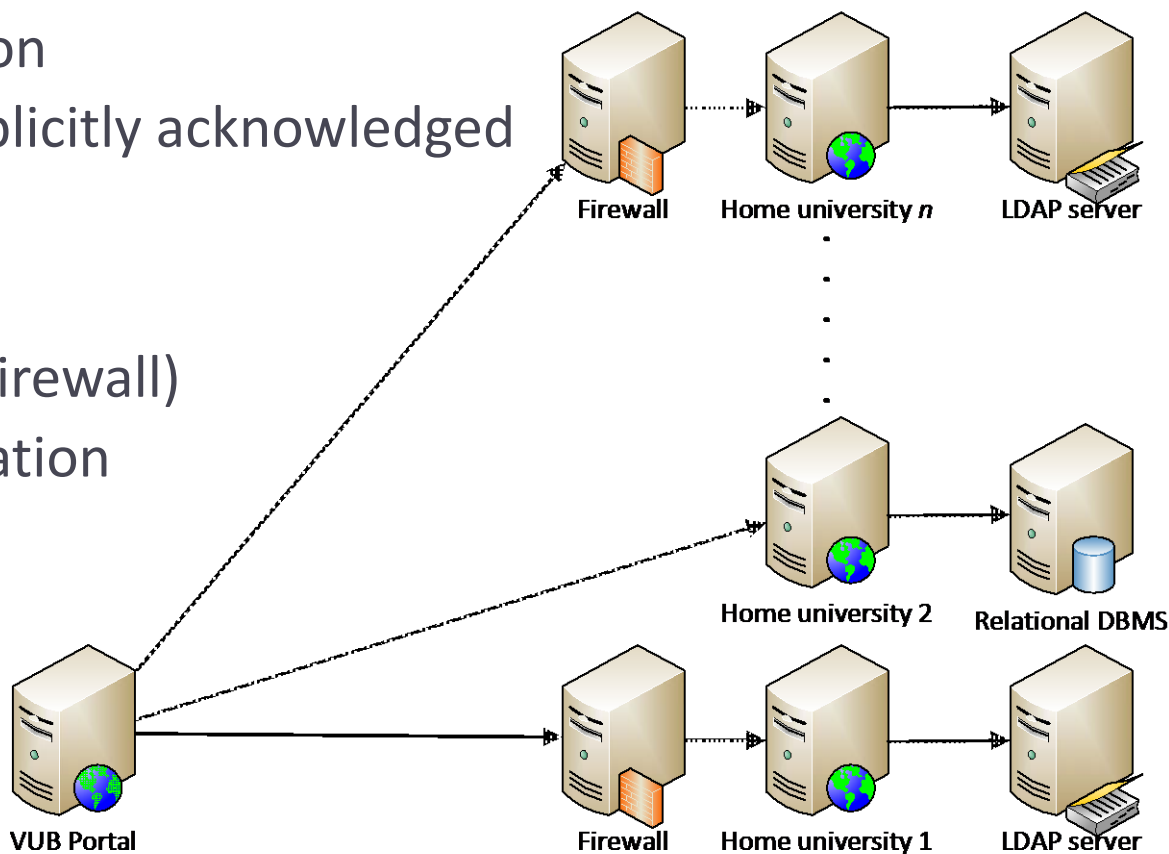


▶ Functionality

- ▶ Send add / delete events in near-real-time
- ▶ Batch operations
- ▶ Full re-synchronization
- ▶ Each operation is explicitly acknowledged

▶ Security

- ▶ IP address filtering (firewall)
- ▶ SSL-based authentication and encryption
- ▶ Operation counter limits (“anti-DoS”)

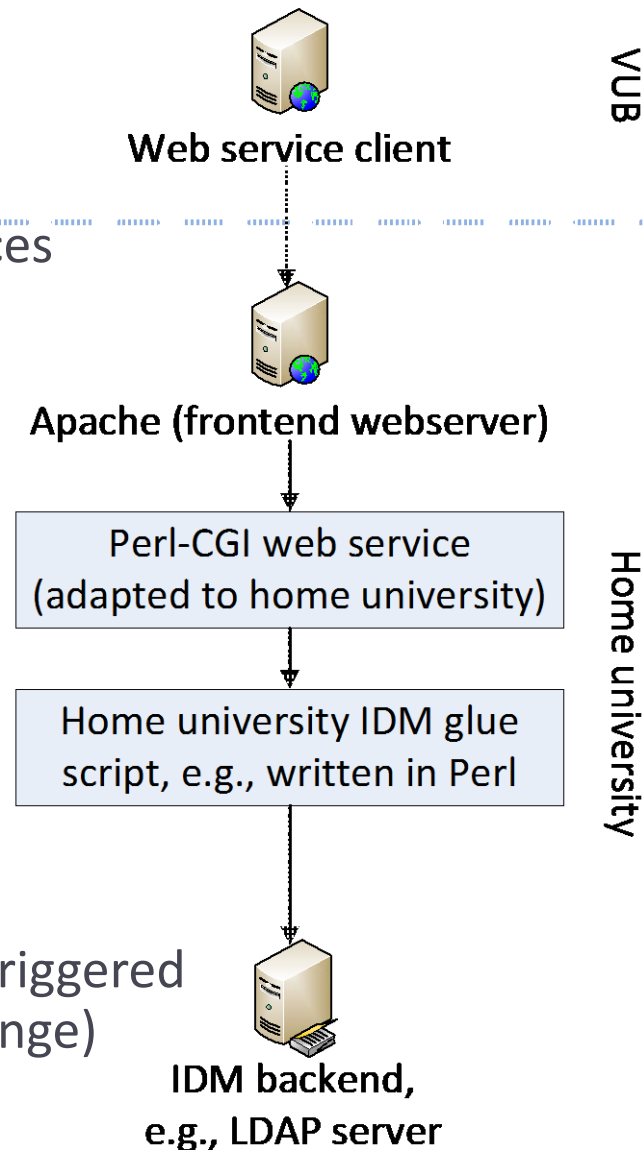


▶ Platform independence

- ▶ 30+ HEIs have various OS, web application servers, and programming language preferences
- ▶ Runs on Linux/Apache and Windows/IIS
- ▶ Supports LDAP and SQL backends
- ▶ Axis2-based Java and Perl-CGI implementations

▶ Automated metadata mgmt. (later)

- ▶ Manage endpoint changes w.r.t. IP filters
 - ▶ VUB's web service client IP address may change
 - ▶ Home universities' service IP:port may change
- ▶ VUB-sided web services for home-university-triggered actions will be needed (re-sync, metadata change)





Conclusion



- ▶ Lightweight technical solution had its drawbacks
 - ▶ User privacy
 - ▶ Operational stability

- ▶ New web service based solution
 - ▶ Fixes these issues
 - ▶ Has additional benefits
 - ▶ But comes at higher implementation costs

- ▶ Pilot usage planned for 3rd quarter 2011